LES DOSSIERS TECHNIQUES

ANALYSE DE RISQUES EN PRATIQUE

Pour qui ? Pourquoi ? Comment ?

Décembre 2022

CLUSIF

L’article L. 122-5 de la propriété intellectuelle n’autorisant pas les représentations ou reproductions intégrales, ou partielles, faites sans le consentement de l’auteur ou de l’ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d’une source licite et strictement réservées à l’usage privé du copiste et non destinées à une utilisation collective », analyses et les courtes citations dans un but d’exemple et d’illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du Clusif constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du code de la propriété intellectuelle.

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Anne-Catherine	**VIÉ**	ALL4TEC

Les contributeurs :

William	**BOURGEOIS**	WILLIAM BOURGEOIS CONSULTING
Hélène	**COURTECUISSE**	LISIS CONSEIL
Jean-Marc	**GRÉMY**	CABESTAN CONSULTANTS
Michaël	**JACQUES**	CYBERSECURITY BUSINESS SCHOOL
Jean-Philippe	**JOUAS**	CLUSIF
Xavier	**NICARD**	CONSEIL DÉPARTEMENTAL DU VAL-DE-MARNE
Jean	**OLIVE**	CGI FRANCE
Lazaro	**PEJSACHOWICZ**	CLUSIF
Thierry	**PERTUS**	CONIX
Hervé	**SCHAUER**	HS2

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Introduction

Ce guide, produit par l'Espace Risques et Méthodes du Clusif, est une introduction à l'analyse de risques. Il a pour objectif de vous familiariser avec les concepts et principes de base de toute analyse de risques, que ce soit dans le domaine de la cybersécurité ou ailleurs.

Ce document a semblé nécessaire, car mener une analyse de risques « à valeur ajoutée » reste un exercice difficile. Le succès de la démarche dépend de nombreux facteurs : de la mise en place du projet, en passant par l'implication des parties prenantes (managers, équipes, etc.), le choix de la méthode[1], sans même parler de son impact sur l'organisation ni du fait qu'il faut généralement faire vivre cette analyse de risques dans le temps. Dans ce cas, il ne s'agit pas d'une analyse ponctuelle, mais bien d'un processus et il serait plus juste de parler de gestion, voire de gouvernance des risques.

L'analyse de risques est une discipline ancienne, largement utilisée dans le domaine de la sûreté de fonctionnement. Elle est devenue depuis quelques années un élément clé des systèmes de management inspirés de l'ISO 9001, comme de l'ISO/CEI 27001 qui traite de la sécurité de l'information.

Il a été pris le parti de s'inspirer de l'ISO/CEI 27005, qui contient des lignes directrices relatives à la gestion des risques liés à la sécurité des systèmes d'information. L'ISO/CEI 27005 n'est pas une méthode, mais un ensemble de recommandations qui permettent de déployer correctement une méthode d'analyse de risques dans le cadre d'un processus.

L'approche « systèmes d'information » peut sembler restrictive, mais il faut prendre conscience que nous-mêmes, personnes physiques, sommes une partie essentielle des systèmes d'information, que ces derniers ne peuvent pas fonctionner sans locaux ni énergie ou maintenance et que tout dysfonctionnement peut avoir des conséquences financières, juridiques…

Certes, il existe des risques non couverts par cette approche (par exemple, la non-solvabilité d'un client important), néanmoins, cette démarche permet une vision globale des risques d'exploitation et peut être transposée à d'autres domaines.

2 Contexte du document

2.1 À qui est destiné ce document ?

Le public visé par la première partie de ce guide est large :

- Toute personne, expert ou non expert, qui a besoin de faire une ou des analyses de risques, obligatoires ou non ;
- Les différents interlocuteurs qui vont recevoir les résultats des analyses de risques et notamment les décideurs qui doivent valider la démarche et les moyens mobilisés ;
- Les RSSI, DSI et autres personnes impliquées dans la gestion des risques de leur organisme : chefs de projet, consultants, directions générales, etc. ;
- Plus généralement, les parties prenantes dont il est question par la suite.

La seconde partie donne quelques pistes en matière d'outils et est destinée à un public plus averti.

La démarche d'analyse de risques est née du souci des spécialistes d'aider les entreprises à préserver la continuité de leur informatique et de protéger les informations qui y étaient traitées. Initialement, des documents spécifiques en général liés aux méthodes étaient

[1] *Par méthode (d'analyse de risques), il est entendu un ensemble structuré de processus et de tâches conduisant à l'identification, l'analyse, l'appréciation et l'évaluation des risques, dans un contexte défini.*

suffisants, puisque généralement, seules les conclusions étaient présentées aux « non-initiés ».

Comme le traitement de l'information a pénétré l'ensemble des fonctions de l'entreprise et qu'il est de ce fait devenu transverse, les risques auxquels cette information et ce traitement étaient exposés sont devenus très (voire trop) importants pour des métiers n'ayant pas nécessairement de rôle dans les analyses.

L'analyse et le traitement des risques liés à l'information sont aujourd'hui exigés dans un nombre important de domaines. Par exemple, l'accord bancaire Bâle 2 introduit le risque informationnel parmi les risques opérationnels du monde de la finance, la loi Sarbanes-Oxley (loi SOX)[2] oblige les dirigeants à maîtriser les informations ou encore le RGS oblige les autorités administratives à homologuer la bonne maîtrise des risques dans tous les traitements exposés en externe.

D'ailleurs, pour les entreprises, le RGPD élargit le besoin d'analyse à toutes les personnes concernées par le traitement des données : une analyse d'impact relative à la protection des données (AIPD) est obligatoire quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Ces quelques exemples montrent qu'une population bien plus importante que celle habituée aux analyses de risques, composée des DG, DAF, DRH, DSI et bien d'autres, ont aujourd'hui besoin de s'impliquer dans le processus de détermination des risques informationnels et de leur maîtrise.

C'est en pensant à eux et à leurs besoins que l'Espace Risques et Méthodes du Clusif a réalisé ce document.

Les experts ne devraient rien découvrir de nouveau dans ce document. Néanmoins, sa lecture pourra alimenter leur réflexion pour déterminer les formes de dialogue avec leur public, voire les aider à sensibiliser leurs interlocuteurs.

2.2 De quoi parle ce document ?

Il est question de risques et d'analyse de risques.

La notion de risque est difficile à définir de manière générale sans prendre en compte son contexte d'usage. Il existe en effet plusieurs types de risques : humains, juridiques, financiers, environnementaux, industriels, etc.

Tentons une première définition issue de l'ISO 31000 (ISO 73) : « le risque est l'effet de l'incertitude sur l'atteinte des objectifs ».

Le présent document s'intéresse aux risques liés au système d'information.

La notion de système d'information inclut tous les modes de traitement de l'information dont les supports écrits et oraux.

2.2.1 De quels risques parle-t-on ?

Appliquée spécifiquement au système d'information, l'incertitude peut, par exemple, être le fait qu'un « hacker » profite d'une faille du site web pour s'introduire dans le réseau informatique de l'entreprise ou bien le fait qu'un utilisateur commette une négligence en diffusant par erreur des informations confidentielles.

L'analyse de risques de sécurité des systèmes d'information ne s'intéresse pas directement aux scénarios de risques dont les origines relèvent de facteurs financiers, juridiques, etc. En revanche, elle intègre bien l'évaluation des conséquences de nature financière, juridique, etc.

Il est essentiel de ne pas confondre analyse de risques et audit de sécurité. Un audit de sécurité procède à un examen méthodique de toutes les composantes et de tous les acteurs

[2] *Public Law 107-204*

de sécurité[3] effectué à des fins de contrôle de conformité, d'évaluation de l'adéquation des moyens (organisationnels, techniques, humains, financiers) investis au regard des risques encourus, d'optimisation, de rationalité et de performance.

2.2.2 Des risques sur l'information à ceux issus du cyberespace

Dans l'ensemble de « l'univers des risques » auquel tout organisme peut se voir confronté, le présent document, compte tenu du domaine de compétences revendiqué par le Clusif et comme déjà énoncé au §1.4, s'intéresse spécifiquement aux risques liés aux systèmes d'information. Ces derniers concernent les sources (défaillance, erreur de manipulation, cybermenace, etc.) et facteurs (exposition en matière de connectivité, vulnérabilités, défaut de protection, négligence, etc.) de risques susceptibles d'affecter les systèmes d'information en tant qu'éléments de la chaîne de productivité (actifs) à protéger, avec pour conséquence de potentielles répercussions générant des impacts directs ou indirects divers et variés (opérationnels, juridiques, financiers, réputationnels, industriels, sociétaux, etc.). Ainsi, il est admis que le champ d'application couvre potentiellement le « portefeuille de risques » suivant :

- **Risques informationnels** : risques liés aux actifs informationnels et supports associés, qu'ils soient tangibles (documents papier, système d'éditique, etc.) ou intangibles (données structurées telles que les documents numériques ou les data lake, données non structurées telles que les bases de données, etc.). Les critères de risque sont multiples (qualité / sécurité / traçabilité des données, efficience / interopérabilité / maintenabilité des systèmes, traitements et services, optimisation / agilité / contrôle des processus, etc .).
- **Risques numériques (ou informatiques) :** risques liés aux actifs numériques ou au « digital » (infrastructures informatiques, services et traitements informatisés, personnel utilisateur, exploitant ou mainteneur des ressources informatiques, processus métier informatisés, projets digitaux ou de transformation numérique, processus de gestion des systèmes d'information, etc.). Les critères de risques restent du même ordre que ceux mentionnés précédemment.
- **Risques liés à la sécurité de l'information (ou à la sécurité des systèmes d'information) :** risques spécifiquement liés à la sécurité des actifs informationnels (domaine incluant la protection des données personnelles). Les critères de risque, ou « critères de sécurité », communément admis sont à minima la disponibilité, l'intégrité, la confidentialité (on parle alors de critères DIC), parfois étendus à la traçabilité (possibilité d'audit, imputabilité, non-répudiation, etc.), l'authenticité (authentification, légitimité d'accès, etc.).
- **Cyberrisques :** risques spécifiquement liés à la sûreté numérique vis-à-vis de la malveillance intentionnelle issue généralement du cyberespace, mais éventuellement internes (codes malveillants, hacktivisme, cybercriminalité, cyberterrorisme, etc.) ; les risques endogènes liés à des menaces internes non intentionnelles (erreur de manipulation, usage inapproprié, traitement illégitime) ou encore à des défaillances d'origine accidentelle (panne, dysfonctionnement, etc.) étant généralement exclus, par convention. Les critères de sécurité restent du même ordre que ceux mentionnés pour les risques liés à la sécurité de l'information.

Il est également intéressant de préciser que ces types de risques peuvent se trouver « combinés », c'est-à-dire que les risques liés à la sécurité de l'information (comme pour les risques informationnels) peuvent aussi être traités comme des cyberrisques / risques numériques.

Ce sont ces risques dont il est question dans ce document.

[3] *Politique, mesures, solutions, procédures, et moyens mis en œuvre par une organisation, pour sécuriser son environnement.*

2.3 Glossaire

Avant de poursuivre, il semble important de préciser les significations de tous les acronymes déjà utilisés et à venir sur la suite du document :

Acronyme	Signification
Afnor	Association française de normalisation
AIPD	Analyse d'impact relative à la protection des données
AMDEC	Analyse des modes de défaillances, de leurs effets et de leur criticité
ANSSI	Agence nationale pour la sécurité des systèmes d'information
AR	Analyse de risques
CNIL	Commission nationale de l'informatique et des libertés
DAF	Direction administrative et financière
DG	Direction générale / directeur général
DIC (P ou T)	Disponibilité, intégrité, confidentialité (preuve ou traçabilité) = critères de sécurité
DINUM	Direction interministérielle du numérique
DRH	Direction / direction des ressources humaines
DPS2	Directive sur les paiements et services v2
DSI	Direction / directeur des systèmes d'information
DUER	Document unique d'évaluation des risques
EBIOS (RM)	Expression des besoins et identification des objectifs de sécurité (risk manager) : méthode d'analyse de risques développée et supportée par l'ANSSI
ISO/CEI	International Standard Organisation / Commission électrotechnique internationale
IT	Information Technology
LPM	Loi de programmation militaire
LSF	Loi de sécurité financière
MEHARI	Méthode harmonisée d'analyse de risque : méthode d'analyse de risques développée et supportée par le Clusif
MOA/MOE	Maîtrise d'ouvrage / maîtrise d'œuvre
NIS	Network and Information Security
PSSIE	Politique de sécurité des systèmes d'information de l'État
PSST	Protection du potentiel scientifique et technologique
RGPD	Référentiel général de protection des données
RGS	Référentiel général de sécurité
RSSI	Responsable de la sécurité des systèmes d'information
(S)SI	(Sécurité du) système d'information
SMSI	Système de management des systèmes d'information

3 Les notions de base

Le vocabulaire et les définitions varient d'une méthode à l'autre, cependant les points fondamentaux restent les mêmes.

Il s'agit d'identifier des « événements » qui ont des « impacts » négatifs sur des « actifs vulnérables », avec une certaine « vraisemblance ».

Le risque se définit comme la combinaison d'un niveau de gravité (en lien avec le ou les impacts sur l'entreprise) et de la vraisemblance de ces événements. La combinaison de la gravité et de la vraisemblance donne le niveau de risque.

Ce niveau est ensuite comparé à un niveau d'acceptabilité défini par l'entreprise. Chaque risque non acceptable doit être traité en définissant, puis en mettant en œuvre une ou des mesures de sécurité pour le réduire ou par des mesures d'évitement ou de transfert.

3.1 Pourquoi s'intéresser aux risques ?

3.1.1 Identifier les risques de l'organisation

Le premier des champs d'application de l'analyse de risques est sans grande surprise celui de l'identification des risques de l'organisation.

Dans bien des cas, il peut être très difficile pour des dirigeants, des responsables métier et même des RSSI, de **déterminer des risques qui peuvent avoir des conséquences importantes** pour leurs propres objectifs. Pour garder une objectivité dans la démarche, seule une méthode d'analyse des composantes du risque peut être utilisée.

Parmi les conséquences importantes de risques pour une entreprise ou un organisme public, les éléments suivants peuvent être cités :

- la perte financière,
- la perte de réputation,
- la fraude,
- l'atteinte à la propriété intellectuelle et industrielle,
- la perte de savoir-faire ou d'avantage concurrentiel,
- la dégradation de la qualité des produits,
- l'accident humain ou environnemental ;
- la pénalité et la perte de contrat,
- la plainte et procédure judiciaire,
- la chute de cours de bourse.

Pour identifier ces risques, en déterminer les conséquences ainsi que les conditions et raisons de leur occurrence, et afin de les mettre sous contrôle, il est nécessaire de réaliser une analyse de risques.

3.1.2 Identifier les risques liés aux exigences légales ou réglementaires

De plus en plus de lois nationales, de législations internationales ou de réglementations sectorielles ont des exigences de sécurité logiques et physiques pour les systèmes d'information.

- Réglementations générales :
  - européennes :
    - Référentiel général pour la protection des données (RGPD – sécurité des données personnelles) ;
    - Network and Information Security (NIS – sécurité des opérateurs de services essentiels et des fournisseurs de services numériques) ;
    - Autres
  - françaises :
    - loi relative à la protection des données personnelles (CNIL),
    - loi de programmation militaire (LPM – sécurité des opérateurs d'importance vitale) ;
    - référentiel général de sécurité (RGS – téléservices des administrations),
    - politique de sécurité des systèmes d'information de l'État (PSSIE – organismes publics) ;
    - code pénal ;
    - instruction générale interministérielle sur la protection du secret de la défense nationale (IGI 1300) ;
    - protection du potentiel scientifique et technologique (PPST).
    - Autres
- Réglementations sectorielles :
  - internationales : PCI-DSS (protection des données porteur de cartes de paiement), SOXA, etc. ;
  - européennes : Bâle (banques), solvabilité (assurances), directive sur les paiements et services v2 (DPS2), etc. ;
  - françaises : Autorité des marchés financiers (établissements financiers), ACPR (assurances), hôpital numérique et certification HAS (hôpitaux), etc.

Ces **réglementations font toutes clairement apparaître l'existence des risques** comme des conséquences négatives sur l'organisme d'événements connus s'ils venaient à se produire. À ce titre, l'analyse de risques qui doit être faite revêt deux dimensions :

- Les mesures exigées par la réglementation ou la loi sont-elles en place ?
- Les composantes du risque sont-elles sous contrôle ?
  La réponse à cette dernière question pourra être positive si :
  - la menace et l'agent de la menace sont clairement identifiés et surveillés ;
  - les possibles vulnérabilités techniques ou les faiblesses de l'organisation sont connues et maîtrisées.

Certaines réglementations induisent un vocabulaire spécifique, par exemple :

- les « risques élevés » du RGPD (analyse d'impacts, analyse de risques),
- la rédaction d'un document unique d'évaluation des risques (DUER),
- l'homologation de sécurité : obligatoire par des textes, tels que l'IGI 1300, le RGS et la PSSIE.

Un point important, sous-tendu dans cette approche, est la vision « conformité » de la gestion des risques et ne pas être conforme à ces réglementations induit plusieurs types de risques :

- Amendes pour la société ou l'organisme (Code civil, RGPD, CNIL, etc.).
- Perte d'agrément, de certification ou d'autorisation de fonctionnement (par exemple : AMF, Bâle, solvabilité, hôpital numérique/HAS, HDS, NIS, etc.).

- Perte de réputation en cas d'incidents de sécurité.

La non-conformité devient donc un risque à part entière. C'est sans doute à cause de cette posture que la conformité n'est jamais égale à la sécurité. Le seul but recherché est de répondre aux exigences, mesurables et vérifiables. Un rare cas de figure est sans doute l'alignement de la conformité à un ensemble d'exigences cadré et suivi dans un SMSI certifié.

3.1.3 Piloter par les risques

La démarche d'identification, d'analyse et la gestion des risques doit s'intégrer aux processus décisionnels de l'organisation afin d'ancrer les résultats de cette analyse dans la vie opérationnelle de l'entité (par exemple, au travers d'une revue formelle en comité de direction).

Il s'agit là de mettre en œuvre un réel « pilotage par les risques » afin, notamment, de prendre conscience des enjeux qui en découlent pour l'organisation. Il sera important d'effectuer des revues de ces risques à intervalles réguliers, de remettre en contexte ces risques et les évolutions de l'organisation (business, managériale, contexte politique, etc.) afin que ce travail d'analyse de risques permette un pilotage en amont des problématiques.

3.1.4 Les avantages induits par une analyse de risques

D'autres avantages pour l'entreprise peuvent aussi justifier des analyses de risques :

- *Mieux manager un projet* : l'efficacité et même la valeur d'une entreprise dépendent des informations qu'elle possède et de la qualité de son traitement. Il en résulte que les risques encourus par ses informations peuvent avoir un impact important sur l'état de santé de l'entreprise. Or, à chaque nouveau projet informatique, de nouvelles expositions aux risques en matière de critères DIC (P ou T) sont générées. Il est donc pertinent de faire une analyse de risques pour tout projet majeur de traitement de l'information, et très particulièrement si ces informations se trouvent exposées aux cyberrisques ;
- *Formaliser des méthodes de développement de projets informatiques* : si des analyses de risques complètes sont nécessaires pour les grands projets, ceci n'est pas en général envisageable pour les petits ou ceux non exposés aux cyberrisques. Toutefois, afin de ne pas créer des maillons faibles, il est important que la méthodologie de développement intègre les besoins de protection des informations. Une démarche d'analyse de risques sera donc nécessaire pour bien prendre en compte les risques spécifiques de l'entreprise ;

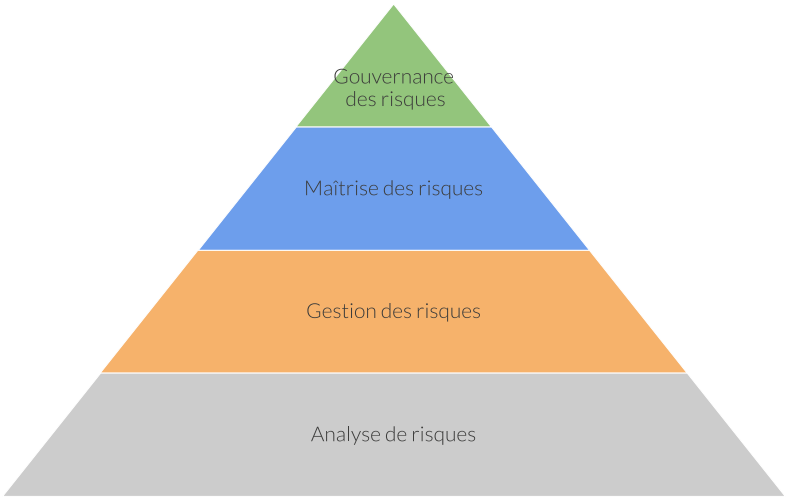
  Ce point est particulièrement important dans le cas du développement des projets avec la méthode Agile où l'utilisation de l'approche Agile et la sécurité numérique de l'ANSSI sont fortement conseillées. Par ailleurs, une nouvelle version de cette approche est en cours d'élaboration par l'ANSSI avec la collaboration de la DINUM et du Clusif ;
- *Procurer un* avantage *concurrentiel* : l'analyse de risques, au-delà de ses aspects « défensifs », peut être vue, dans certains cas, comme un apport, donnant un avantage concurrentiel à l'entreprise. Si la sécurité de l'information est de plus en plus une demande des clients, il peut être nécessaire de faire une analyse de risques et la compléter par une certification de la gestion des risques du type 27001 ou plus spécifique. Toutefois, et notamment dans le cas de recherche d'un partenaire, des sociétés peuvent donner une nette préférence à des partenaires qui ont bien identifié leurs risques, surtout si ces partenaires ont mis en place une démarche d'amélioration continue et de traitement des risques / d'information.
- Offrir une méthode pour aborder la négociation des polices d'assurance cyberrisque permettant d'adapter celles-ci aux risques réels encourus par l'entreprise.
- *Sensibiliser* : la mise en évidence de risques avec des scénarios réalistes et des impacts concrets pour l'organisation est une composante majeure de toute sensibilisation qui veut donner un contenu concret aux différents sujets traités, permettant que celle-ci ne se résume pas à une quantité de règles abstraites.

- *Optimiser l'allocation des ressources dédiées à la sécurité du système d'information* : l'analyse de risques permet d'identifier les domaines où focaliser les efforts et le budget : cela aide à déterminer des priorités pour éviter de soupoudrer les ressources limitées de l'organisation.

3.2 Les concepts intangibles

3.2.1 Gouvernance, maîtrise, gestion et analyse de risques

L'analyse de risques fait partie d'un tout que l'on peut représenter par la pyramide ci-dessous :



Analyse de risques :

- Processus d'identification, d'estimation et d'évaluation des risques afin de décider du traitement des risques retenus (AFNOR – FD X50-117).
- Déclinaison des menaces en cartographie des risques et définition des plans de contrôle.

Gestion de risques :

- Processus de traitement, de suivi et de contrôle, de mémorisation des risques recensés et des actions entreprises pour les traiter (AFNOR - FD X50-117).
- Identification et évaluation des risques opérationnels.

Maîtrise des risques :

- Maîtriser les risques à un niveau acceptable en fonction des critères de risques retenus.
- Mettre en place un plan d'action pour traiter les risques résiduels et choix des actions à mettre en œuvre pour leur réduction.

Gouvernance des risques :

- Assumer la responsabilité générale de l'approbation des politiques de gestion des risques.
- Assumer les responsabilités de surveillance de la gestion des différents risques.
- Vision globale des risques de l'entreprise (risques stratégiques, financiers, opérationnels, etc.).
- La gouvernance des risques est un volet central dans toute démarche de gestion de risques.

3.2.2 Le vocabulaire

Celui qui découvre les principes d'une analyse de risques peut rencontrer des difficultés lorsqu'une même notion peut avoir des termes différents suivant les méthodes utilisées.

C'est pourquoi, le vocabulaire de base a été rassemblé dans ce tableau :

Termes / expressions	Signification
Source de menace	Elle peut être accidentelle (événement climatique, panne d'un équipement) ou délibérée (une organisation criminelle à but crapuleux, un état à but d'affaiblissement d'un adversaire, un employé frustré souhaitant se venger, etc.).
Actif primordial (ISO 27005) Bien essentiel (EBIOS 2010) Valeur métier (EBIOS RM) Actif primaire (MEHARI)	Information, connaissance, procédé, processus de management ayant une valeur pour l'entreprise (qui est nécessaire à son fonctionnement, lui fournit un avantage concurrentiel, qu'elle doit contractuellement protéger, etc.). (ISO 27005)
Actif support (ISO 27005, MEHARI) Bien support (EBIOS 2010 / RM)	Support (système, fichier, personne, papier, etc.) qui contient un actif primordial et peut comporter des vulnérabilités.
Menace	Cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme (humaine, technique, environnementale, etc. (ISO 27000)
Mesure de sécurité	Mesure qui modifie un risque. (ISO 27005/ISO 73:2009) NOTE 1 : Une mesure de sécurité du risque en sécurité de l'information inclut n'importe quel processus, politique, procédure, recommandation, dispositif pratique ou organisation, qui peut être d'ordre administratif, technique, managérial ou juridique et qui modifie le risque en sécurité de l'information. NOTE 2 : Une mesure de sécurité du risque n'aboutit pas toujours à la modification voulue ou supposée. NOTE 3 : Une mesure de sécurité du risque est également utilisée comme synonyme de protection ou contre-mesure.
Vulnérabilité	Faille qui peut être exploitée par une ou plusieurs menaces. (ISO 27000)
Risque	Menace qui exploite une vulnérabilité et a un impact sur un actif.
Base de connaissances	Une **base de connaissances** regroupe des connaissances spécifiques à un domaine spécialisé donné, sous une forme exploitable par un ordinateur.
Propriétaire du risque	Personne qui va assumer la gestion du risque au quotidien.
Niveau de risque	S'exprime en termes de combinaison des conséquences et de vraisemblance. (ISO 27000)
Traitement du risque	Processus destiné à modifier un risque. (ISO 31000)

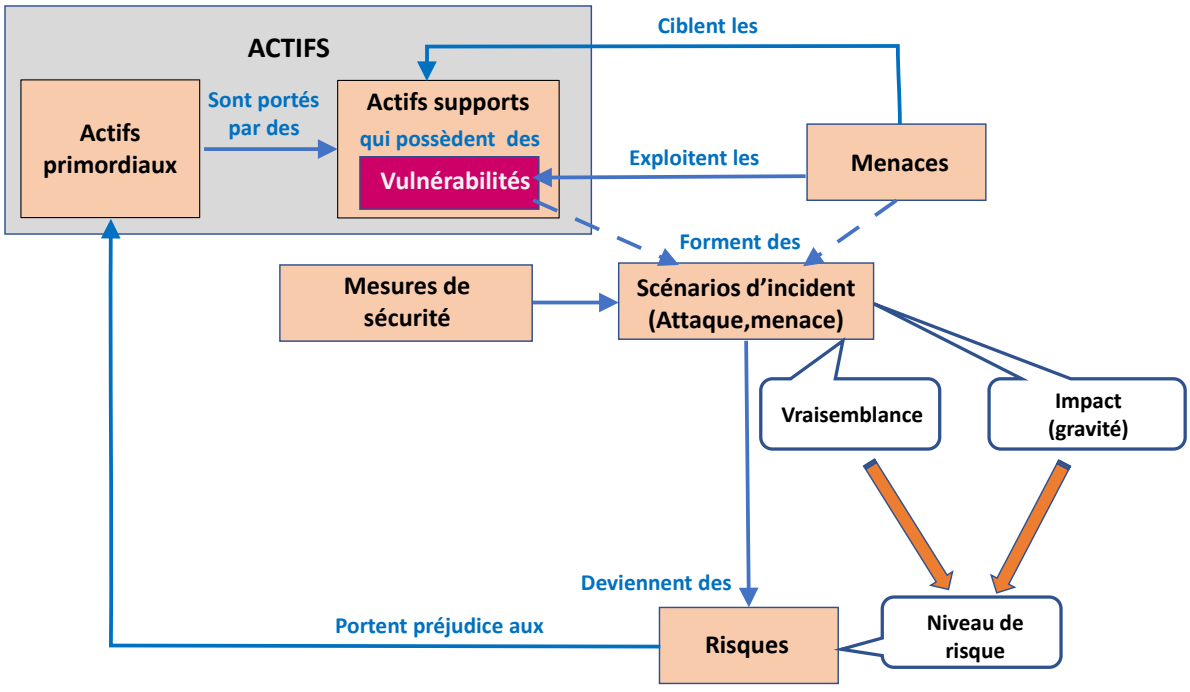
Termes / expressions	Signification
	NOTE 1 : Le traitement du risque peut inclure : • un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque, • la prise ou l'augmentation d'un risque afin de saisir une opportunité, • l'élimination de la source de risque, • une modification de la vraisemblance, • 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. NOTE 2 : 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 ». NOTE 3 : Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

3.2.3 Risque, menace, actifs : comment s'y retrouver ?

Une menace intentionnelle ou délibérée cible un actif (support) dont elle exploite une vulnérabilité.

L'incident ainsi généré a un impact sur l'actif primordial.

La combinaison de la vraisemblance et de la gravité (issue des conséquences) permet d'estimer le niveau du risque.



3.2.4 Contenu de l'analyse de risques

Identification et analyse détaillée des scénarios de risque

Faire une analyse de risques, c'est d'abord étudier en détail et analyser ce qui pourrait arriver de préjudiciable en termes d'impacts sur le périmètre considéré (un ou plusieurs systèmes ou voire au niveau de l'organisation elle-même).

Les éléments étudiés sont :

- les sources de menace accidentelles et délibérées ;
- les causes et les menaces :
  - certaines sont très anciennes et assez bien identifiées :
    - incendies, inondations, phénomènes climatiques ;
    - pannes, coupures ;
    - erreurs ;
    - vols, pertes ;
    - bugs.
  - d'autres apparaissent régulièrement, au fur et à mesure des évolutions technologiques, et ne sont pas maîtrisées :
    - chiffrement de fichiers par un ransomware ;
    - attaque avancée persistante (APT) ;
    - mails de phishing (hameçonnage, filoutage) ;
    - ingénierie sociale sur les réseaux sociaux ;
    - vol de données dans le Cloud ;
  - certaines sont plus probables que d'autres ;
- Le ou les événements déclencheurs ;
- Les facteurs internes aggravants (vulnérabilités, faiblesses) :
  - de même que pour les causes / menaces, certaines vulnérabilités sont très anciennes et assez bien maîtrisées :
    - absence de détection incendie ;
    - salle informatique en sous-sol près d'un lac ;
    - onduleur mal maintenu / télé maintenu ;
    - absence de procédures ;
  - d'autres apparaissent régulièrement, au fur et à mesure des évolutions technologiques, et ne sont pas maîtrisées :
    - chiffrement obsolète ;
    - absence de contrat avec le fournisseur d'informatique en nuage (cloud) ;
    - patchs de sécurité non mis à jour ;
  - certaines sont plus faciles à exploiter que d'autres ;
- la nature des conséquences (dommages, impacts) sur l'entreprise ou l'organisme public : certaines sont plus graves que d'autres ;
- les mesures déjà en place : elles peuvent être prises en compte, selon la méthode utilisée, pour évaluer la vraisemblance des scénarios ou en limiter les conséquences.

Estimation et évaluation des risques

C'est ensuite estimer un niveau de risque pour chaque risque identifié et analysé puis évaluer globalement l'acceptabilité, en l'état, de chaque risque.

Il y a plusieurs façons concrètes de réaliser une analyse de risques en sécurité des SI. Elles dérivent de méthodes industrielles plus anciennes (AMDEC, etc.). Des normes et des méthodes existent, pour faciliter et guider ces analyses. Depuis la norme ISO 27005 (2008), beaucoup de ces méthodes ont évolué et convergé. Elles n'ont pas toutes le même vocabulaire, ni les mêmes étapes détaillées, mais les mêmes grandes lignes s'y retrouvent toujours. Certaines sont descriptives, d'autres cherchent à quantifier (numériquement) les niveaux de risques pour ensuite mieux les comparer. Avant de choisir une méthode, il faut en comprendre le déroulement, les livrables, la valeur ajoutée.

3.2.5 Faut-il utiliser une méthode ?

Bien qu'il existe de nombreuses méthodes d'analyse de risques (EBIOS, MEHARI, etc.), l'entreprise peut très bien inventer sa propre méthode. Même la norme ISO 27001, qui rend obligatoire l'analyse de risques, n'impose aucune méthode en particulier. Alors pourquoi utiliser une méthode ? Si la norme ISO 27001 n'en impose pas une spécifique, elle fixe cependant un certain nombre de points incontournables que doit respecter un processus d'appréciation du risque. Nous en citerons trois :

- le processus d'analyse de risques doit définir les critères d'acceptation des risques. Chaque risque sera évalué et comparé à ce critère. Chaque risque dépassant ce critère ne sera pas accepté ;
- la répétitivité du processus (probablement l'un des points les plus importants qui motivent l'usage d'une méthode d'analyse de risques). Cela signifie qu'un réexamen des niveaux de risque doit produire des résultats comparables. Seule une méthode avec une démarche structurée permet de garantir ceci ;
- le processus doit permettre de déterminer le niveau de risque, en prenant en compte la vraisemblance d'apparition des risques et leurs conséquences potentielles. Cela revient à définir des métriques et une grille d'évaluation du risque.

L'analyse de risques est ainsi un processus à part entière, qui exige une démarche structurée, et dont les caractéristiques seront vues à la prochaine section. Adopter une méthode, c'est adopter une démarche structurée.

Enfin, utiliser une méthode d'analyse de risques, c'est bénéficier des bases de connaissances éventuellement fournies par la méthode telles que la liste des actifs types, des menaces génériques, des bases de scénarios types et des vulnérabilités.

4 L’analyse de risques en pratique

4.1 Avant de se lancer

« La gestion des risques est un processus dans lequel sont impliquées plusieurs directions de l'entreprise, parmi elles la DSI et la SSI (ou cybersécurité). »

Un des résultats majeurs de ce processus est de dresser une cartographie de tous les risques auxquels est exposée l'entreprise et quelle que soit la nature (ou catégories) de risques à considérer.

Ainsi, la première réflexion doit être :

- Quelle est la finalité du travail à mener pour que le résultat puisse s’intégrer à la gouvernance de l’entreprise ou des directions concernées (renforcer la sécurité d’une application ou d’un SI, définir des exigences de sécurité lors de la conception d’un projet, réaliser la cartographie des risques d’un métier ou respecter une obligation de conformité, être en mesure de prioriser les chantiers) ?
- Comment les résultats produits vont être appliqués et maintenus à jour tout au long de la vie de la cible de l’étude ?
- Existe-t-il un cadre de gouvernance des risques défini dans l'entreprise ? (Dans ce cas, y inscrire la gestion des cyberrisques s'ils n'en faisaient pas partie, sinon il faudra le définir.)

4.1.1 Les questions à se poser

Ainsi, il conviendra d’étudier les différents aspects suivants :

- Quel budget (coût humain et financier) pour l’analyse mais également pour le traitement des risques ?
- Le commanditaire de l’analyse est-il légitime pour impliquer les parties prenantes ? A-t-il un pouvoir suffisant pour décider des arbitrages dans la gestion des risques ?
- Le périmètre est-il cohérent ? N’est-on pas en train d’oublier un élément essentiel impactant la sécurité de la cible à étudier ?
- Prévoir l'éventuelle décomposition du périmètre en sous-périmètres.
- Prévoir les éventuelles itérations de la méthode.
- Choisir le niveau de granularité approprié de l’analyse.
- Choisir les activités pertinentes, la manière de les réaliser et les résultats à produire.
- Prévoir les éventuels ajustements de terminologie et des bases de connaissances.

4.1.2 L’organisation à mettre en œuvre

La conduite d’une analyse de risques peut nécessiter dans l’étude l’intervention de nombreuses parties prenantes de natures différentes.

Il faut distinguer :

- la maîtrise d’ouvrage, décisionnaire dans l’étude ;
- les professionnels de la gestion des risques maîtrisant la démarche et, le cas échéant, ayant connaissance des pratiques de l’organisme en matière de processus de gestion des risques ;
- les experts de la SSI ;
- les personnes ayant une bonne connaissance des aspects de l’écosystème relatant des menaces et des risques pesant sur la cible ;
- et de manière générale, toute personne capable d’apporter des informations impactant les risques, que ce soit sur la conception, l’utilisation ou le maintien en conditions opérationnelles de la cible de l’étude.

4.1.3 Analyse de risques et confidentialité

Les informations traitées dans le cadre de ce type d'étude sont généralement confidentielles. Elles doivent donc être accessibles, échangées, stockées et détruites de manière adaptée.

4.1.4 L'outillage

L'outillage n'est pas obligatoire, un simple tableau blanc peut suffire. Néanmoins, il devient nécessaire dans le cas d'études complexes et lorsque la maturité de l'organisme est suffisante pour assurer un maintien à jour fréquent. L'utilisation d'une méthode est fortement recommandée (voir section 2.2.5) et peut également s'appuyer, nécessiter l'utilisation d'un outil.

4.1.5 La démarche : « one shot », itération, etc.

Dans une grande majorité des méthodes d'analyse de risques (comme c'est le cas pour EBIOS RM et ISO 27005), une approche par approfondissements successifs est recommandée. Il est vrai qu'en pratique, force est de constater que ce type d'approche est rarement utilisé en raison du coût engendré et de la disponibilité des personnes.

La norme de référence, l'ISO 27005, préconise une approche itérative afin d'assurer *« un bon équilibre entre la minimisation du temps et des efforts investis dans l'identification des mesures de sécurité et l'assurance que les risques élevés sont correctement appréciés ».*

Cette même norme précise : *« Il est possible que le traitement du risque ne donne pas immédiatement un niveau acceptable de risque résiduel. Dans ce cas, une nouvelle itération de l'appréciation du risque utilisant, si nécessaire, de nouveaux paramètres de contexte (par exemple, l'appréciation du risque, l'acceptation du risque ou les critères d'impact) peut être requise et suivie d'un autre traitement du risque. »*

À cette raison, il faut en ajouter deux autres :

- au niveau de l'organisme, bien des paramètres peuvent changer les risques encourus, leurs conséquences (contexte stratégique, impacts économiques ou autres, activités critiques, etc.) ou leur vraisemblance (évolutions techniques ou d'architecture des SI, etc.) ;
- les menaces sont en évolution permanente, ne serait-ce que par l'évolution des technologies.

Globalement, une approche itérative est certainement recommandable, mais cela ne veut pas dire que toutes les itérations demanderont le même effort en termes d'implication des responsables ou du budget : des analyses plus ciblées pourront être réalisées, en fonction des besoins de réactualisation.

4.2 Comment convaincre ?

Convaincre la direction est une première étape essentielle au bon démarrage d'une démarche d'analyse de risques, non seulement pour obtenir les moyens financiers pour la réaliser, mais surtout pour avoir son appui auprès des personnes qui vont contribuer à l'analyse de risques tout au long du processus.

Il est donc évident que la façon dont est présenté aux directions le besoin d'une analyse de risques est un point important de la démarche. C'est avec la bonne présentation des objectifs à atteindre que le soutien de la direction est obtenu pour une analyse de risques.

Il semble alors que la situation la plus facile pour obtenir le soutien de la direction pour la démarche d'analyse de risques soit le cas où elle découle d'une obligation réglementaire. Toutefois, il ne faut pas se laisser entraîner par la facilité. Dans la plupart des cas, la réglementation apporte une rationalité qui, presque toujours, aide les entreprises à mieux effectuer leur travail. Il est intéressant d'essayer de comprendre cette rationalité et de

présenter la démarche d'analyse de risques à réaliser en incluant l'aspect obligation en parallèle de l'aspect avantages. En abordant la situation de cette façon, il est aussi possible de montrer qu'une extension de cette analyse au-delà du périmètre fixé par la norme, peut avoir un réel bénéfice pour l'entreprise.

Une bonne approche est d'avoir un premier aperçu des risques principaux de l'entreprise. Cela peut se faire en quelques entretiens avec certains postes clés, en particulier la MOA et la MOE. Il est important d'avoir non seulement une vision « objective » mais également d'identifier l'aspect d'aversion au risque c'est-à-dire ce qui, dans la culture de l'entreprise, est considéré comme inadmissible ou grave sans pour autant être objectivement établi. Les premiers aperçus du risque et de l'aversion aux risques seront des arguments essentiels pour convaincre la direction.

Un autre point, assez récent celui-ci, est que de plus un plus de cyberratings, c'est-à-dire des quantifications de tests externes réalisées à la demande d'une entreprise ou même à l'insu de celle-ci, sont publiés et peuvent avoir un impact sur l'image, voire sur la valorisation d'une entreprise. Il peut être utile, pour convaincre, de mentionner ce point.

Une autre méthode de valorisation de l'entreprise est l'obtention d'une certification ISO 27001 qui requiert aussi, comme préalable, une analyse de risques.

Enfin, un rappel des avantages induits pertinents pour l'organisme (voir 2.1.5) peut s'avérer utile.

4.3 Définition des rôles

Définir les rôles et les responsabilités de chaque utilisateur est un prérequis à toute analyse de risques. Plusieurs rôles peuvent être nécessaires pour la réussite de l'analyse de risques et ce, en fonction du contexte de l'organisation et de sa taille. La définition et l'attribution des rôles sont une étape essentielle avant le démarrage du projet.

- propriétaire de l'étude : sponsor de l'étude, il met à disposition les ressources nécessaires pour mener l'étude ;
- responsable de l'étude : il dirige la conduite de l'étude ;
- propriétaire des risques : il est propriétaire des actifs informationnels associés à l'étude, il a pour rôle d'accepter les risques résiduels et le plan de traitement. Il est en général l'utilisateur responsable de l'évaluation des impacts ;
- responsable de la sécurité de l'information : en tant que RSSI, il participe activement à l'étude et, dans de nombreux cas, il dirige l'analyse ;
- équipe technique : pour mener à bien l'étude, il est nécessaire de faire appel à des spécialistes, notamment pour évaluer les probabilités que les menaces se produisent ;
- consultant spécialisé : il conseille l'organisation, notamment avec son retour d'expérience.

Il convient de préparer les équipes en fonction des compétences et de la méthodologie retenue avec des formations et des opérations de sensibilisation.

Un modèle de type RACI (voir https://www.manager-go.com/gestion-de-projet/dossiers-methodes/matrice-raci) dans le cas d'une analyse de risques n'est pas nécessairement compliqué :

1) Le « A » est normalement le sponsor de la démarche qui doit avoir, de préférence, autorité sur l'ensemble du périmètre concerné.
2) Le « R » est la personne qui réalise ou dirige la réalisation de l'analyse de risques.
3) Les « C » sont prédéterminés nécessairement par une réunion de « R » avec le staff de « A » et sont complétés au fur et à mesure de l'avance des travaux. Mais, en principe, tous les propriétaires des actifs, aussi bien primordiaux que du support, doivent être consultés.
4) Enfin, les « I » sont, à des niveaux différents, l'ensemble des personnes du domaine.

4.4 Cadrage du projet

Identifier le besoin :

- Contexte :
  - contraintes légales, normatives, internes, etc. Une certification est-elle nécessaire ?
  - domaine d'application métier (finance, médical, etc.) : impact sur le choix du ou des référentiel(s) et de la méthode ;
  - métiers ou services de l'entreprise concernés ;
  - système existant ou démarche préalable à un développement/déploiement ;
  - périmètre :
    - périmètre opérationnel (restreint au strict nécessaire) ;
    - concerne un projet, un déploiement, un système d'information… : analyse ponctuelle (projet), analyse de risques à maintenir dans le cadre d'un processus.
- Organisation nécessaire :
  - ressources humaines disponibles :
    - décideurs qui valident les conclusions pour ensuite engager des moyens ;
    - identifier les parties prenantes : professionnels de l'analyse de risques, opérationnels (métier et support : SI, services généraux : administratif, RH, locaux…), propriétaires d'actifs… Sont-elles sensibilisées ? Faut-il le faire ? Sont-elles disponibles ? Motivées ?
  - cartographie des données, flux, etc. : est-elle disponible, accessible ?
  - communication interne/externe, préalable, en cours de réalisation, à faire par la suite ?
- Évaluer la maturité de l'organisation, des intervenants.
- Un accompagnement est-il nécessaire ?
- Faut-il former les parties prenantes ?
- Commencer par un « préprojet » : par exemple identifier les actifs avant de lancer la démarche complète (permet de mesurer l'effort nécessaire, d'impliquer les parties prenantes, de motiver les décideurs qui ont généralement une conscience intuitive de la valeur des actifs).

La maîtrise d'un système de management est utile : réflexes documentaires, traçabilité, estimation du coût, etc.

4.5 Les caractéristiques des méthodes d'analyse de risques

Cette partie du document se concentre sur les caractéristiques essentielles des méthodes d'analyse de risques, en analysant les manières dont elles contribuent à :

- identifier les risques ;
- apprécier leur gravité au travers des conséquences qu'elles induisent ;
- apprécier leur vraisemblance (ou leur probabilité) ;
- évaluer globalement le niveau de chaque risque ;
- traiter les risques ;
- proposer ou non des solutions ou des pistes d'action pour réduire les risques, si nécessaire ;
- produire un plan d'action ou un plan de traitement des risques.

4.5.1 L'identification des risques

Les méthodes se différencient, sur ce point, par :

- La manière dont elles définissent ou limitent leur périmètre d'action :
  - périmètre ouvert aux risques liés à tout type d'information : numérique o,u non, quel que soit son support ;
  - périmètre limité aux données des systèmes informatisés ou non ;
  - périmètre limité aux vulnérabilités des systèmes d'information et de communication (IT) ou non ;
  - périmètre excluant ou non les risques couverts par les mesures de sécurité habituelles (supposant acquises les « mesures d'hygiène ») ;
  - l'arborescence utilisée et la démarche suivie pour définir les divers éléments de chaque risque :
    - démarche déductive partant des métiers de l'organisme, pour remonter aux contingences (biens, services et informations), puis aux événements redoutés, aux menaces pour définir des « scénarios de risque » ;
    - démarche partant des menaces pour définir les cibles potentielles et aboutir aux scénarios de risque ;
    - autre démarche.
- L'utilisation ou non de bases de connaissances :
  - démarche cadrée par l'utilisation de bases de connaissances conduisant à une liste de scénarios de risque imposée et prédéfinie ;
  - démarche guidée par l'utilisation de bases de connaissances « ouvertes » conduisant à une liste spécifique de scénarios ;
  - démarche libre non guidée par des bases de connaissances.

4.5.2 L'appréciation de la gravité liée aux conséquences de la réalisation des risques

Les méthodes se différencient, sur ce point, par :

- la grille de définition des niveaux de conséquence :
  - nombre de niveaux,
  - précision de la définition de ce que recouvre chaque niveau ;
- le critère de jugement d'un niveau de conséquence : évaluation du niveau maximal des conséquences possibles (ce qui peut arriver de pire) ;
- évaluation de la probabilité des conséquences (ce qui arrivera le plus souvent) ;
- la manière de prendre en compte, dans cette appréciation, les mesures de sécurité pouvant limiter les conséquences :
  - évaluation différenciée des conséquences « intrinsèques » (hors toute mesure de sécurité) et de l'effet des mesures de sécurité pour limiter les conséquences ;
  - évaluation globale du niveau de conséquences compte tenu des mesures de sécurité déjà en place.

4.5.3 L'appréciation de la vraisemblance (ou probabilité) des risques

Les méthodes se différencient sur ce point par :

- La grille de définition des niveaux de probabilité :
  - nombre de niveaux,
  - précision de la définition de ce que recouvre chaque niveau.

- La manière de prendre en compte, dans cette appréciation, les mesures de sécurité pouvant limiter les probabilités d'occurrence :
  - évaluation différenciée des vraisemblances « intrinsèques » (hors toute mesure de sécurité) et de l'effet des mesures de sécurité pour limiter les vraisemblances ;
  - évaluation globale du niveau de vraisemblance compte tenu des mesures de sécurité déjà en place.
- L'existence ou non d'une base de connaissances de menaces types assorties de vraisemblances standards.

4.5.4 L'appréciation globale du niveau de risque

Les méthodes se différencient, sur ce point, par :

- La grille de définition des niveaux de risque :
  - nombre de niveaux,
  - précision de la définition de ce que recouvre chaque niveau.
- La manière d'apprécier ce niveau en fonction des niveaux de conséquence et de vraisemblance :
  - formule mathématique,
  - grille préétablie (éventuellement modifiable),
  - évaluation libre.

4.5.5 Le traitement des risques

Le traitement des risques consiste à retenir une option pour la gestion du risque.

La norme ISO27005 : 2018 prévoit quatre options de traitement :

Traitement	Actions en découlant
Réduction du risque	Ajout, suppression ou modification de mesures de sécurité nécessaires pour que le risque résiduel soit acceptable après la mise en œuvre des mesures.
Maintien du risque (ou acceptation)	Maintien du risque sans aucune autre action.
Refus du risque (ou évitement)	Suppression de la source du risque.
Partage du risque	Partage du risque (ou transfert) avec (vers) une autre partie prenante capable de gérer de manière plus efficace le risque.

Le choix de l'option dépendra du seuil d'acceptabilité du risque au-delà duquel le risque devra être traité. La direction peut prendre la décision, au vu des informations liées au risque, d'accepter un risque ou de le prendre en tenant compte soit de la faible gravité de ce dernier soit de sa faible probabilité d'occurrence. Il est important dans ce cas de bien mesurer les conséquences de ce choix et de l'assumer. Généralement, le ratio bénéfice / coût est dans ce cas analysé pour valider ce choix.

L'étape de traitement des risques est essentielle et doit être approuvée par la direction ou par un propriétaire du risque.

4.5.6 Les propositions de plans d'action ou de réduction des risques

Cette partie, qui n'est proposée que par quelques méthodes, peut être caractérisée par :

- L'existence, ou non, d'un « modèle » de risque faisant apparaître :
  - des types d'effets des mesures de sécurité ;
  - la manière dont ces effets peuvent se compléter et se cumuler ;
  - la manière dont ces effets agissent sur les niveaux de conséquence et de vraisemblance.
- L'existence ou non d'une base de connaissances de « services de sécurité », comprenant, ou non :
  - une typologie et une liste de services de sécurité ;
  - une description desdits services ;
  - une méthode d'évaluation de la qualité (efficacité) desdits services ;
  - des questionnaires d'évaluation de leur efficacité (et d'autres caractéristiques éventuellement).
- L'existence ou non d'une méthodologie et de processus pour :
  - sélectionner les mesures (ou services de sécurité) adéquates pour réduire les risques et les ramener à un niveau acceptable ;
  - simuler l'effet de la mise en place de ces mesures sur les niveaux de risque.
- L'existence ou non d'outils de pilotage des risques.

4.6 Prise de décision sur l'acceptation du risque

Le traitement des risques a été abordé en §3.5.5.

Il faut revenir sur un point, indépendant des méthodes, quand la décision est l'acceptation du risque.

Il importe, pour les cas d'acceptation ou de maintien :

- d'établir qui a le droit d'accorder une exception et d'accepter un risque – tout le monde n'est pas autorisé ;
- de documenter clairement la décision et ses attendus (pour éviter que les responsables de l'acceptation, si jamais le risque se réalise, puissent argumenter qu'ils n'étaient pas conscients des conséquences) ;
- de documenter les conditions éventuelles ayant conduit à l'acceptation (en attendant un événement, pour une durée de temps déterminée, contre une action, etc.) ;
- d'effectuer un suivi régulier des risques ayant été acceptés : ce qui est vrai aujourd'hui ne le sera pas forcément demain.

4.7 Des erreurs à éviter

Les erreurs les plus rencontrées et décrites plus amplement dans le document du Clusif « Analyse de risques SSI et loi de Murphy – tout ce qui peut bien … ou mal tourner » sont résumées ci-dessous :

- ne pas identifier l'attendu précis de l'analyse de risques : une analyse de risques n'est pas faite seulement pour se donner bonne conscience ;
- ne pas avoir de sponsor rattaché à la direction : il est indispensable pour donner l'impulsion et apporter sa connaissance des enjeux de l'entreprise ;
- ne pas donner au sponsor un rôle de médiateur : les résultats produits par les analyses de risques peuvent conduire à révéler des manquements internes plus ou moins graves et générer des règlements de compte. Dans de tels cas, le sponsor peut être essentiel pour arbitrer et traduire la volonté de la direction ;

- ne pas disposer de praticien de la méthode choisie : il est nécessaire de disposer dans l'équipe projet d'au moins une personne qui connait la méthode et a déjà réalisé des analyses de risques, afin de guider les autres intervenants ;
- ne pas avoir considéré, avant de lancer une analyse de risques, la volumétrie des biens ni s'être posé la question de la granularité de l'étude : pour éviter l'apocalypse, l'analyse de risques ne doit pas se dérouler sur plus de quelques mois, ni aboutir à l'identification de plus d'une centaine de risques ;
- ne pas analyser en détail le périmètre qui formera la base de l'analyse de risques, afin de bien doser les efforts et les investissements : un périmètre excessif ou non critique peut entraîner de gros surcoûts ;
- opter pour une méthode ou une granularité extrêmement complexe ou inversement pour une simplification excessive ;
- ne pas prévoir une étape de cadrage visant à s'assurer de la cohérence entre le fonctionnel et l'opérationnel ;
- écarter trop rapidement les menaces dont la probabilité semble très faible ;
- négliger la communication : si les sujets évoqués portent des germes de discorde (la sécurité du réseau, des salles informatiques, etc.), l'importance de la communication est encore plus grande pour dépasser les conflits et les non-dits ;
- ne pas maîtriser les techniques de questionnement : il importe de recueillir les « vraies » réponses ;
- confondre analyse de risques et audit : aucun jugement de conformité ne doit être émis. Il faut bien expliquer la finalité de l'analyse de risques aux personnes qui seront interviewées et à celles qui recevront les conclusions ;
- ne pas protéger les résultats des analyses de risques, qui sont très confidentiels : leur divulgation permettrait d'attaquer l'entreprise avec une grande facilité.

Tour Eria
5, rue Bellini
92821 Puteaux cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr