IRM | institut du risk management

Rapport de projet présenté devant un Jury de Soutenance

Expert ERM

Expert(e) Management des Risques Financiers et Assurantiels

Le 28/10/2022

Par : Ounaïzat DUBOISSET

Titre : **Favoriser la cyber résilience d'une entreprise d'assurance par l'ERM**

Confidentialité : ☒ NON ☐ OUI (Durée : ☐ 1an ☐ 2 ans)

La durée de confidentialité expire aux 31 décembre N+1 (1 an) ou N+2 (2 ans)

Les stagiaires s'engagent à ce que les données de l'Entreprise présentées dans le cadre des travaux de la formation (rapport de projet & présentation) respectent les règles relatives à la protection des données à caractère personnel conformément aux dispositions de la Loi informatiques et Liberté n°78-17 du 6 janvier 1978 modifiée par la Loi du 6 août 2004 ainsi que par la loi n° 2018-493 du 20 juin 2018 (RGPD)

Membres présents du jury :

_____

_____

_____

_

_____

_____

Par ma signature j'autorise la publication sur un site de diffusion de documents actuariels du rapport de projet
(après expiration de l'éventuel délai de confidentialité)

Nom : DUBOISSET

Prénom : Ounaïzat

Signature du stagiaire 

Si binôme :

Nom :

Prénom :

Signature du stagiaire

Favoriser la cyber résilience d'une entreprise d'assurance par l'implémentation d'une démarche ERM

Ounaïzat DUBOISSET
Formation ERM - Session 2022

Sommaire

Introduction

Face à l'accroissement constant des menaces qui visent nos outils informatiques et dans un contexte où le télétravail et l'usage des nouvelles technologies se développent à un rythme sans précédent, il ne faut plus envisager seulement le risque cyber mais bien penser en termes de cyber résilience*[1].

De nos jours, les entreprises considèrent qu'elles sont armées et préparées contre les cyberattaques, parce qu'elles ont mis en place un dispositif de « cybersécurité*» qui repose sur un ensemble de moyens humains, organisationnels et techniques visant à protéger leur système d'information contre toute attaque.

Force est de constater que cela ne suffit pas, et la menace subsistera tant que les cyber criminels continueront de s'adapter plus rapidement aux changements que les solutions de sécurité qui sont sur le marché.

Une étude menée par le *World Economic Forum* sur *« l'État de la cybersécurité en 2022[2] »* a par ailleurs révélé que le ransomware* est l'attaque la plus redoutée par les entreprises. En outre, le secteur de l'assurance et de la finance constituerait le 8ème secteur le plus exposé en Europe et dans le monde, selon le baromètre du ransomware *« Anozr Way »*[3],

Ces entreprises sont des cibles stratégiques car :
- elles manipulent des données sensibles et volumineuses,
- elles sont hautement solvables, par conséquent plus à même de payer les rançons,
- les informations dont elles disposent permettent aux cybercriminels de propager leurs attaques.

En France, plusieurs acteurs du monde de l'assurance ont déjà été victimes de cyberattaques (MMA, MNH, Verlingue, Assureone en 2021, et plus récemment le groupe B2V).

Face à ce constat, les organismes prennent conscience de l'urgence de planifier une stratégie de **cyber résilience** afin de limiter les impacts financiers, opérationnels, réglementaires et d'image sur leurs activités. Une vision partagée par l'ACPR qui incite déjà fortement les assureurs à renforcer leur dispositif de sécurité[4].

Le principal enjeu de la cyber résilience réside dans la capacité d'une entreprise à survivre dans un environnement ou les cyber menaces semblent inévitables. C'est une stratégie qui va au-delà de la cybersécurité qui, bien que nécessaire, repose sur une logique assez passive de détection-réponse. A l'inverse la cyber résilience constitue une approche proactive qui contribue ainsi à créer de la valeur.

Le présent mémoire a pour objet la problématique suivante :

Comment mettre en œuvre une démarche ERM dans la gestion du risque informatique d'une entreprise d'assurance, afin de favoriser sa cyber résilience ?

[1] Les termes suivis d'un « * » sont définis ou développés dans le glossaire en fin de mémoire

[2] https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[3] Baromètre Anozr Way du ransomware, Edition du 8 septembre 2022

[4] notice publiée en juillet 2021 par l'ACPR, concernant la mise en œuvre des orientations de l'AEAPP en matière de sécurité et de gouvernance des Technologies de l'Information et de la Communication par les organismes d'assurance relavant du régime Solvabilité 2. (EIOPA-BoS-20/600). Version du 18/06/2021

1. Périmètre de l'étude

1.1 Présentation de l'entreprise RUNEO et de sa stratégie de digitalisation

Considérons une mutuelle santé et prévoyance fictive, nommée « RUNEO ». Le cas de cette entreprise est inspiré d'une situation réelle, avec certains éléments de contexte fictifs.

Chiffres clés RUNEO 2021

Nb de personnes protégés	900 000		
Chiffre d'affaire	530 M€	Fonds propres	490 M€
Résultat net	30 M€	Total Bilan	1 020 M€
Provisions techniques S1	190 M€	Ratio de couverture	233%

Forte de sa présence et de sa renommée à l'échelle nationale, RUNEO a mis tout en œuvre au cours de ces 2 dernières années pour développer son réseau informatique et digital. L'objectif est de rester compétitive, maintenir une qualité de service optimale et favoriser la proximité avec ses adhérents.

Elle a pour cela revu l'ensemble de son *business model* en 2021 (offre, distribution et services) en optant pour une stratégie de digitalisation et de numérisation à horizon 3 ans. Celle-ci consiste à développer une plateforme en ligne unique afin :

- d'aider les adhérents dans la réalisation de leurs opérations courantes (déclaration de sinistres, gestion de leur dossier et des réclamations) ;
- de conquérir de nouvelles parts de marché (devis et souscription en ligne, assistant virtuel et contrats avec des courtiers digitaux) ;
- d'adopter une démarche éco-responsable dans le cadre de sa politique RSE (zéro papier, signature électronique des contrats et mise en place d'une GED[5] pour la conservation des pièces justificatives).

Pour mener à bien ce projet, RUNEO a engagé une transformation importante de ses outils informatiques internes (nouvelles interfaces automatisées, dématérialisation des dossiers…) et a migré ses applicatifs métiers vers un service de *Cloud Computing*[6] géré par un prestataire externe. Une transformation qui porte d'ores et déjà ses fruits, puisque RUNEO a vu son résultat net augmenter de près de 5% dès la 1ère année de transition.

En ce qui concerne l'organisation du réseau informatique du Groupe, il est entièrement piloté par la Direction Informatique qui assure également la sécurité des Systèmes d'Information.

1.2 Un projet ambitieux qui rend vulnérable son Système d'Information

En raison de l'impact de ce plan de transformation sur le Système d'Information (SI) de RUNEO, la Direction Générale a demandé en janvier 2022 à sa Direction des Risques **(dont je suis la Responsable)** et au RSSI[7] de **dresser un état des lieux du niveau de maturité du dispositif de sécurité actuel**.

Elle souhaiterait par ailleurs que l'on puisse anticiper et se préparer à tous les scénarios possibles, notamment en cas d'attaque avérée, de manière à limiter le risque opérationnel et les pertes financières que celle-ci pourrait occasionner.

[5] Logiciel de Gestion Électronique des Documents

[6] Le Cloud Computing ou « l'infonuagique » est une prestation de service informatique qui permet à l'entreprise et à ses clients d'accéder via internet à des ressources informatiques, de stockage et de réseau hébergées dans un ou plusieurs centre de données externes. Selon les besoins de l'entreprise il existe différents types de modèles de services.

[7] Responsable de la Sécurité des Systèmes d'Information

2. Démarche ERM

2.1 Système de gouvernance et de maitrise des risques au sein de RUNEO

La gouvernance de RUNEO est fondée sur la complémentarité entre les membres du Conseil d'Administration (CA), le Directeur Générale et les responsables des fonctions clés (Vérification de la conformité, Actuariat, Gestion des risques et Audit interne). Leur rôle est de garantir une gestion saine, prudente et efficace des activités de l'entreprise en accord avec la stratégie qui a été définie et en tenant compte de l'univers de risque de RUNEO (décrit en annexe 1).

L'intégration de la dimension risque dans le pilotage de l'entreprise est donc favorisé par la mise en œuvre d'un système de gouvernance et de maitrise des risques. Conçu pour identifier les événements susceptibles d'affecter l'organisation et pour gérer les risques dans la limite de son appétence, ce système implique aussi bien les dirigeants que l'ensemble des collaborateurs de RUNEO. **Il couvre en priorité les 6 domaines[8] de risque prévus par l'article 44 de la directive Solvabilité 2, dont le risque informatique (y compris cyber) ancré dans la famille du « risque opérationnel ».**

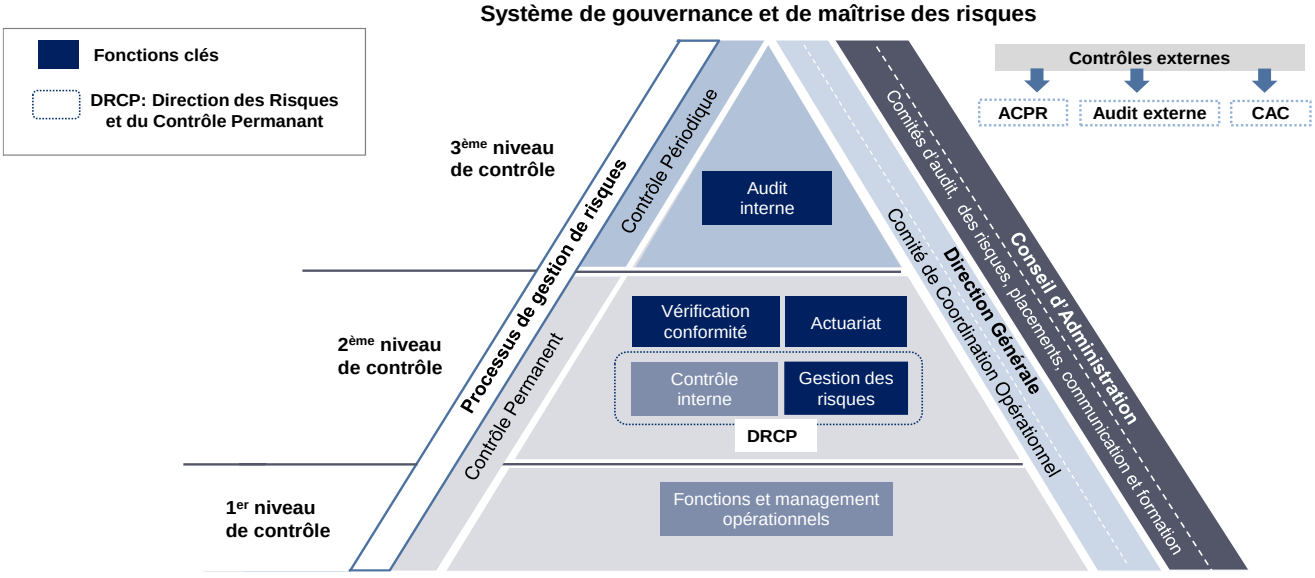
Globalement, ce dispositif est structuré autour de 3 niveaux de contrôle, sous la responsabilité des instances dirigeantes citées précédemment (cf. schéma ci-dessous et § suivants).

Pour faciliter la transmission d'information (ascendante/descendante) et la prise de décision, 6 comités spécialisés ont été mis en place au sein de cette organisation :

- Les comités d'audit, des risques, des placements, de la communication et de formation qui dépendent directement du CA
- Le comité de coordination opérationnel (CCO) qui, animé par les responsables métiers, relève du Directeur Générale

D'un point de vue opérationnel, ce système comprend **un processus de gestion des risques** que nous présenterons en partie 2.2 de ce mémoire. Celui-ci est complété par des politiques écrites (dont une Politique de Sécurité des SI), des procédures d'alertes et de limites, l'ORSA ainsi que des modèles de calcul et des reporting.

Système de gouvernance et de maîtrise des risques



[8] La souscription et le provisionnement, la gestion actif-passif, les investissements, en particulier dans les instruments financiers à terme, la gestion du risque de liquidité et de concentration, la gestion du risque opérationnel ainsi que la réassurance et les autres techniques d'atténuation du risque.

- **1er niveau de contrôle :** concerne toutes les activités de RUNEO. À ce stade, les collaborateurs et les managers réalisent des contrôles permanents afin de mieux maîtriser les risques opérationnels et techniques générés sur leur périmètre. Ceux-ci sont suivis par la Direction Générale en CCO.

  Concernant le risque informatique (IT), la DSI constituée de 6 personnes, veille au maintien du dispositif de sécurité en place et s'assure que la PSSI soit respectée et déployée sur l'ensemble des activités.

❖ **Une PSSI partiellement appliquée**

⇒ *Sa mise en œuvre n'est pas effective. On constate par exemple que la revue annuelle des habilitations n'est pas toujours effectuée, ou que les accès logiques ne sont pas contrôlés*

⇒ *En outre, la DSI et actuellement mobilisée sur le projet de digitalisation ce qui entraine une hausse de incidents non traités et une diminution des contrôles*

- **2ème niveau de contrôle** : est constitué des fonctions clés « vérification de la conformité », « actuariat » et « Gestion des risques », cette dernière formant une seule et même Direction avec le Contrôle interne (Direction des Risques et du Contrôle permanent : DRCP).

  La DRCP a pour mission principale de recenser, évaluer et mesurer tous les risques de l'entreprise et notamment les risques informatiques. Elle a également la charge de contrôler la bonne réalisation des contrôles de 1er niveau.

  Les sujets relatifs à la sécurité des SI sont présentés périodiquement en Comité des Risques (CMDR) constitué de 3 administrateurs, des Directeurs des fonctions clés, du Directeur Général et du Directeur de la Sécurité Informatique. La Direction de la Conformité joue par ailleurs un rôle important dans la veille et le contrôle du respect des dispositions réglementaires en matière de sécurité de l'information et de la protection des données.

- **3ème niveau de Contrôle :** est exercé par la fonction clé Audit Interne dont le rôle est de réaliser des contrôle périodiques afin de fournir aux instances dirigeantes une assurance et des recommandations relatives à la bonne gestion du contrôle interne et des risques de l'entreprise.

  Elle est rattachée directement à la Direction Générale et présente ses travaux au Comité d'Audit qui se réunit trimestriellement. Celui-ci comprend 2 administrateurs, le Directeur Général et le Directeur des Risques.

  Conformément à ses prérogatives, l'Audit interne **doit s'assurer que le dispositif de Sécurité des SI est efficace** en réalisant ponctuellement des audits de sécurité.

❖ **Un contrôle encore lacunaire**

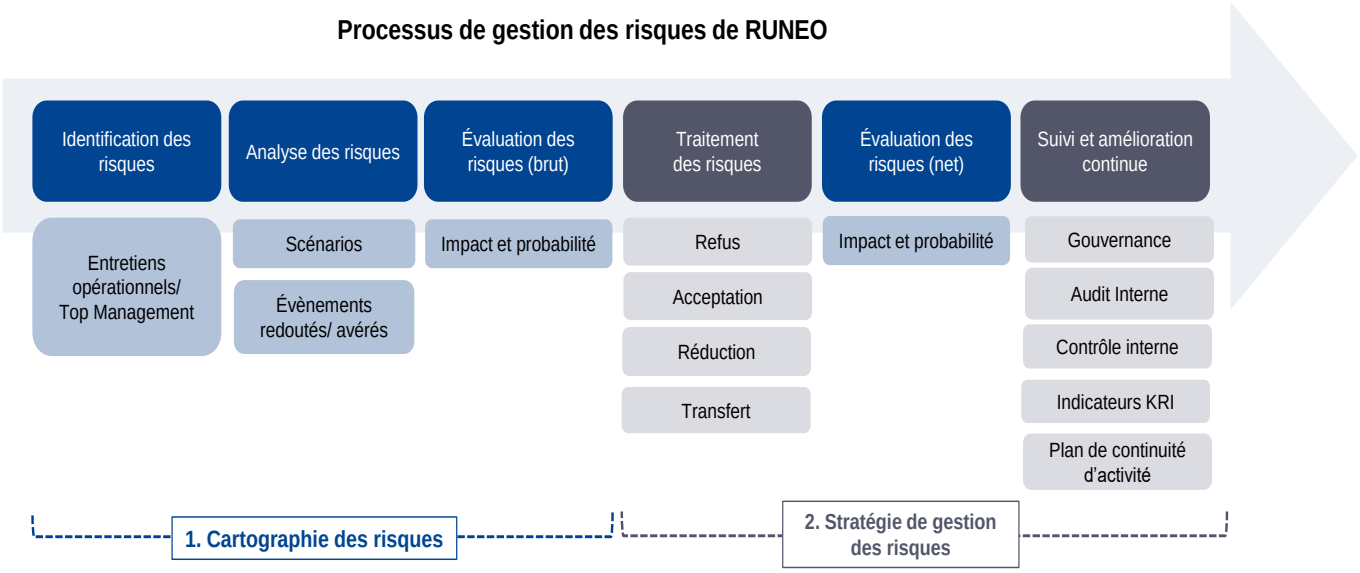
⇒ *Aucune mission d'audit de sécurité des SI n'a été menée depuis 2019*

2.2 Piloter l'entreprise par le risque IT : domaine d'application et enjeux

❖ **Domaine d'application**

Le processus mis en place au sein de RUNEO permet l'identification, l'évaluation, la surveillance la gestion et le reporting de **l'ensemble de ses risques**. Établit selon la norme ISO 31000 : 2018 (figure 3 de l'annexe 2), ce processus repose sur 2 éléments principaux :

- une cartographie des risques globale mise à jour une fois par an et donnant une vision consolidée et hiérarchisée du profil de risque de RUNEO.
- une stratégie de gestion des risques qui a été validée par le Conseil d'Administration



❖ **Enjeux**

Dans la cartographie des risques actuelle de RUNEO, le risque informatique et cyber se résume à **un seul facteur de risque**. Il est traité de manière générique, sur la base d'un scénario unique décrivant « une intrusion du SI suite à une faille de sécurité ».

⇒ Cette vision ne nous permet pas d'évaluer de manière exhaustive notre exposition au risque (étant donné que tous les facteurs de risques ne sont pas pris en compte) et de mettre en place une stratégie de gestion des risques adaptée.

2.3 Approche proposée

Notre mission consiste à donner à la l'organe d'administration et de gouvernance une vision complète et éclairée de notre exposition au risque.

❖ **Recommandation principale**

1. *réaliser une cartographie spécifique aux risques informatiques, qui sera combinée à celle déjà existante*
2. *compléter la stratégie de gestion de ce risque, par des indicateurs de suivi et des recommandations, dans une perspective d'amélioration continue et de résilience.*

2.3.1 Cartographie des risques informatiques de RUNEO

2.3.1.1 Identification des risques

Afin d'identifier les principaux facteurs de risques informatiques de RUNEO, nous avons mené différents entretiens auprès :

- des équipes opérationnelles de la DSI, de la Direction Commerciale, de la Direction Technique et Actuarielle, de la Direction Juridique et de la Direction des Ressources Humaines
- du top management (Directeurs des fonctions clé et Directeur général).

Les facteurs de risques que nous avons retenus[9] sont détaillés dans le tableau suivant. Chacun de ces risques est défini en annexe 3 de ce mémoire.

Facteurs de risque de RUNEO

Famille de risque	Typologie de risque	Code Risque	Risque
RISQUES OPERATIONNELS	Risque de fraude interne	R_OP1	Activité non autorisée
		R_OP2	Vol de données a des fins de divulgation, d'extorsion et/ou de détournement de fonds
		R_OP3	Fausses déclarations/collusion
		R_OP4	Usurpation de compte ou d'identité par un employé
		R_OP5	Déstruction maveillante des biens ou des systèmes
	Risque de fraude externe	R_OP6	Vol de données a des fins de divulgation, d'extorsion et/ou de détournement de fonds
		R_OP7	Ransomware et/ou cryptage des données
		R_OP8	Usurpation de compte ou d'identité par un tiers
		R_OP9	Fraude au président
		R_OP10	Faux et usage de faux
	Clients/tiers, produits et pratiques commerciales	R_OP11	Risque de sous-traitance
		R_OP12	Divulgation intentionnelle d'informations confidentielles
		R_OP13	Non-respect de la réglementation en matière de pratiques commerciales
		R_OP14	Mauvaise qualité des données
		R_OP15	Erreur de manipulation ou de paramétrage d'un modèle/système
		R_OP16	Défaut de preuve (archivage, traçabilité) / piste d'audit (qualité des données)
		R_OP17	Erreur/retard de paiement à un prestataire
		R_OP18	Erreur/retard de paiement des sinistres
	Risque informatique	R_OP19	Risque d'intrustion du système / cyber attaque
		R_OP20	Panne ou indisponibilité passagère de ressources informatiques internes
		R_OP21	Panne ou indisponibilité passagère de ressources informatiques externes
		R_OP22	Risque propagation d'une attaque
		R_OP23	Perte ou altération irrémédiable de données informatiques
		R_OP24	Retard/absence de traitement des incidents informatiques
		R_OP25	Rationalisation insuffisante du SI
		R_OP26	Maitrise insuffisante de l'externalisation
		R_OP27	Mauvaise gestion du nomadisme
RISQUES STRATEGIQUES ET ENVIRONNEMENTAUX	Législatifs, réglementaires et judiciaires	R_SE1	Non-respect des lois et règlements
	Organisationnel	R_SE2	Pilotage budgétaire défaillant
		R_SE3	Retard dans les délais de mise en production des nouveaux logiciels
	Risques environnentaux	R_SE4	Inaccessibilité des locaux ou des actifs informatiques
	Risque stratégique	R_SE5	Mauvaise gestion des changements (projets, évolutions, corrections)

[9] Source complémentaire : « Document de réflexion sur le risque informatique », ACPR, https://acpr.banque-france.fr/document-de-reflexion-sur-le-risque-informatique-version-finale

2.3.1.2 Évaluation et priorisation des risques bruts

❖ **Méthode d'évaluation des risques**

Chaque risque a été évalué à partir de l'échelle d'impact et de probabilité de RUNEO ci-dessous.

ECHELLE DE PROBABILITE				
Cotation	Peu probable (1)	Probable (2)	Très probable (3)	Certain (4)
Occurance	Une fois tous les 10 ans	Une fois tous les 3 à 5 ans	Une à 2 fois par an	Plusieurs fois par an

ECHELLE D'IMPACT				
Impact/Cotation	Faible (1)	Significatif (2)	Importante (3)	Critique (4)
Financier	Inférieur à 0,1% du Chiffre d'affaire	Entre 0,1% et 0,5% du CA	Entre 0,5% et 1% du CA	>1% du CA
Opérationnel	Interruption durable du service = 1 jour ouvré	Interruption durable du service <5 jours ouvrés	Interruption durable du service >=5 jours ouvrés	Interruption durable du service >15 jours ouvrés
Image	Visible uniquement en interne Réglementaire mineur	Dégradation de l'image auprès de peu de clients/fournisseurs	Mention dans la presse spécialisée et/ou nationale	Publication d'une condamnation (journaux nationaux/site internet)
Réglementaire	Avertissement/Mise en demeure	Amende	Amende et condamnation	Retrait d'agréement/droit d'exercer
Stratégique	Atteinte >95% des objectifs majeurs du plan stratégique	Atteinte entre 80% et 95% des objectifs majeurs du plan stratégique	Atteinte entre 40% et 80% des objectifs majeurs du plan stratégique	Atteinte <40% des objectifs majeurs du plan stratégique

Selon la nature du risque, cette évaluation peut être quantitative et/ou qualitative :

Approche qualitative

S'agissant d'une étude de cas fictif, cette approche repose sur 3 sources d'évaluations complémentaires (toutes choses égales par ailleurs) :

- **une évaluation « à dire d'expert »** suites aux entretiens que j'ai mené
  - en interne au sein de mon entreprise actuelle (5 personnes ont été interrogées dont 2 de la DSI, une de l'actuariat, le RSSI et le Directeur des Risques)
  - en externe (4 personnes ont été interrogées dont le Directeur générale d'une entreprise de cybersécurité et 3 personnes travaillant en assurance dans la gestion des risques).

- **ma vision du risque**, ayant moi-même vécu une cyber attaque en 2021 au sein de la mutuelle ou j'étais en charge de la gestion des risques groupe

- **le guide des bonnes pratiques définit par la norme ISO 27002** en matière de sécurité des SI.

Approche quantitative

Pour les risques concernés l'impact est principalement financier. La méthode d'évaluation appliquée consiste à formaliser le risque par un scénario concret et ensuite à mesurer l'impact sur le chiffre d'affaires de l'entreprise.

Pour rappel le chiffre d'affaires 2021 de RUNEO s'élève 530 M€ avec un total de 900 000 membres participants.

L'exemple que nous décrivons en page suivante permets de donner une vision éclairée de cette étape.

Exemple d'évaluation quantitative du risque [R_OP7] : Ransomware et/ou cryptage des données.

Le scénario envisagé est « l'intrusion du SI par un hacker en raison d'une vulnérabilité de sécurité et le cryptage des données contre paiement d'une rançon ». Le périmètre retenu concerne les données de sinistres et des prestations.

- **Probabilité d'occurrence :** « Très probable » (estimée à 2 à 4 fois par an par la DSI)
- **Nature de l'impact :** Financier, image, opérationnel, juridique et réglementaire

Mesure de l'impact financier

	En M€	Hypothèses retenues
1. Coûts de détection et de correction	0,5M€	Inclut l'engagement d'experts externes, l'enquête technique et la sécurisation des données
2. Coûts de notification de l'intrusion	5% x 900 000 x 7€ = 0,315	Concernent la notification des clients qui ne possèdent pas d'adresse email (5%). Coût estimé à 7€/client
3. Coûts de perte d'attractivité	2,215 M€	Détail ci-dessous
**dont Perte de marge technique (résiliations clients)*	*530 M€ x 1% x 30% =1,590*	*Perte de 1% du chiffre d'affaire diminuée de la charge sinistre associée (estimée à 70% de ces 1%), l'entreprise conservant ses frais généraux, en raison de la publicité négative.*
**dont perte d'affaires nouvelles*	*Affaires Nouvelles annuelle = 25 M€ soit (6,25 M€ par trimestre)* *(6,25 x 20% + 6,25 x 5%+ 6,25 x 1%) x 30% = 0,488 M€*	*Perte d'affaires nouvelles de :* *- 20% sur le 1er trimestre qui suit l'incident* *- 5% des affaires nouvelles sur le 2ème trimestre suivant l'incident* *- 1% des affaires nouvelles sur le 3ème trimestre suivant l'incident* *Le total est pondéré à 30% compte tenu des sinistres (70%) non réglés sur ces contrats non souscrits*
** dont Coût de l'indisponibilité des sytèmes durant 48H*	*25 M€/365 x 2 = 0,137M€*	*Perte de 2 jours de production nouvelle*
4. Coût des relations publiques	0,150 M€	16% du budget de communication (estimé à 1 M€)
5. Coûts de remédiation	0,5 M€	Coût du renforcement a posteriori du dispositif de sécurité. 25% du budget informatique (estimé à 2 M€)
6.Honoraires d'avocats, frais de justice et sanctions réglementaires	0,5 M€	Détail ci-dessous
** dont amende CNIL/RGPD de 2% du chiffre d'affaire*	*0 M€*	*Scénario non envisagé étant donné que RUNEO a mis en place toutes les dispositions requises pour être conforme à RGPD*
**dont coûts lié aux actions juridiques des clients en cas de fuite de leur données*	*0,5 M€*	*Hypothèse forfaitaire*
Coût et évaluation du risque Brut	**4,180 M€**	**Risque Important**

❖ **Point d'attention sur les hypothèses retenues**

Ces hypothèses ont été définies par rapport aux échanges que j'ai pu avoir avec la Direction technique, les experts en cybersécurité et mon retour d'expérience sur l'attaque que j'ai vécu en 2021.

Certaines d'entre elles :

- ⇒ *dépendent de la taille de l'entreprise et des moyens dont elle dispose*
- ⇒ *n'intègrent pas tous les coûts « indirects » (tels que la perte de confiance des fournisseurs/partenaires ou encore la dépréciation de la valeur de l'entreprise). Ceux-ci pouvant être difficilement quantifiables.*

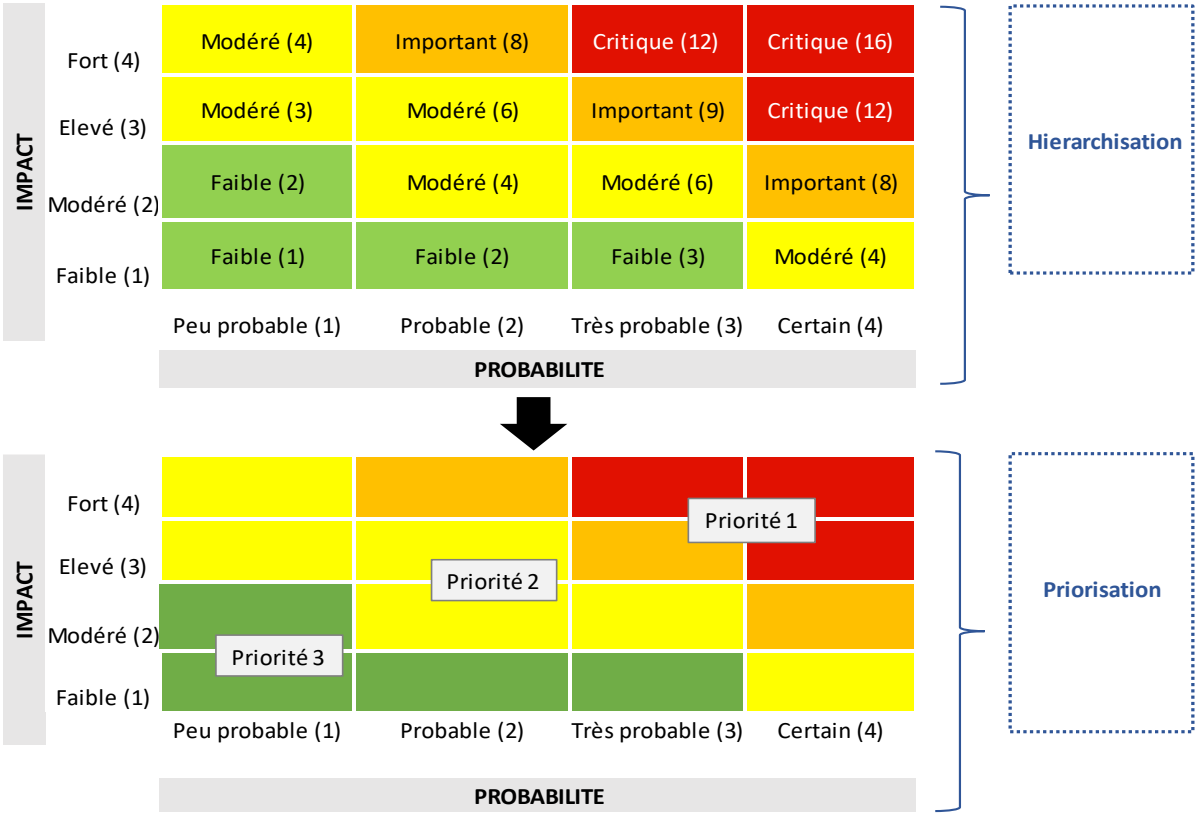
Le coût final de 4,2 M€ reste toutefois dans la moyenne estimée pour ce type d'attaque *(de l'ordre de 4,54M$ en 2022 selon le rapport d'IBM Security[10]).*

❖ **Méthodologie de priorisation du risque**

La méthodologie de priorisation des risques que nous avons appliqués consiste à :

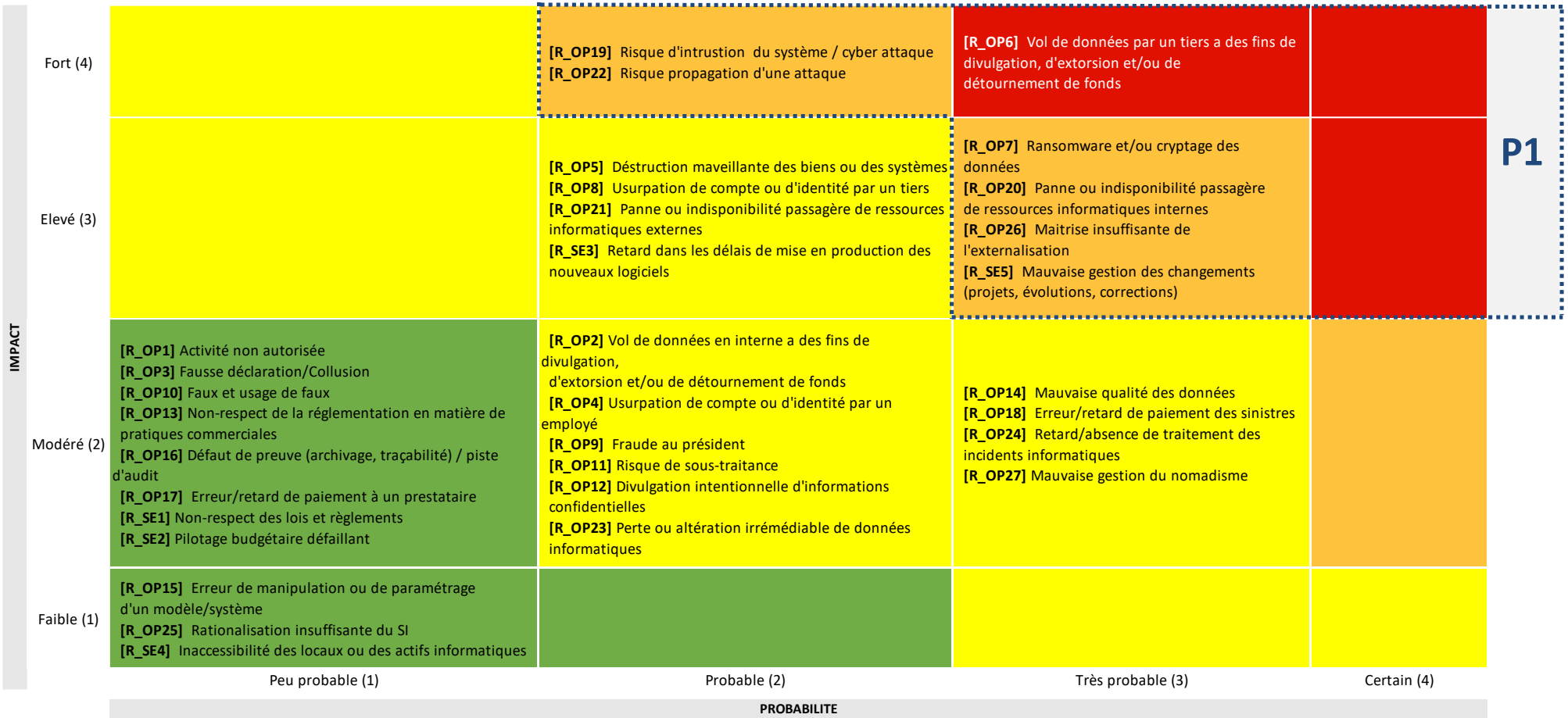
1. hiérarchiser les risques à partir de leur évaluation (note finale obtenue en fonction de l'**impact et de la probabilité**)

2. Prioriser les risques bruts majeurs (i.e. importants et critiques) conformément à la politique de gestion des risques de RUNEO



[10]« Rapport 2022 sur le coût d'une violation de données : Résumé analytique » https://www.ibm.com/downloads/cas/WY5EQ5MJ

L'application de cette méthodologie nous a ainsi permis de synthétiser l'évaluation des risques bruts de RUNEO dans la matrice de chaleur suivante :



Dans la suite de ce mémoire nous allons principalement nous intéresser aux risques majeurs informatiques (i.e. de priorité 1) :

- **[R_OP6]** : Risque de vol de données par un tiers, à des fins de divulgation, d'extorsion et/ou de détournement de fonds
- [R_OP19] : Risque d'intrusion du système/ cyber-attaque
- [R_OP22] : Risque de propagation d'une attaque
- [R_OP7] : Ransomware et/ou cryptage des données
- [R_OP20] : Panne ou indisponibilité passagère de ressources informatiques internes
- [R_OP26] : Maîtrise insuffisante de l'externalisation
- [R_SE5] : Mauvaise gestion des changements

2.3.2 Stratégie de gestion des risques majeurs

2.3.2.1 Traitement du risque et évaluation du risque résiduel

Le choix de/des options de traitement de risque **(refus, acceptation, réduction et transfert)*** a été déterminé en tenant compte des **objectifs de l'entreprise, des coûts, des avantages et des inconvénients** de leur mise en place.

Pour chacun de ces risques et en fonction des options qui ont été choisies, des éléments de maîtrise des risques (EDMR) ont été définis par les équipes de la DSI. L'objectif est qu'ils contribuent à diminuer le risque et à améliorer le dispositif de sécurité des SI déjà en place au sein de RUNEO.

Enfin, la dernière étape consistait à évaluer l'efficacité des EDMR afin de déterminer si le risque net est acceptable ou non, auquel cas des mesures complémentaires ou une revue de l'EDMR devrait être envisagées.

Code Risque	Risque	Cotation risque brut	Option de traitement	EDMR	Cotation risque net	Niveau d'acceptation	
R_OP6	Vol de données par un tiers a des fins de divulgation, d'extorsion et/ou de détournement de fonds	Fort	**REDUCTION TRANSFERT**	**[EDMR 1]** Renforcement de la sécurité périmètrique du SI **[EDMR 2]** Renforcement du dispositif antimalware sur l'ensemble des équipements et des logiciels **[EDMR 3]** Durcissement les mots de passe : authentification à double facteurs **[EDMR 4]** Sensibilisation et formation de l'ensemble des collaborateurs à la sécurité des SI **[EDMR 5]** Souscription d'une assurance cyber risque	Modéré	**Surveillance**	
R_OP7	Ransomware et/ou cryptage des données	Elevé			Modéré	**Surveillance**	
R_OP19	Risque d'intrustion du système / cyber attaque	Elevé			Modéré	**Surveillance**	
R_OP20	Panne ou indisponibilité passagère de ressources informati	Elevé		**[EDMR 6]** Renforcement de la sauvegarde "hors ligne" des données	Faible	**Assumé**	
R_OP22	Risque propagation d'une attaque	Elevé	**REDUCTION**	**[EDMR 7]** Segmentation et isolement des réseaux vitaux	Faible	**Assumé**	
R_OP26	Maitrise insuffisante de l'externalisation	Elevé	**REFUS REDUCTION**	**[EDMR 8]** Analyse des risques SI du prestataire avant contractualisation **[EDMR 9]** Définition de clauses contractuelles de sécurité conformes à la PSSI de RUNEO **[EDMR 10]** Suivi des incidents majeurs	Modéré	**Surveillance**	
R_SE5	Mauvaise gestion des changements (projets, évolutions, corrections)	Elevé	**REDUCTION ACCEPTATION**	**[EDMR 11]** Mise en place d'un comité de suivi et de coordination des travaux **[EDMR 12]** Réalisation de tests suffisants (recettes fonctionnelles et techniques)	Modéré	**Surveillance**	

2.3.2.2 Le suivi et l'amélioration : les clés d'un dispositif de sécurité cyber résilient

Suite à la présentation de nos travaux au CMDR le 15 avril 2022, La Direction Générale nous a demandé de proposer des indicateurs de suivi des risques majeurs, qu'elle intégrera ensuite dans son cadre d'appétence au risque. Nous avons donc établi un tableau de bord de KRI *« Key Risque Indicator »*[11] jugés pertinents que nous avons complété par des recommandations visant à renforcer le dispositif de contrôle actuel.

Indicateurs de risques (KRI)

TABLEAU DE BORDS DES KRI			
Catégorie	**Code**	**Description**	**Objectif**
Financier	**KRI_1**	Dépenses sécurité = (CAPEX/OPEX)[12] en sécurité IT / (Capex + Opex) IT cible	Assurer une meilleure gestion du budget de sécurité IT (privilégier les OPEX ou les CAPEX), gagner en efficience et en sécurité
RH	**KRI_2**	Taux de formation du personnel à la cybersécurité	Sensibiliser l'ensemble des collaborateurs pour diminuer le risque d'attaque
Opérationnel et Financier	**KRI_3**	Nb d'attaques/incidents détéctés (durée, impact financier, coûts)	Anticiper et améliorer le temps de réponse aux attaques Améliorer la qualité des données Mettre en place des plans d'actions
Stratégique	**KRI_4**	Taux d'avancement du plan de renforcement de la sécurité des SI de RUNEO	Prioriser les actions à mener en fonction du niveau : - d'exposition au risque cyber - de protection souhaité/acceptable
	KRI_5	Niveau de conformité des prestataires aux exigences contractuelles de sécurité (scoring)	Maitrise de l'externalisation

Principales recommandations

Reco 1 - La DSI devrait améliorer sa gestion opérationnelle de sécurité des SI

Un dispositif de sécurité cyber résilient commence par une bonne hygiène informatique. Or comme nous l'avons observé, les contrôles de niveau 1 ne sont pas forcément effectués ou bien réalisés malgré l'existence d'une politique de Sécurité des Systèmes d'Information.

Il parait de ce fait pertinent de mettre en place un « guide opérationnel d'hygiène informatique » à destination de la DSI et qui détaillerait sous forme de *check-list* les points de contrôle décrits dans la PSSI et à prioriser.

Reco 2 - L'Audit Interne devrait renforcer ses contrôles en matière de cybersécurité

Le fait qu'aucune mission d'audit cyber n'ait été menée depuis 2019 est une menace pour l'entreprise. En tant qu'organe de contrôle et relais d'information du Conseil d'Administration, l'Audit interne doit à minima :

- ⇒ réaliser annuellement une mission « cybersécurité » sur les actifs et systèmes d'exploitation **« critiques »** (audit d'intrusion[13], test du dispositif de sauvegarde…) et tous les 2 ans sur le dispositif global de sécurité
- ⇒ mandater une personne qualifiée pour mener spécifiquement ces audits avec l'équipe en place
- ⇒ s'assurer que les actions de sensibilisation sont réalisées de manière continue par le premier et second niveau de contrôle
- ⇒ communiquer directement avec la Direction Générale et alerter sur toute situation présentant un risque (rapport d'audit annuel, points biannuels sur les vulnérabilité observées, suivi des KRI…)

[11] Source : Guide des risques Cyber de l'Ifaci (2020)

[12] Indicateur consistant à mesurer (en %) le poids des dépenses d'investissement (CAPEX) en sécurité IT par rapport aux dépenses d'exploitation (OPEX) en sécurité IT et à calculer ensuite (en €) ce que cela représente sur le budget d'investissement cible en sécurité IT (CAPEX +OPEX).

[13] Un exemple est donné en annexe 4 de ce rapport

Reco 3 - La Direction des Risques devrait intégrer un scénario de crise cyber dans son Plan de Continuité d'Activité

La différence entre une crise cyber et non-cyber c'est qu'elle peut se propager très rapidement (de l'ordre de quelques minutes), être furtive, et même impacter le PCA. Il convient donc de se préparer à cette situation en :

- ⇒ formalisant une procédure spécifique de poursuite des activités en situation très dégradée (scénario extrême d'absence de SI pendant plusieurs jours voire plusieurs semaines)
- ⇒ définissant une organisation de gestion crise avec l'identification des parties prenantes, leur rôles et responsabilités (instances dirigeantes, DSI, RSSI, cellule de crise, intervenant externes)
- ⇒ définissant des outils de gestion de crise en l'absence de SI
- ⇒ définissant un plan de communication
- ⇒ définissant un plan de retour à la situation normale
- ⇒ testant périodiquement le dispositif de gestion de crise via des simulations de crise
- ⇒ prévoyant un retour d'expérience post-crise de manière à continuellement améliorer le plan

Conclusion : Faire face et survivre à un agresseur invisible

Le risque cyber évolue constamment, à mesure que la digitalisation et les technologies de pointe rendent l'entreprise plus vulnérable (Intelligence Artificielle, robotique, blockchain, IOT[14], Cloud Computing) mais aussi avec la sophistication croissante des attaques cybercriminelles.

Une évolution qui remet fondamentalement en cause la stratégie de cybersécurité adoptée par les organisations. Désormais, **la résilience aux cyber menaces est un critère de survie essentiel**. Sans investissement et engagement continu dans cette direction, les entreprises seront de plus en plus vulnérables aux cyberattaques et s'exposeront à des problèmes financiers, de réputation, et d'exploitation potentiellement insurmontables.

L'étude de cas de RUNEO a permis de mettre en lumière la démarche de cyber résilience qu'une entreprise d'assurance pourrait mettre en place. Celle-ci repose sur deux phases principales :

1. L'identification, l'évaluation et la gestion par une approche holistique des risques associés à son réseau et à son système d'information
2. Le renforcement de la gouvernance du risque IT ainsi qu'une meilleure gestion de la continuité de ses activités

En somme, cette approche permet non seulement de se prémunir d'une cyber attaque, mais aussi d'être en mesure d'y apporter une réponse rapide et opportune, ce qui favorisera la confiance et la création de valeur.

La cyber résilience demeure toutefois un concept relativement complexe à mettre en oeuvre. Selon le *World Economic Forum*[15], en 2022, 59% des responsables cyber ne font pas de distinction entre la cyber sécurité et la cyber résilience et seulement 19% des entreprises considèrent qu'elles sont cyber résilientes.

Pour autant, ces entreprises sont aujourd'hui prêtes à l'intégrer dans leur ecosystème et dans le pilotage de l'entreprise, grâce à une gestion proactive des risques liés à leur SI et en investissant notamment dans des technologies d'analyse, d'automatisation, de DevSecOp[16] et SOAR (orchestration, automatisation et réponse de sécurité).

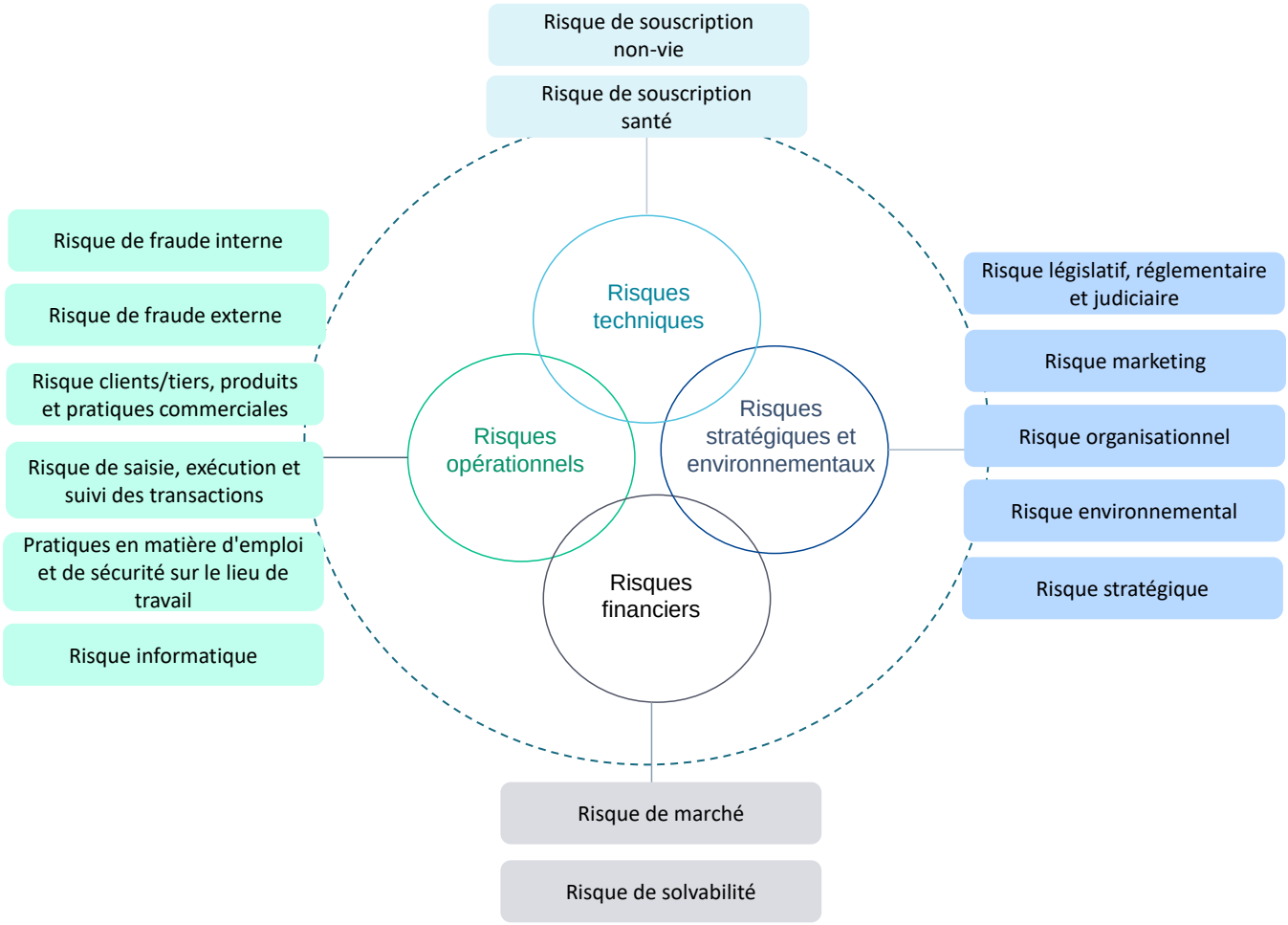
[14] *Internet Of Things* (l'internet des objets) désigne l'ensemble des infrastructures et technologies mises en place pour faire fonctionner des objets divers par le biais d'internet

[15] *« Global Cyberecurity outlook 2022 »* https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[16] Développement, Sécurité et Opérations

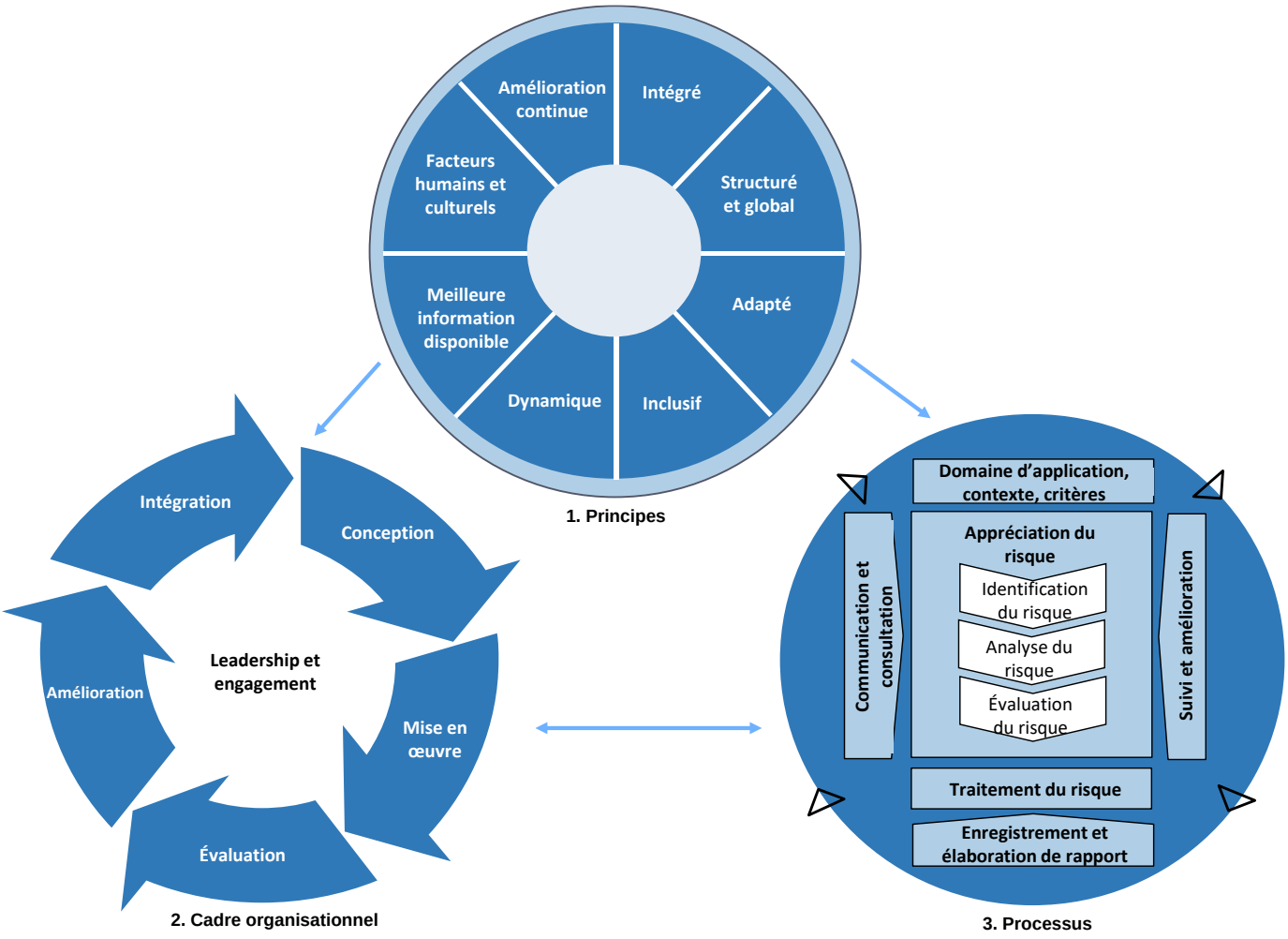
Annexes

Annexe 1 : L'univers de risque de RUNEO



Annexe 2 : Rappel de la norme ISO 31000 : 2018 relative au management des risques

Selon cette norme, les bases fondamentales du management du risque reposent sur les trois axes suivants[17] :



Les principes présentés en figure 1, constituent la pierre angulaire d'un management efficace des risques :

- Il doit être **intégré** à l'ensemble des activités de l'entreprise,
- Il requiert une approche **structurée**, **globale** et **dynamique** qui doit être **adaptée** à l'organisation et à ses objectifs,
- Il doit être **inclusif** (en impliquant les acteurs susceptibles de mener des actions pertinentes), et prendre en compte les **facteurs humains et culturels de l'entreprise,**
- C'est un processus qui suit un cycle **d'amélioration continue** et qui nécessite pour cela de disposer de **la meilleure information disponible**.

Ce sont ensuite ces principes qui vont permettre de définir **le cadre organisationnel de l'entreprise (figure 2)** et **les processus (figure 3)**

[17] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr

Annexe 3 : Nomenclature des risques informatiques de RUNEO

Code Risque	Risque	Définition du risque
R_OP_1	Activité non autorisée	Risque de perte financière causée par des activités non autorisées (non-criminelles) d'employés, des approbations ou un dépassement de l'autorité.
R_OP_2	Vol de données en interne a des fins de divulgation, d'extorsion et/ou de détournement de fonds	Acte volontaire d'un employé de voler des données de l'entreprise suite à une faille dans le dispositif de protection de l'intégrité des systèmes et des données
R_OP_3	Fausses déclarations/collusion	Activité criminelle entrainant des poursuites et incluant le risque de détournement d'actifs, de fraude corruptive et de fraude à l'information financière.
R_OP_4	Usurpation de compte ou d'identité par un employé	Utilisation frauduleuse par un employé des habilitations d'un autre employé dans le but d'accéder à un équipement ou une application
R_OP_5	Déstruction maveillante des biens ou des systèmes	Acte volontaire de vandalisme et de destruction des actifs physiques et/ou logiques de l'entreprise
R_OP_6	Vol de données par un tiers a des fins de divulgation, d'extorsion et/ou de détournement de fonds	Acte délibéré d'un tiers de voler des données de l'entreprise suite à une faille dans le dispositif de protection de l'intégrité des systèmes et des données
R_OP_7	Ransomware et/ou cryptage des données	Piratage ou tentative d'accès par un tiers aux systèmes de l'entreprise à des fins de vol, d'utilisation abusive et de manipulation d'informations ou pour endommager des données sur les systèmes
R_OP_8	Usurpation de compte ou d'identité par un tiers	Accès aux habilitations d'un employé par un tiers et utilisation frauduleuse
R_OP_9	Fraude au président	Tentive d'escroquerie par un tiers via différents canaux (phishing, appels, mails)
R_OP_10	Faux et usage de faux	Risque de délivrer un faux document dans le cadre de démarches administratives ou d'attestations
R_OP_11	Risque de sous-traitance	Risque de défaillance d'un prestataire important et critique
R_OP_12	Divulgation intentionnelle d'informations confidentielles	Risque de transmission par un employé d'informations confidentielles relatives à un client/prestataire
R_OP_13	Non-respect de la réglementation en matière de pratiques commerciales	Ventes agressives, pratiques commerciales trompeuses/douteuses ou interdites par la loi
R_OP_14	Mauvaise qualité des données	Risque caractérisé par: • une erreur dans la saisie, le suivi ou le chargement des données • défaut de contrôle de la qualité des données
R_OP_15	Erreur de manipulation ou de paramétrage d'un modèle/système	Mauvaise appropriation des outils par les utilisteurs causé par le non respect ou une mauvaise interprétation des procédures
R_OP_16	Défaut de preuve (archivage, traçabilité) / piste d'audit (qualité des données)	Risque lié à l'absence de dispositif de sauvegarde des données
R_OP_17	Erreur/retard de paiement à un prestataire	Risque de mauvaise manipulation des outils de paiements

R_OP_18	Erreur/retard de paiement des sinistres	Risque de mauvaise manipulation des outils de paiements
R_OP_19	Risque d'intrustion du système / cyber attaque	Décrit toute tentative d'accéder au système d'information de l'entreprise par un hacker
R_OP_20	Panne ou indisponibilité passagère de ressources informatiques internes	Impossibilité d'accès au serveur interne et aux applicatifs de l'entreprise
R_OP_21	Panne ou indisponibilité passagère de ressources informatiques externes	Impossibilité d'accès au site internet de l'entreprise ou à une solution informatique fournie par un prestataire
R_OP_22	Risque propagation d'une attaque	Risque de contamination de l'ensemble du réseau d'exploitation y compris le réseau des prestataires à la suite d'une attaque
R_OP_23	Perte ou altération irrémédiable de données informatiques	Risque de perte définitive des données stockées dans le serveur interne de l'entreprise
R_OP_24	Retard/absence de traitement des incidents de risque informatique	Risque d'insuffisance dans la détéction et la gestion des erreurs et des anomalies
R_OP_25	Rationalisation insuffisante du SI	Risque de manquement dans la gestion de l'obsolescence des outils informatique. Il inclut la non maîtrise de l'architecture (urbanisation) et l'incohérence des normes informatiques
R_OP_26	Maitrise insuffisante de l'externalisation	Risque reposant sur: • un cadre contractuel inadapté • une dépendance forte à une solution externalisée • un suivi insuffisant des niveaux de service et de la sécurité des SI • un dispositif de réversibilité insuffisant
R_OP_27	Mauvaise gestion du nomadisme	Dispositif de sécurité inadapté au télétravail
R_SE_1	Non-respect des lois et règlements	Risque de non-conformité des besoins des métiers au droit applicable, de non-conformité du système d'information par rapport aux préconisations juridiques des métiers et à l'incompatibilité des normes informatiques avec le droit applicable
R_SE_2	Pilotage budgétaire défaillant	Risque se traduisant par: • une allocation budgétaire insuffisamment alignée avec la stratégie • une allocation budgétaire absente ou insuffisamment claire • un suivi des dépenses insuffisant
R_SE_3	Retard dans les délais de mise en production des nouveaux logiciels	Risque de non-anticipation des besoins métier et des évolutions
R_SE_4	Inaccessibilité des locaux ou des actifs informatiques	Risque d'indisponibilité des locaux du siège
R_SE_5	Mauvaise gestion des changements (projets, évolutions, corrections)	Risque se traduisant par: • une mauvaise organisation dans la conduite du projet de transformation digitale de RUNEO • une mauvaise prise en compte des exigences fonctionnelles et techniques • un défaut dans les logiciels • une insuffisance des tests

Annexe 4 : Exemple de test d'intrusion sur le logiciel de Gestion Electronique des Données de RUNEO

1. Objectif et périmètre du test d'intrusion

Objectif

Le test d'intrusion est un moyen d'identifier les failles de sécurité d'un système d'information, d'une application web ou d'un logiciel. Il peut être fait en interne (depuis le réseau interne de l'entreprise) ou en externe (à partir d'une connexion internet).

Selon le type de test, le scénario de l'attaque sera différent :

	Test d'intrusion externe	Test d'intrusion interne
Profil de l'attaquant	Un pirate informatique malveillant qui tente de s'introduire dans le SI cible d'une organisation qu'il ne connait pas.	Un collaborateur, un prestataire ou toute personne mal intentionnée ayant déjà accès au réseau de l'entreprise.
Type de test	**Test d'intrusion « Boite Noire »** ■	**Test d'intrusion « Boite Grise »** ■
	L'attaquant ne dispose d'aucune information sur sa cible et doit en amont effectuer des recherches pour trouver une faille qui lui donnera accès au SI de l'entreprise.	L'attaquant dispose de quelques informations au départ (un identifiant et un mot de passe par ex.)

Périmètre : les tests d'intrusions sont menés par un prestataire externe et portent sur le logiciel de Gestion Électronique des Données (GED) de RUNEO

⇒ Test d'intrusion « boîte noire »

⇒ Test d'intrusion « boîte grise »

Date des tests d'intrusion : du 27 au 28 juillet 2022

2. Vulnérabilités observés et recommandations associées

Les résultats des 2 tests d'intrusion ont permis d'observer certaines vulnérabilités sur l'application. Celles-ci ont donné lieu aux recommandations suivantes :

#	Constat	Gravité	Recommandation	Priorité
V01	Divulgation des hashes des mots passe des utilisateurs de la solution	Élevée	Durcir la configuration du service Domino	Élevée
V02	Utilisation du protocole HTTP	Modérée	Forcer l'utilisation du protocole HTTPS pour l'ensemble de l'application	Très élevée
V03	Faille de type Cross-Site Scripting (XSS) volatile	Modérée	Protéger les entrées utilisateur contre les attaques de type Cross-Site Scripting	Très élevée
V04	Cookies de session non sécurisés	Modérée	Sécuriser les cookies de session	Élevée

Glossaire

Risque informatique : « Risque de perte résultant d'une inadéquation ou d'une défaillance des processus d'organisation, de fonctionnement, ou de sécurité du système d'information, entendu comme l'ensemble des équipements systèmes et réseaux, des logiciels et des données, ainsi que des moyens humains contribuant au traitement de l'information de l'institution » (ACPR)

Cybersécurité : « La cybersécurité est l'ensemble des contrôles et des mesures d'organisation ainsi que des moyens (humains, techniques, etc.) utilisés pour protéger les éléments du système d'information et des réseaux de communication contre toutes attaques logiques, que celles-ci soient conduites par le biais de brèches de sécurité physique ou logique. Ces contrôles et mesures incluent la prévention, la détection et la réponse à toute activité informatique malicieuse ou à toute négligence, qui pourrait affecter la confidentialité, l'intégrité ou la disponibilité des systèmes et des données, de même que la traçabilité des opérations effectuées sur ce système et ces réseaux. » (BCE)

Cyber résilience : La capacité d'un agent économique à surmonter le sinistre que peut constituer une attaque informatique, qu'elle soit furtive, sournoise (vol de données, sabotage, etc…) ou qu'elle soit ouverte (ransomware, déni de service, etc…), en insistant autant sur la prévention et la réduction du risque que sur les moyens concrets pour rétablir le plus vite possible son activité normale.

Ransomware : En français « Rançongiciel » désigne une technique d'attaque cybercriminelle qui consiste à s'introduire dans le SI d'une entreprise et à y installer un logiciel malveillant qui va chiffrer les données et perturber le bon fonctionnement du réseau informatique. Seul le paiement d'une rançon par l'entreprise aux cyber criminels permettrait d'obtenir la clé de déchiffrement.

CAPEX et OPEX : Catégories comptables permettant de classer les dépenses d'une entreprise.

- Les CAPEX (Capital Expenditures) désignent les dépensent d'investissement de l'entreprise dans l'objectif d'une croissance à long terme.
- A l'inverse, les OPEX (Operational Expenditures) désignent les dépenses d'exploitation courantes de l'entreprise.

Dans le pilotage du budget informatique d'une entreprise, ces 2 indicateurs sont indispensables. Ils permettent de définir une stratégie budgétaire en ligne avec les objectifs de l'entreprise. Chaque investissement ou dépense doit en effet être rentable.

L'entreprise peut par exemple faire le choix d'investir dans un service externalisé de « Cloud » pour heberger ses données (dépenses OPEX) plutôt que d'investir dans l'achat de ses propres serveurs (dépense CAPEX).

Le traitement du risque : Phase ayant pour but de mettre en œuvre des options afin de diminuer le risque auquel une entreprise est exposé. Ces options sont les suivantes :

- Le refus : consiste à ne pas s'engager ou maintenir l'activité porteuse de risque
- L'acceptation : marqué par le maintien d'un risque fondé sur une décision mesurée (pour saisir une oportunité par exemple)
- La réduction : consiste à limiter la source de risque par différents moyens (prévention, procédures, politiques)
- Le transfert : repose sur le partage du risque (souscription d'une couverture d'assurance)

Un risque peut impliquer une ou plusieurs options, selon les objectifs de l'entreprise et les ressources dont elle dispose.

Bibliographie

« BAROMÈTREANOZR WAY DU RANSOMWARE - Évolution de la menace de janvier à avril 2022 »
https://anozrway.com/fr/barometre-ransomware/

« Le risque informatique - Document de réflexion » ACPR. Janvier 2019
https://acpr.banque-france.fr/sites/default/files/medias/documents/819017_acpr_risque-informatique_fr_web.pdf

« Notice relative aux modalités de mise en œuvre par les organismes de retraite supplémentaire des orientations relatives à la sécurité et à la gouvernance des technologies de l'information et de la communication (EIOPA-BoS-20/600) » ACPR. Juillet 2021
https://acpr.banque-france.fr/sites/default/files/media/2021/07/02/20210702_notice_orientations_aeapp_orps.pdf

« Cyber Risk in the Insurance Sector A2ii – IAIS Consultation Call » Sept.19
https://www.a2ii.org/sites/default/files/2019-10/eng_1_cyber_risk_in_the_insurance_sector_a2ii_iais_consultation_call.pdf

« Guide d'hygiène informatique » ANSSI[18]
https://www.ssi.gouv.fr/particulier/guide/guide-dhygiene-informatique/

« PANORAMA DE LA MENACE INFORMATIQUE 2021 » ANSSI. Mai 2022
https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf

« Global Cybersecurity Outlook 2022 » World Economic Forum. Janv 2022
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

« Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing » CNIL
https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

« Supporting on-going capture and sharing of digital event data » CRO[19] Forum
https://www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf

« Rapport 2022 sur le coût d'une violation de données : Résumé analytique »
https://www.ibm.com/downloads/cas/WY5EQ5MJ

« Cyberattaques : l'assurance et le secteur financier premières cibles des ransomware » Argus de l'assurance
MARIE-CAROLINE CARRÈRE | 31/01/2022

« Cyberattaque : un groupe de protection sociale à l'arrêt » Argus de l'assurance
NICOLAS THOUET | 18/10/2022

[18] Agence Nationale de la Sécurité des Systèmes d'Information
[19] Chief Risk Officer