|  |
| --- |
|  |
| Nom de l’organisation |
| Titre du projet |
| Rapport d’analyse des risques |

Informations générales

|  |  |
| --- | --- |
| Numéro de séquence | Q140 |
| Version | 4.9 |
| État | Projet |
| Approuvé par | … |
| Date d’approbation | 15/04/19 |
| Classification | Interne |

Liste de distribution

|  |  |  |
| --- | --- | --- |
| Destinataire | Canal | Raison |
|  | Choisir | Validation |
|  | Choisir | Validation |

Historique

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Auteur | Modifications |
| 0.1 | … |  |  |
| 0.2 | … |  |  |

Groupe de travail

|  |  |
| --- | --- |
| Nom | Entité |
| Groupe de travail Client (Liste avec première lettre du prénom et nom) | Customer |
| Groupe de travail itrust (Liste avec première lettre du prénom et nom) | itrust consulting |

Approbations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom | Rôle | Responsabilité | Date | Signature |
|  | Choisir | Choisir | … |  |
|  | Choisir | Choisir | … |  |

Sommaire analytique

##### Contexte

Ce document présente les résultats de l’appréciation du risque effectuée par Name of the consultant. Ce projet visait à obtenir une évaluation du risque détaillée pour établir une vue de la gestion du risque courant et un plan de traitement utilisé pour améliorer la sécurité des traitements de l’information au cours des prochaines années. L’appréciation et le traitement des risques ont suivi les conseils de la norme ISO/IEC 27005 sur la gestion du risque et se sont fondés sur l’outil TRICK Service développé par itrust consulting.

##### Périmètre de l’analyse

Le périmètre de l’analyse de risque était le suivant : Résumé du scope

##### Résultats et limitations

En accord avec le Customer les résultats de la présente analyse sont suffisants pour mettre en œuvre le plan de traitement des risques et accepter les risques résiduels. Cependant, ces résultats devront faire l’objet d’une révision périodique pour être en mesure de décrire l’état réel du risque de l’organisation.

##### Actifs considérés dans l’étude et évaluation du risque afférent

Les actifs considérés dans le périmètre d’étude représentent une valeur total de **0** k€ et la somme total des risques de l’organisation relatifs à ces actifs a été estimé à **0** k€/an (ALE).

|  |  |  |
| --- | --- | --- |
| Type d’actif | Valeur par type d’actif (k€) | Risque par type d’actif (k€/an) |
| Information | 0 | 0 |
| Logiciel | 0 | 0 |
| Matériel | 0 | 0 |
| Réseau | 0 | 0 |
| Ressource humaine | 0 | 0 |
| Service | 0 | 0 |
| Processus métier | 0 | 0 |
| Conformité | 0 | 0 |
| Financier | 0 | 0 |
| Immatérielle | 0 | 0 |
| Total | 0 k€ | 0 k€/an |

##### Niveau de sécurité actuel

Le niveau d’implémentation de la sécurité est estimé en moyenne à **0** % des exigences des normes et règlement considérés lors de l’étude. Il est à noter que le niveau d’implémentation des mesures de sécurité relatif aux normes et règlements considérés doit être supérieur à 0 % pour assurer un niveau de conformité suffisante par rapport aux spécifications minimum de sécurité contenues dans lesdites normes et règlements.

##### Plan de traitement du risque

Un plan de traitement du risque a été établi, contenant **0** phases :

La rentabilité moyenne annuelle des investissements (ROSI) en termes de mesures de sécurité est estimée à 0 k€ pour l’ensemble du plan de traitement. Le plan de traitement permettra d’atteindre un ROSI relatif estimé à 0 % ce qui signifie que tout euro investi dans une mesure de sécurité permettra en moyenne de limiter de 0 € la perte annuelle due à des incidents qui se pourraient se produire sans cet investissement.

Les risques annuels devraient passer de **0** k€ à **0** k€ après les phases d’implémentation, ce qui est inférieur au niveau de risque acceptable.

Table des matières

[1 Introduction 7](#_Toc506976207)

[1.1 Contexte 7](#_Toc506976208)

[1.2 Objectifs du document 7](#_Toc506976209)

[1.3 Périmètre de l’analyse 7](#_Toc506976210)

[1.4 Audience 7](#_Toc506976211)

[1.5 Structure de ce document 7](#_Toc506976212)

[1.6 Références 7](#_Toc506976213)

[1.7 Acronyme 8](#_Toc506976214)

[1.8 Terminologie 8](#_Toc506976215)

[2 Méthodologie et déroulement de l’analyse 10](#_Toc506976216)

[2.1 Méthodologie 10](#_Toc506976217)

[2.1.1 Établissement du contexte 10](#_Toc506976218)

[2.1.2 Appréciation du risque 10](#_Toc506976219)

[2.1.3 Traitement des risques 11](#_Toc506976220)

[2.1.4 Acceptation des risques 11](#_Toc506976221)

[2.2 Déroulement de l’étude 12](#_Toc506976222)

[3 Contexte du risque 13](#_Toc506976223)

[3.1 Considérations générales 13](#_Toc506976224)

[3.2 Critères de bases 13](#_Toc506976225)

[3.2.1 Critères d’évaluation des risques 13](#_Toc506976226)

[3.2.2 Critères d’impact 13](#_Toc506976227)

[3.2.3 Critères d’acceptation du risque 13](#_Toc506976228)

[3.3 Description de la cible 14](#_Toc506976229)

[4 Appréciations des risques 15](#_Toc506976230)

[4.1 Réunion d’appréciation des risques 15](#_Toc506976231)

[4.2 Identification des risques 15](#_Toc506976232)

[4.2.1 Identification des actifs 15](#_Toc506976233)

[4.2.2 Brainstorming 16](#_Toc506976234)

[4.2.3 Cartographie des menaces 16](#_Toc506976235)

[4.2.4 Cartographie des vulnérabilités 16](#_Toc506976236)

[4.2.5 Cartographie des risques 16](#_Toc506976237)

[4.3 Analyse des risques 16](#_Toc506976238)

[4.3.1 Scénarios de risque, probabilité et échelle d’impact 17](#_Toc506976239)

[4.3.2 Vue d’ensemble des résultats de l’analyse 17](#_Toc506976240)

[4.3.3 Classification des risques actuels 17](#_Toc506976241)

[4.4 Evaluation des risques 19](#_Toc506976242)

[5 Plan de traitement des risques 20](#_Toc506976243)

[5.1 Considération générale regardant l’indentification des mesures 20](#_Toc506976244)

[5.1.1 Paramétrage et validité des résultats 20](#_Toc506976245)

[5.1.2 Une méthodologie fondée sur la rentabilité 20](#_Toc506976246)

[5.2 Résumé du plan de traitement 20](#_Toc506976247)

[5.3 Augmentation du taux de conformité et rentabilité des phases 21](#_Toc506976248)

[5.4 Détail du plan de traitement 22](#_Toc506976249)

[6 Acceptation du risque 23](#_Toc506976250)

[7 Boucle de rétroaction du processus d’appréciation des risques 23](#_Toc506976251)

[7.1 Communication et consultation sur les risques 23](#_Toc506976252)

[7.2 Surveillance et revue des risques 23](#_Toc506976253)

[8 Niveau d’implémentation 24](#_Toc506976254)

[8.1 Modus operandi 24](#_Toc506976255)

[8.2 Evolution du niveau de conformité de l’organisation 25](#_Toc506976256)

[8.2.1 Niveau de conformité ISO/IEC 27001 25](#_Toc506976257)

[8.2.2 Niveau de conformité ISO/IEC 27002 26](#_Toc506976258)

[Annexe : Liste des mesures de sécurité applicables à la TOE 27](#_Toc506976259)

Liste des figures

Figure 1: Le processus d’appréciation du risque 10

Figure 2 : Perte annuelle attendue (ALE) par actif 18

Figure 3 : Perte annuelle attendue (ALE) par type d’actif 18

Figure 4 : Perte annuelle attendue (ALE) par scénario de risque 19

Figure 5 : Perte annuelle attendue (ALE) par type de scénario de risque 19

Figure 6 : Rentabilité du plan de traitement des risques 22

Figure 7 : Taux de conformité ISO/IEC 27001 pendant les différentes phases d’implémentation 25

Figure 8 : Taux de conformité ISO/IEC 27002 pendant les différentes phases d’implémentation 26

Liste des tableaux

[Table 1 : Considérations générales sur l’envergure de l’analyse de risque 14](#_Toc506976268)

[Table 2: Liste des réunions organisées avec les experts pour réaliser l’appréciation des risques 15](#_Toc506976269)

[Table 3 : Liste des actifs appartenant à la cible de l’analyse des risques 15](#_Toc506976270)

[Table 4 : Liste des actifs non considérés appartenant à la cible de l’analyse des risques 15](#_Toc506976271)

[Table 5 : Échelle de niveau d’exposition au risque 16](#_Toc506976272)

[Table 6 : Cartographie des menaces 16](#_Toc506976273)

[Table 7 : Liste des vulnérabilités 16](#_Toc506976274)

[Table 8 : Cartographie des risques 16](#_Toc506976275)

[Table 9 : Scénarios de risques considérés 17](#_Toc506976276)

[Table 10 : Échelle de probabilité d’un scénario de risque 17](#_Toc506976277)

[Table 11 : Échelle d’impact d’un scénario de risque 17](#_Toc506976278)

[Table 12 : Résumé des caractéristiques des phases d’implémentation 21](#_Toc506976279)

[Table 13 : Plan de traitement du risque selon TRICK Service 22](#_Toc506976280)

[Table 14 : Échelle d’implémentation des mesures de sécurité 24](#_Toc506976281)

# Introduction

## Contexte

La mise en œuvre raisonnée de mesures de sécurité pour protéger le traitement de l’information, en particulier dans le cas de la mise en place d’un système de gestion de la sécurité de l’information (SMSI), requiert de la part d’une organisation d’effectuer une analyse de risque afin d’adapter la réponse de sécurité aux menaces, aux impératifs tant du métier que légaux à l’appétit au risque de l’organisation elle-même. Dans cette optique, Customer a décidé de réaliser une analyse conforme aux guidances de la norme ISO/IEC 27005 en usant de l’application web d’analyse de risque TRICK Service développé par itrust consulting.

## Objectifs du document

Ce document présente l’épreuve publiée des résultats de l’analyse de risque réalisée par Nom du Consultant. La version mise à jour et applicable est cependant la version web de l’analyse de risque consultable via l’application web TRICK Service.

## Périmètre de l’analyse

L’analyse de risque décrite dans ce rapport s’applique au système de traitement de l’information compris dans le périmètre suivant : Résumé du scope

## Audience

Ce rapport s’adresse en premier lieu aux responsables, ensuite aux propriétaires des actifs ou s’ils diffèrent des risques et enfin à tout le personnel concerné.

## Structure de ce document

La structure du document est la suivante :

* Le chapitre 2 décrit la méthodologie de l’analyse des risques.
* Le chapitre 3 décrit le contexte, la cible, et les valeurs des actifs considérés dans l’analyse des risques, selon de la démarche ISO/IEC 27005.
* Le chapitre 4 présente le résultat de l’estimation des risques.
* Le chapitre 5 renseigne sur le niveau d’implémentation et les coûts des mesures de sécurité déjà mise en place conformément aux normes et règlement considérés.
* Le chapitre 6 présente une proposition de plan de traitement de risques, consistant en une liste de mesures de sécurité tirée de normes internationales ou de bonnes pratiques de sécurité.
* L’annexe est constituée par l’ensemble des états d’implémentation des mesures de sécurité venant des différentes normes internationales et bonnes pratiques considérées.

## Références

1. ISO/IEC 27001:2013(F) Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences.
2. ISO/IEC 27002:2013(F) Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information.
3. ISO/IEC 27005:2011(F), Technologies de l'information — Techniques de sécurité — Processus de gestion de risque de la sécurité de l'information.

## Acronyme

|  |  |
| --- | --- |
| ALE | Annual Loss Expectancy (Perte annuelle attendue) |
| MAGERIT | Analyse de Risque et Méthodologie de Management pour les Systèmes d’Information (méthodologie d’analyse des risques publié par le gouvernement espagnole) |
| ROSI | Return On Security Investment (le retour sur investissement d’un projet de sécurité) |
| TRICK- | Tool for RIsk management based on Central Knowledge base |
| TOE | Target of Evaluation |

## Terminologie

|  |  |
| --- | --- |
| Acceptation du risque | Processus destiné à valider le traitement du risque mise en place pour obtenir un risque acceptable pour les partis prenants c’est-à-dire à valider formellement les mesures mises en place pour diminuer ou transférer le risque et à accepter les risques résiduels. |
| Analyse du risque | Processus permettant de comprendre la nature du risque et de déterminer le niveau du risque de la TOE. |
| Appréciation du risque | Processus complet comprenant l’identification du risque, l’analyse du risque et l’évaluation du risque. |
| Consultation et communication du risque | Processus continu et itératif, conduit par les organes chargés de la gestion du risque, pour fournir, partager et obtenir de la part des parties intéressées de l’information regardant la gestion du risque, au cours d’un réel dialogue avec eux. |
| Contre-mesure | En anglais « Control » : mesure qui modifie un risque. Appelé aussi mesure de sécurité. |
| Critères du risque | Base de référence à partir de laquelle est jugée l’importance d’un risque. |
| Évaluation du risque | Processus consistant d’une part à comparer les résultats de l’appréciation des risques avec les critères de risque et d’autre part à déterminer si le risque ou son amplitude est acceptable ou tolérable. |
| Identification du risque | Processus permettant de recherche, d’expertise et de description du risque  Note1 : l’identification des risques implique l’identification de leurs origines, de leurs causes et de leurs conséquences potentielles.  Note2 : lors de l’identification des risques sont pris en compte les données historiques, les analyses théoriques, les avis documentés et experts et les besoins des partis prenants. |
| ISO/IEC 27001 | Norme internationale élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l’information. |
| ISO/IEC 27002 | Norme internationale qui a pour objet de servir d'outil de référence permettant aux organisations de sélectionner les mesures nécessaires dans le cadre d'un processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/IEC 27001 ou de guide pour les organisations mettant en œuvre des mesures de sécurité de l'information largement reconnues. |
| ISO/IEC 27005 | Norme internationale qui fournit un guide pour la gestion des risques liés à l’information en supportant en particulier les exigences d’un système de gestion de l’information (SMSI) selon l’ISO/IEC 27001. |
| Partis prenants | En anglais « Stakeholders » : personne ou organisation qui peuvent affecter, sont affectées ou se considèrent comme affectées par une décision ou une activité. |
| Perte annuelle attendue | Annual Loss Expectancy (Perte annuelle attendue), c’est la métrique pour comparer des risques (en €). |
| ROSI | Le retour sur investissement d’un projet de sécurité, obtenu comme différence entre le changement du risque avant et après la mise en place de la mesure (Delta ALE) et le coût annuel de cette mesure. |
| Cible d’évaluation (TOE) | « Target Of Evaluation » - partie d’une organisation ou processus accompagné de toutes les entités (technique, organisationnel ou humain) directement afférentes pour son bon fonctionnement faisant l’objet de l’appréciation et le traitement des risques. |
| Traitement du risque | Processus destiné à modifier le risque. |
| TRICK Service | Outil d’appréciation et le traitement des risques de la société itrust consulting. |
| Surveillance et revue du risque | Processus permettant de surveiller le niveau du risque et d’évaluer si celui-ci demeure dans les limites acceptables fixées et d’identifier tous risques nouveaux du fait d’un changement de contexte interne ou externe à la TOE. |

# Méthodologie et déroulement de l’analyse

## Méthodologie

L’appréciation du risque et l’établissement du plan de traitement des risques ont été conduits dans le respect du processus de gestion des risques tel qu’il est décrit dans la norme ISO/IEC 27005 et tel qu’il est représenté dans la figure ci-dessous.



Figure 1: Le processus d’appréciation du risque

### Établissement du contexte

Ce processus vise à spécifier les critères de base de l’évaluation des risques, la cible et le périmètre de cette analyse, l’organisation du processus de gestion des risques.

### Appréciation du risque

Ce processus se décompose en trois phases distinctes permettant d’identifier les risques selon leur occurrence probable, leur gravité.

#### Identification des risques

L’objectif de l’identification des risques est de déterminer ce qui pourrait causer des pertes et de comprendre comment, où, et pourquoi ces pertes pourraient arriver. Cette phase prépare l’estimation des risques proprement dits. Elle s’est déroulée selon les phases suivantes :

1. Identification des actifs (voir section 3.3.2)
2. Identification des menaces (voir section 4.1).
3. Identification des mesures de sécurité existante (voir chapitre 5 et Annexe).
4. Identification des vulnérabilités (inhérente à l’identification des spécificités des risques) (voir section 4.2).
5. Identification des conséquences (lors d’une discussion pour l’estimation des conséquences, en considérant les critères d’impact (cf. section 4.3).

#### Analyse des risques

L’analyse des risques inclut plusieurs phases :

1. Le choix de la méthodologie.
2. L’estimation des conséquences (voir section 4.4.2)
3. L’estimation des probabilités d’occurrences (voir section 4.4.2).
4. L’estimation du niveau de risque (voir section 4.4.3).

#### Évaluation des risques

Le processus d’évaluation des risques compare la liste de risques avec les critères d’acceptation du risque et permet d’établir une liste ordonnée de risques conformément aux critères précédents en vue d’un plan de traitement. En sus, le processus considérera les obligations légales et contractuelles à mettre en œuvre.

### Traitement des risques

Le traitement du risque consiste à choisir les mesures afin de réduire, éviter, ou transférer les risques, à décider de retenir certains risques, et à planifier la mise en œuvre de ces mesures.

Le choix des mesures dépend des coûts des mesures, mais aussi de l’avantage attendu ou de l’obligation[[1]](#footnote-1) de ces mesures. Le traitement des risques inclut nécessairement une indication du niveau de risque après mise en œuvre du plan de traitement de risques.

Cette phase produit un plan de traitement de risques qui est une liste planifiée des mesures proposées pour réduire les risques et une indication du risque résiduel, c'est-à-dire du risque après mis en œuvre pour validation par les managers de l’organisation.

### Acceptation des risques

Cette phase consiste pour les responsables de l’organisation à accepter le risque résiduel et à prendre la responsabilité de mettre en œuvre un plan de réduction du risque adéquate pour atteindre ce niveau résiduel. Cette décision inclut l’acceptation du plan de traitement des risques, c’est-à-dire l’engagement de mettre en œuvre les ressources financières et humaines, d’assurer la délégation des charges nécessaire à sa mise en œuvre selon ce qui a été défini.

La décision doit être formellement enregistrée.

Note : L’acceptation du risque n’est pas formellement couverte par ce rapport et doit faire l’objet d’un processus dédié.

## Déroulement de l’étude

Afin d’apprécier les risques de Nom de l’organisation, nous avons suivi la démarche suivante :

1. Description de la cible de l’analyse des risques.
2. Identification des actifs par rapport à la connaissance du métier.
3. Classification et estimation de la valeur des actifs sélectionnés.
4. Étude du niveau actuel d’implémentation des spécifications et mesures de sécurité préconisées par les référentiels suivants :
   1. ISO/IEC 27001 ;
   2. ISO/IEC 27002 ;
5. Estimation de la valeur ajoutée lors de l’implémentation des mesures de sécurité additionnelles à l’aide de la base de connaissance TRICK Service;
6. Validation des résultats ;
7. Validation du plan de traitement des risques ;
8. Résumé et présentation des conclusions.

# Contexte du risque

## Considérations générales

Le processus d’analyse des risques consiste à réaliser une évaluation haut-niveau des risques en collaborations avec les propriétaires des actifs, à peaufiner l’évaluation du niveau du risque des systèmes de traitement compris dans le périmètre de l’étude, à définir le niveau d’acceptation du risque souhaité et à formuler un plan de traitement du risque pour atteindre ce niveau souhaite de risque.

L’approche pour l’évaluation des risques est une combinaison des méthodes suivantes :

1. Identification des risques selon la cartographie des menaces de la méthode MAGERIT et documentation de contre-mesures dédiées en réunion d’experts.
2. Estimation quantitative des risques par actif avec TRICK Service.
3. Évaluation du niveau d’implémentation des mesures de sécurité et estimation des coûts pour atteindre une conformité complète.
4. Estimation de la rentabilité des mesures de sécurité avec TRICK Service.
5. Pondération des mesures de sécurité en vue d’établir un plan de traitement des risques.

## Critères de bases

### Critères d’évaluation des risques

Dans cette première itération du processus, les risques sont évalués en considérant :

* L’importance des informations pour assurer le fonctionnement de l’activité afférente à la cible de l’analyse des risques ;
* Les conséquences financières directes pour les recettes et dépenses ;
* Les trois aspects de sécurité (confidentialité, intégrité, disponibilité).

### Critères d’impact

L’impact d’un incident de sécurité est estimé en matière de coût, c’est-à-dire de perte financière potentiel. Si cette estimation est trop incertaine, l’impact est estimé en attribuant un niveau formel qualitatif d’impact, à savoir : vital, extrêmement sérieux, très sérieux, sérieux, mineur, insignifiant. Cependant, bien que qualitatif en apparence, cette échelle est une échelle logarithmique, pour laquelle à chaque seuil est associé une estimation financière des pertes telles qu’elles pourraient être ressenties par l’organisation lors de de la survenance de tels impacts. Ces seuils seront généralement liés à un pourcentage du chiffre d’affaire et aux conditions de pérennisation de l’activité.

Note : Même si les impacts seront généralement calculés en considérant les coûts associés à la perte d’une ou de plusieurs propriétés de sécurité des actifs, à savoir la confidentialité, l’intégrité, et la disponibilité.

### Critères d’acceptation du risque

Les critères d’acceptation du risque ont été définis comme suit :

1. Les risques pour lesquels l’exposition de la cible est évaluée comme faible ou très faible selon la première démarche d’appréciation des risques (méthode MAGERIT cf.) sont acceptés et non considérés explicitement dans le traitement des risques.
2. Les risques dont l’exposition est considérée comme importante ou très importante selon la première démarche d’appréciation des risques nécessitent que soient identifiées des contre-mesures applicables. Les risques sont considérés comme acceptés si les responsables de Nom de l’organisation ont été formellement informés et qu’ils ont accepté l’implémentation des contremesures identifiées.
3. Les risques considérés comme normaux sont acceptés dès que le responsable de Nom de l’organisation est informée de l’estimation du risque et que :
   1. soit l’implémentation de toutes les mesures de sécurité prévues dans les normes et règlement et estimées comme rentables avec la méthode TRICK Service a été planifiée,
   2. soit que suffisamment de mesures ont été planifiées pour que les pertes annuelles soient inférieures à \*\*.\* k€, seuil correspondant à une perte connue et acceptable relativement au chiffre d’affaire de l’organisation (% du chiffre d’affaire).

Note : un niveau de risques supérieur de \*\*.\* k€ à la limite précédente peut temporairement subsister à condition que l’organisation ait formellement accepté un plan de traitement des risques destiné à les réduire en deçà de cette limite et endéans de \*\* mois.

## Description de la cible

Le tableau ci-dessous résume les principales caractéristiques ainsi que les contraintes pour l’appréciation et le traitement des risques de la cible et de son environnement.

Table 1 : Considérations générales sur l’envergure de l’analyse de risque

# Appréciations des risques

L’appréciation des risques est composée de trois phases distinctes permettant d’identifier, d’analyser et d’évaluer les risques.

## Réunion d’appréciation des risques

L’appréciation des risques a été effectuée lors de réunion avec des experts métiers. Le tableau suivant énumère les différentes réunions qui ont eu lieu dans ce but.

|  |  |  |
| --- | --- | --- |
| Départment | Participants | Date des réunions |
|  |  | 1. jj/mm/aaaa 2. jj/mm/aaaa 3. jj/mm/aaaa |
|  |  | 1. jj/mm/aaaa 2. jj/mm/aaaa 3. jj/mm/aaaa |
|  |  | 1. jj/mm/aaaa 2. jj/mm/aaaa 3. jj/mm/aaaa |

Table 2: Liste des réunions organisées avec les experts pour réaliser l’appréciation des risques

## Identification des risques

L’objectif de l’identification des risques est de déterminer ce qui pourrait causer des pertes, et comprendre comment, où et pourquoi ces pertes pourraient se produire. Cette phase prépare l’appréciation des risques. Elle se déroule selon l’ordre déterminé suivant :

1. Identification des assets ;
2. Identification des menaces, des vulnérabilités et des risques spécifiques (lors d’une réunion de type brainstorming) ;
3. Identification des mesures existantes de sécurité (cf. Annexe) ;
4. Indentification des conséquences que la perte de confidentialité, d’intégrité ou de disponibilité pourrait avoir pour la cible choisie de l’appréciation des risques (le détail de cette analyse est inclus dans l’annexe de ce document).

### Identification des actifs

Le tableau suivant fait la liste des actifs considéré comme suffisamment critique pour être inclus dans le processus d’analyse de risque. Cette liste comprend une évaluation de la valeur financière de chaque actif considéré. Cette valeur correspond soit au prix d’achat soit au coût d’investissement pour (re-)créer l’actif en question.

Table 3 : Liste des actifs appartenant à la cible de l’analyse des risques

Le tableau suivant énumère tous les actifs qui ne seront pas pris en compte dans le processus d’analyse de risque car non considérés comme critiques.

Table 4 : Liste des actifs non considérés appartenant à la cible de l’analyse des risques

### Brainstorming

Au cours des réunions réunissant les experts, des listes standards (tirées de la méthode MAGERIT) de menaces, vulnérabilités et risques spécifiques, ordonnées de manière logique, seront évaluées pour savoir si l’organisation présente une exposition élevée (Niveau ++ ou +), normale (niveau n) ou faible (niveau – et --) par rapport à la moyenne.

|  |  |  |
| --- | --- | --- |
| Exposition | | |
| Zone | **Symbole** | **Description** |
| 1 | - - | Très faible |
| - | Faible |
| 2 | N | Normale |
| 3 | + | Importante |
| + + | Très importante |

Table 5 : Échelle de niveau d’exposition au risque

### Cartographie des menaces

Dans cette phase, différentes menaces sont prises en compte. Afin d’assurer que les menaces abordées sont suffisamment complètes, les menaces seront cartographiées selon la méthode MAGERIT. L’exposition de l’organisation est déterminée selon l’échelle présentée plus haut (cf. Tableau 1) en regard de la définition formelle de la menace et de l’exposition généralement admise d’organisation de même dimension et exerçant le même type d’activité.

Table 6 : Cartographie des menaces

### Cartographie des vulnérabilités

Une menace peut seulement devenir un risque s’il existe des vulnérabilités. Ainsi il est très important de connaître ses vulnérabilités afin de pouvoir prendre des mesures préventives pour éviter qu’une menace puisse exploiter une telle vulnérabilité et créer un impact.

Table 7 : Liste des vulnérabilités

### Cartographie des risques

Après avoir considéré les aspects marquants dans cette cartographie, on a considéré la liste des menaces regroupées par source, afin d’évaluer l’exposition relative de la cible. Cette évaluation considère non seulement la force et la fréquence de la menace, mais aussi le niveau de vulnérabilité des actifs ciblés.

Table 8 : Cartographie des risques

## Analyse des risques

L’analyse de risque comprend les étapes suivantes :

1. Le choix de la méthodologie
2. La détermination des conséquences des risques estimées en regard d’une échelle prédéfinie.
3. La détermination de la probabilité d’occurrence des risques estimée en regard d’une échelle prédéfinie.
4. La détermination du niveau de risque (cf. Annexe).

### Scénarios de risque, probabilité et échelle d’impact

Dans cette prochaine étape, les risques ont été quantifiés en utilisant l’outil TRICK Service. Les pertes annuelles ont été évaluées en considérant un certain nombre de scénarios de risque. Ces scénarios considèrent les menaces et vulnérabilités essentielles en relation avec les 3 critères de sécurité de l’information : Confidentialité, Intégrité, et Disponibilité.

Table 9 : Scénarios de risques considérés

Il revient normalement au consultant en relation avec les responsable métiers d’estimer les risques en considérant les pertes financières probables en cas de survenance du risque. Cependant au cours de l’estimation des risques, il arrive qu’une estimation quantitative soit trop incertaine et qu’elle ne puisse être envisagée que de manière qualitative. Et afin, malgré tout, de pouvoir établir un bilan financier des pertes attendues et de mesures de la rentabilité des mesures, nous traduisons les estimations qualitatives en estimation quantitative en nous servant des échelles de valeurs suivantes.

Table 10 : Échelle de probabilité d’un scénario de risque

Table 11 : Échelle d’impact d’un scénario de risque

### Vue d’ensemble des résultats de l’analyse

Le tableau suivant contient, pour chaque paire actif-menace, les estimations :

* De l’impact quand la menace se produit sur l’actif (en kilo euros ou en utilisant une valeur de l’échelle d’impact) ;
* De la probabilité annuelle d’occurrence de la menace.

Ces estimations ont permis de calculer la Perte Annuelle Attendue ou ALE (Annual Loss Expectancy) qui représente le risque financier actuel de l’organisation quant à la sécurité de l’information. L’ALE est calculée en multipliant l’impact pour un scénario choisi et la probabilité de réalisation de cet impact par an. L’ALE global (pour l’ensemble des critères) d’un actif est obtenue en additionnant les sous-ALE de l’actif pour l’ensemble des scénarios.

### Classification des risques actuels

Les figures incluses dans cette section permettent d’une part d’identifier quels actifs ou types d’actif sont les plus exposés aux risques (Figure 2 et Figure 3)et d’autre part quels scenarios ou quel type de scenarios sont les plus à même de conduire à ces risques (Figure 4 et Figure 5)

Figure 2 : Perte annuelle attendue (ALE) par actif

Figure 3 : Perte annuelle attendue (ALE) par type d’actif

Figure 4 : Perte annuelle attendue (ALE) par scénario de risque

Figure 5 : Perte annuelle attendue (ALE) par type de scénario de risque

## Evaluation des risques

L’évaluation des risques consiste à comparer les résultats de l’analyse des risques avec les critères d’acceptation des risques qui ont été défini avec les partis prenant (cf. section).

Tous les risques considérés comme non-acceptable doivent être traités dans un plan déterminé de traitement des risques.

# Plan de traitement des risques

Afin de traiter les risques identifiés lors de ce projet et qualifiés pour un traitement, nous avons dressé une liste d’actions recommandées destinées à être implémentées. La liste est déduite de l’analyse de normes et guides de bonnes pratiques proposant des mesures de sécurité qui ont été agencées en un plan réfléchi d’implémentation en utilisant l’outil TRICK Service. La mise en œuvre de cette liste d’action permettra de réduire les risques à un niveau acceptable.

Le plan de traitement des risques inclut une indication du niveau du risque après l’implémentation effective du plan de traitement des risques. Le plan de traitement des risques comporte plusieurs phases pour améliorer dans le temps la sécurité et atteindre le niveau de risque choisi dans un temps raisonnable et conformément aux ressources de l’organisation.

## Considération générale regardant l’indentification des mesures

### Paramétrage et validité des résultats

L’outil d’estimation du risque permet, via un paramétrage expert, de régler les effets des mesures mise en œuvre pour les adapter aux scénarios de risque. Ces paramètres ont été discuté et consolidé en réunion d’expert. Par ailleurs, ils ont été peaufinés au cours de nombreuse évaluations effectuées par itrust consulting.

Les résultats obtenus ont été étudiés en collaboration avec les responsables métier et considérés comme plausibles durant la phase de validation.

### Une méthodologie fondée sur la rentabilité

En utilisant la méthodologie implémentée dans l’outil TRICK Service, nous avons pu estimer les réductions de risque induites par la mise en place des mesures de sécurité choisie. Nous avons alors dans un premier temps établi un plan de traitement dans lequel toutes les mesures de sécurité manquantes étaient mise en œuvre durant la même période. A partir de ce premier plan, nous avons alors décidé d’implémenter les mesures dans diverses phases pour des raisons pratiques. Pour ce faire, nous avons considéré la disponibilité des ressources tant financières qu’humaines de l’organisation, les interdépendances entre les diverses mesures à mettre en œuvre ainsi que le ROSI de chacune (retour sur investissement appliqué à la sécurité), et préféré les solutions les plus simples d’implémentation afin d’ordonner de manière logique et pragmatique les mesures en plusieurs phases. Ce travail a été le fruit d’un processus itératif pour aboutir non seulement à un plan de traitement complet mais plausible et réalisable. Dans les sections qui suivent nous présentons ce plan de traitement dans une approche top-down.

## Résumé du plan de traitement

Afin d’atteindre le niveau de sécurité proposé, il est nécessaire de mettre en œuvre une liste de mesures de sécurité. L’efficacité des mesures de sécurité est indiquée dans le tableau suivant. Ce tableau montre pour chaque phase d’implémentation :

* **Les caractéristiques de la phase** :
  + Le début et la fin de la phase ;
  + Le taux d’implémentation de la mesure ;
  + Le nombre de mesures dont le taux d’implémentation, atteint 100 % concernant l’ISO/IEC 27002 à la fin de la phase.
* **La rentabilité des mesures de sécurité envisagées** :
  + L’ALE en k€ à la fin de la phase (Phase « P0 » correspondant à l’ALE actuel avant tout traitement) ;
  + La réduction du risque en k€ (c.-à-d. la différence entre l’ALE de départ et l’ALE après l’implémentation de la phase) ;
  + Le coût moyen annuel de la phase (considérant le coût de set-up, la durée de vie et la maintenance annuelle).
  + Le Retour annuel sur Investissement en Sécurité (ROSI pour Return On Security Investment) en k€. Le ROSI est calculé en déduisant les coûts moyens annuels de mise en œuvre des mesures de sécurité à la réduction annuelle de risque (ΔALE en k€).
  + Le ROSI relatif (%), qui est le ROSI total divisé par le total des coûts d’implémentation.
* **La planification des ressources** :
  + Les coûts de mise en œuvre initiale des mesures de sécurité :
    - les charges de travail en jour-homme en interne ;
    - les charges de travail en jour-homme en externe ;
    - les investissements initiaux pour mettre en place les mesures de sécurité (en kilo euros)
    - le total de cette mise en œuvre en kilo euros.
  + Les coûts récurrents à prévoir pour maintenir les mesures de sécurité :
    - la charge de travail en interne pour la maintenance (en jour-homme) ;
    - la charge de travail en externe pour la maintenance (en jour-homme) ;
    - les investissements récurrents pour la maintenance en kilo euros ;
    - le total des coûts récurrent en kilo euros.
  + Le coût total de la phase qui comprend les diverses charges de travail (interne et externe) et les coûts d’investissement et de maintenance prévus.

Note: ⯍ le taux moyen d’un jour homme pour un interne est **0** € et celui d’un externe de **0** €.

⯍ l Les coûts moyens annuels sont différents de la somme du coût de set-up avec les coûts récurrents, étant donné que la durée de vie est considérée pour chaque investissement.

L’envergure et l’efficacité des différentes phases sont indiquées dans le tableau suivant :

Table 12 : Résumé des caractéristiques des phases d’implémentation

## Augmentation du taux de conformité et rentabilité des phases

La figure suivante montre l’évolution de la rentabilité et de la conformité en fonction des phases de mise en place des mesures de sécurité :

Figure 6 : Rentabilité du plan de traitement des risques

## Détail du plan de traitement

Le tableau suivant donne la liste complète des mesures de sécurité des guidances appartenant aux normes et aux règlements choisis qui ne sont pas encore implémentées. Cette liste est regroupée par phase d’implémentation, puis triée par rentabilité. Cette liste est appelée, suivant ISO/IEC 27001, le plan de traitement des risques. Elle contient un numéro séquentiel, une référence vers la norme d’où la mesure de sécurité provient, une description de ce qui reste à faire, le risque résiduel après implémentation de la mesure (y compris de toutes les mesures précédentes), la rentabilité de la mesure, le coût annuel, le nombre de jours de travail interne et le nombre de jours de consultance externe pour initier la mesure et le budget d’investissement supplémentaire pour la mesure. La dernière colonne permet d’attribuer la phase dans laquelle la mesure est prévue d’être implémentée.

Table 13 : Plan de traitement du risque selon TRICK Service

# Acceptation du risque

Cette phase consiste à accepter les risques résiduels et s’assurer que le risque actuel sera réduit à ce niveau de risques résiduels d’une manière convenable. Cette décision inclut l’acceptation du plan de traitement des risques, ce qui signifie accepter estimation des ressources nécessaires et l’engagement de fournir ces ressources pour permettre la mise en œuvre du plan comme prévu.

Cette décision doit être formellement documenté dans un document ad-hoc.

# Boucle de rétroaction du processus d’appréciation des risques

## Communication et consultation sur les risques

Le présent rapport en son entièreté ou en parti doit être utilisé pour échanger des informations relatives au risque de l’organisation. La stratégie de communication n’est pas incluse dans ce rapport.

## Surveillance et revue des risques

Ce processus n’est pas documenté dans ce rapport. La surveillance et la revue des risques doit consister à mettre à jour ce rapport au moins annuellement et à chaque fois qu’un changement important et des risques importants apparaissent au sein de l’organisation.

# Niveau d’implémentation

Ce chapitre donne des informations complémentaires sur la manière dont se déroule l’appréciation des risques. Il décrit le modus operandi pour établir quelles mesures de sécurité doivent être appliquées pour améliorer la sécurité de l’information à savoir :

1. Comment identifier les mesures de sécurité à implémenter pour assurer la sécurité de l’information de l’organisation conformément aux normes, règlements et bonnes pratiques applicables.
2. Comment apprécier le niveau actuel d’implémentation de ces mesures.
3. Comment apprécier les ressources nécessaires (calculé en kilo euros) pour implémenter complétement ces mesures au sein de l’organisation.

Tous ces éléments ont été utilisés pour établir le plan de traitement et permettre de décrire l’ »évolution de la conformité de l’organisation en matière de sécurité tout au long des phases du plan de traitement.

## Modus operandi

Pour identifier les mesures de sécurité, évaluer à la fois le niveau d’implémentation actuelle et les ressources nécessaires pour leur pleine mise en œuvre, le consultant a renseigné dans l’outil TRICK Service, pour une liste exhaustive de mesures de sécurité choisi dans les normes, règlements ou bonnes pratiques de sécurité, les informations suivantes :

* **Ref** : La référence des mesures de sécurité ;
* **Domain** : Le domaine (et son titre) ;
* **ST** : Le statut (**AP** : applicable, **NA**: non applicable, **OB** : obligatoire) ;
* **TI** : Le taux d’implémentation actuel (indiquant l’estimation de l’application actuelle de la mesure déterminée lors de l’audit). L’échelle utilisée pour estimer le taux d’implémentation d’une mesure est la suivante :

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Description | Critère de détermination |
| Taux d’implémentation | **0%** | La mesure n’est pas implémentée ni même prise en compte dans la manière de mettre en œuvre la sécurité dans le domaine considéré. | Absence totale de considération et d’implémentation de la mesure. |
| **20%** | La mesure a été considérée dans la mise en œuvre de la sécurité, mais est implémentée de manière informelle. | Considération au niveau du plan de sécurisation. Présence de mesures techniques non structurées (professionnalisme) |
| **50%** | L’implémentation de la mesure a été décidée et une implémentation structurée a été commencée de manière substantielle. | Plan d’implémentation de la mesure existant. Les éléments les plus importants ont été mis en place selon le plan. |
| **80%** | La mesure est implémentée conformément aux décisions, mais l’implémentation n’est pas achevée ou la gestion à long terme doit être vérifiée et consolidée. | Implémentation de la mesure conforme aux décisions du plan et pratiquement achevée. Finalisation et vérification à faire. |
| **100%** | L’implémentation de la mesure est achevée et gérée de manière pérenne conformément au plan de sécurité décidé dans le domaine considéré. | Mise en œuvre de la mesure conforme aux décisions d’implémentation de la sécurité, fiabilisée et sous contrôle. |

Table 14 : Échelle d’implémentation des mesures de sécurité

* **CTI** : Le set-up interne, indiquant combien de jours de travail interne sont nécessaires pour mettre en œuvre la mesure ;
* **CTE** : Le set-up externe indiquant combien de jours de travail d’une personne externe sont nécessaires pour mettre en œuvre la mesure ;
* **INV** : L’investissement indiquant quel budget est à prévoir en supplément des ressources internes et externes pour implémenter la mesure ;
* **LT** : Le lifetime, la durée de vie de la mesure ;
* **MI** : La charge de travail interne pour maintenir la mesure ;
* **ME** : La charge de travail externe pour maintenir la mesure ;
* **IR** : L’investissement annuel à faire pour maintenir la mesure ;
* **CS** : Le coût annuel calculé à partir des paramètres précédents (en tenant compte du coût moyen d’un jour interne, ce taux incluant la coordination avec les ressources internes).
* **Comment**: justification de l’estimation effectuée ;
* **To do**: une description des actions qui doivent être effectuée pour atteindre la conformité maximale.

Le tableau complet des mesures se trouve à la section *Annexe : Liste des mesures de sécurité applicables à la TOE*

## Evolution du niveau de conformité de l’organisation

### Niveau de conformité ISO/IEC 27001

Cette section présente le résultat des estimations du taux de conformité vis-à-vis aux exigences de la norme ISO/IEC 27001. Les numéros représentent les différents chapitres de la norme. Le graphique suivant donne la moyenne du taux de conformité pour chaque chapitre.

Figure 7 : Taux de conformité ISO/IEC 27001 pendant les différentes phases d’implémentation

### Niveau de conformité ISO/IEC 27002

Similaire à la section précédente, on a estimé le taux de conformité à la norme ISO/IEC 27002. La figure suivante présente le niveau de conformité actuelle selon les grands domaines de la sécurité des systèmes d’information :

Figure 8 : Taux de conformité ISO/IEC 27002 pendant les différentes phases d’implémentation

# Annexe : Liste des mesures de sécurité applicables à la TOE

Les tableaux suivants résument pour chaque mesure de sécurité l’état d’implémentation et la charge de travail pour l’implémenter les mesures à 100%.

Le taux d’implémentation et le coût pour les mesures qui n’étaient pas complètement en place ont été estimés.

Pour chacune des mesures de sécurité, nous indiquons :

* **Ref** : La référence ;
* **Domain** : Le domaine (et son titre) ;
* **ST** : Le statut / état (AP : applicable, NA : non applicable, OB : obligatoire) ;
* **TI** : Le taux d’implémentation actuel (indique l’estimation de l’application actuelle de la mesure exprimée en pourcentage) ;
* **CTI** : La charge de travail interne, indique combien de jours de travail d’une personne interne sont nécessaires pour mettre en œuvre la mesure ;
* **CTE** : La charge de travail externe, indique combien de jours de travail d’une personne externe sont nécessaires pour mettre en œuvre la mesure ;
* **INV** : L’investissement, indique quel budget est à prévoir en supplément des ressources internes et externes pour implémenter la mesure ;
* **LT** : Le Lifetime la durée de vie de la mesure (si la valeur est à zéro, l’outil prend par défaut 5 ans) ;
* **MI** : La charge de travail interne pour maintenir la mesure en place ;
* **ME** : La charge de travail externe pour maintenir la mesure en place ;
* **IR** : L’investissement annuel à faire pour maintenir la mesure en place (IR) ;
* **CS** : Le coût annuel, calculé à partir des paramètres précédents (en tenant compte du coût moyen d’un jour interne (0 €) et d’un jour externe (0 €, ce taux inclus la coordination avec les ressources internes) ;
* **Comment**: justification des estimations ;
* **To do**: une description des actions à réaliser pour être conforme ;
* **Resp**: La personne responsable de l’implémentation de la mesure de sécurité.

1. Par exemple lors d’un processus de certification ISO 27001. [↑](#footnote-ref-1)