|  |
| --- |
|  |
| Nom de l’organisation |
| Titre du projet |
| Rapport d’appréciation et de traitement des risques |

Informations générales

|  |  |
| --- | --- |
| Numéro de séquence | Q041 |
| Version | 0.5 |
| État | Final |
| Approuvé par | … |
| Date d’approbation | dd/mm/yyyy |
| Classification | Interne |

Liste de distribution

|  |  |  |
| --- | --- | --- |
| Destinataire | Canal | Raison |
| … | Par email | Validation |
| … | Par email | Validation |

Historique

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Auteur | Modifications |
|  | … | … |  |

Groupe de travail

|  |  |
| --- | --- |
| Nom | Entité |
| Groupe de travail client (List with the first letter of surname and name) | Client |
| Groupe de travail itrust (List with the first letter of surname and name) | itrust consulting |

Approbations

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

Sommaire analytique

Contexte

Le présent rapport présente les résultats de l’appréciation qualitative des risques réalisée par Name of the consultant. Ce projet avait pour but d’établir une appréciation détaillée des risques ainsi qu’un plan de traitement des risques pour améliorer le niveau de sécurité dans les années à venir. Cette analyse des risques suit la norme ISO/IEC 27005 de gestion des risques et a été menée avec l’aide de l’outil TRICK Service développé par itrust consulting.

Envergure

Le périmètre de l’analyse des risques est constitué de  Summary of the scope

Résultats et limitations

En accord avec Client, le résultat de l’analyse effectuée est considéré comme suffisante pour implémenter un plan de traitement et accepter le risque résiduel. Cependant, ces résultats devront être contrôler de manière périodique pour demeurer l’image fidèle des risques de l’organisation.

Plan de traitement du risque

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

Matrice des risques

Table des matières

[1 Introduction 6](#_Toc472584714)

[1.1 Contexte 6](#_Toc472584715)

[1.2 Objectifs du document 6](#_Toc472584716)

[1.3 Cadre d’application 6](#_Toc472584717)

[1.4 Audience 6](#_Toc472584718)

[1.5 Structure de ce document 6](#_Toc472584719)

[1.6 Références 6](#_Toc472584720)

[1.7 Acronymes 7](#_Toc472584721)

[1.8 Terminologie 7](#_Toc472584722)

[2 Méthodologie et déroulement de l’étude 9](#_Toc472584723)

[2.1 Établissement du contexte 10](#_Toc472584724)

[2.1.1 Considérations générales 10](#_Toc472584725)

[2.1.2 Critères de base 10](#_Toc472584726)

[2.1.3 Caractéristiques, contraintes et planification 11](#_Toc472584727)

[2.2 Appréciation des risques 11](#_Toc472584728)

[2.2.1 Plan des réunions 11](#_Toc472584729)

[2.2.2 Identification des risques 11](#_Toc472584730)

[2.2.3 Analyse des risques 13](#_Toc472584731)

[2.2.4 Évaluation des risques 15](#_Toc472584732)

[2.3 Traitement des risques 16](#_Toc472584733)

[2.3.1 Plan de traitement des risques 16](#_Toc472584734)

[2.4 Acceptation des risques 17](#_Toc472584735)

[2.5 Communication relative aux risques 17](#_Toc472584736)

[2.6 Surveillance et revue des risques 17](#_Toc472584737)

[3 Niveau d’implémentation ISO/IEC 27001 et ISO/IEC 27002 18](#_Toc472584738)

[3.1 Méthodologie 18](#_Toc472584739)

[3.2 Niveau de conformité 19](#_Toc472584740)

[Annexe A : Détails de l’analyse des risques 21](#_Toc472584741)

[Annexe B : État d’implémentation des normes et bonnes pratiques considérées 22](#_Toc472584742)

Liste des figures

[Figure 1 : Processus de gestion des risques ISO/IEC 27005 9](#_Toc472584743)

[Figure 2 : Risk Heat Map 14](#_Toc472584744)

[Figure 2 : Nombre de risques faibles, moyens, hauts, critiques par actif 14](#_Toc472584745)

[Figure 3 : Nombre de risques faibles, moyens, hauts, critiques par type actif 14](#_Toc472584746)

[Figure 4 : Nombre de risques faibles, moyens, hauts, critiques par scénario de risque 15](#_Toc472584747)

[Figure 5 : Nombre de risques faibles, moyens, hauts, critiques par type de scénario de risque 15](#_Toc472584748)

[Figure 6 : Taux de conformité ISO/IEC 27001 pendant les différentes phases d’implémentation 19](#_Toc472584749)

[Figure 7 : Taux de conformité ISO/IEC 27002 pendant les différentes phases d’implémentation 20](#_Toc472584750)

Liste des tableaux

[Tableau 1 : Seuil d’acceptation des risques 11](#_Toc472584751)

[Tableau 2 : Considérations générales sur l’envergure de l’analyse de risque 11](#_Toc472584752)

[Tableau 3 : Liste des réunions d’experts dans le contexte de l’appréciation des risques 11](#_Toc472584753)

[Tableau 4 : Liste des actifs appartenant au domaine d’application de l’analyse des risques 12](#_Toc472584754)

[Tableau 5 : Liste des actifs non considérés appartenant au domaine d’application de l’analyse des risques 12](#_Toc472584755)

[Tableau 6 : Échelle de niveau d’exposition 12](#_Toc472584756)

[Tableau 7 : Cartographie des menaces 12](#_Toc472584757)

[Tableau 8 : Liste des vulnérabilités 13](#_Toc472584758)

[Tableau 9 : Spécificités des risques 13](#_Toc472584759)

[Tableau 10 : Scénarios de risques considérés 13](#_Toc472584760)

[Tableau 11 : Échelle de probabilité d’un scénario de risque 13](#_Toc472584761)

[Tableau 12 : Échelle d’impact d’un scénario de risque 13](#_Toc472584762)

[Tableau 13 : Résumé des caractéristiques des phases d’implémentation 16](#_Toc472584763)

[Tableau 14 : Plan de traitement du risque selon TRICK Service 17](#_Toc472584764)

[Tableau 15 : Échelle d’implémentation des mesures de sécurité 18](#_Toc472584765)

# Introduction

## Contexte

L’implémentation de mesures de sécurité, en particulier dans le cas de la mise en œuvre d’un SMSI, nécessite de réaliser une appréciation des risques pour adapter la sécurité à l’état réel des menaces, aux exigences métier ou légales en matière de sécurité et ce en lien avec l’appétence au risque de l’organisation. Dans cette optique, Client a décidé de réaliser une analyse de risque conforme aux guidances de la norme ISO 27005 en utilisant l’outil d’appréciation des risques mis au point par itrust consulting TRICK Service.

## Objectifs du document

Le présent rapport fournit les résultats publiés de l’appréciation des risques réalisée par Name of the consultant. La version à jour et applicable de cette appréciation des risques peut être consultée en utilisant l’application web TRICK Service.

## Cadre d’application

L’appréciation des risques couvre les risques portant sur Summary of the scope.

## Audience

Ce rapport est destiné aux dirigeants de l’organisation, aux propriétaires des risques et à tout le personnel concerné par la mise en œuvre de la sécurité.

## Structure de ce document

Le rapport est structuré en plusieurs chapitres :

Le chapitre 2 décrit la méthodologie utilisée pour mener cette appréciation des risques ;

Le chapitre 3 renseigne sur le contexte, la cible de l’analyse et les actifs pris en considération dans l’analyse ;

Le chapitre 4 présente les résultats de l’appréciation des risques ;

Le chapitre 5 présente le plan de traitement des risques ;

Le chapitre 6 et 7 donnent les informations réglementaires sur le l’acceptation du risque et la boucle de rétroaction inclus dans le processus de gestion des risques ;

LE chapitre 8 décrit l’implémentation actuelle et future ainsi que le niveau de conformité par rapport aux normes et règlements considérés.

L’annexe A inclut les détails de l’analyse des risques en indiquant les actifs, les scénarios de risques ainsi que les résultats de l’estimation des vraisemblances et impacts d’occurrence des scénarios de risques.

L’annexe B 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 — Gestion des risques liés à la sécurité de l'information.

## Acronymes

|  |  |
| --- | --- |
| ISO | International Organization for Standardization |
| IEC | International Electrotechnical Commission |
| TRICK | Tool for RIsk management based on Central Knowledge base |

## Terminologie

|  |  |
| --- | --- |
| Acceptation du risque | Processus destiné à valider le traitement du risque mise en place pour obtenir un risque acceptable pour les parties prenantes c’est-à-dire à valider formellement les mesures mises en place pour traiter le risque et à accepter les risques résiduels. |
| Analyse des risques | Processus mis en œuvre pour comprendre la nature d’un risque et pour déterminer le niveau de risque.  Note 1 : L’analyse des risques fournit la base de l’évaluation du risque et les décisions relatives au traitement des risques.  Note 2 : L’analyse des risques inclut l’estimation des risques. |
| Appréciation du risque | Ensemble du processus d’identification des risques, d’analyse des risques et d’évaluation du risque. |
| Communication et concertation relatives aux risques | Processus itératifs et continus mis en œuvre par une organisation afin de fournir, partager ou obtenir des informations et d’engager un dialogue avec les parties prenantes concernant la gestion des risques. |
| Conséquence | Effet d’un événement affectant les objectifs.  Note 1 : Un événement unique peut engendrer des conséquences multiples.  Note 2 : Une conséquence peut être certaine ou incertaine et dans le cadre de la sécurité de l’information elle est généralement négative.  Note 3 : Les conséquences peuvent être exprimées de façon qualitative ou quantitative.  Note 4 : Des conséquences initiales peuvent déclencher des réactions en chaîne.  Note 5 : Conséquence est également utilisée comme synonyme d’impact. |
| Critères du risque | Termes de référence vis-à-vis desquels le caractère significatif d’un risque est évalué. |
| Évaluation du risque | Processus de comparaison des résultats de l’analyse des risques avec les critères de risque afin de déterminer si les risques et/ou leur importance sont acceptables ou tolérables.  Note : L’évaluation du risque aide à la prise de décision relative au traitement des risques. |
| Événement | Occurrence ou changement d’un ensemble particulier de circonstances.  Note 1 : Un événement peut être unique ou se reproduire, et peut avoir plusieurs causes.  Note 2 : Un événement peut consister en quelque chose qui ne se produit pas.  Note 3 : Il peut parfois être fait référence en tant qu’« incident » ou « accident ». |
| Identification du risque | Processus de recherche, de reconnaissance et de description des risques.  Note1 : L’identification des risques comprend l’identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentielles.  Note2 : L’identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis d’experts et autres personnes compétentes et tenir compte des besoins des parties prenantes. |
| MAGERIT | Méthodologie d’analyse des risques publiée par le gouvernement espagnole. |
| Mesure de sécurité | Mesure qui modifie un risque.  Note 1 : Une mesure de sécurité du risque en sécurité de l’information inclut n’importe quel processus, politique, procédure, recommandation, dispositif pratique ou organisation, qui peut être d’ordre administratif, technique, managérial ou juridique et qui modifie le risque en sécurité de l’information.  Note 2 : Une mesure de sécurité du risque n’aboutit pas toujours à la modification voulue ou supposée.  Note 3 : Une mesure de sécurité du risque est également utilisée comme synonyme de protection ou contre-mesure. |
| Niveau de risque | Importance d’un risque, exprimée en termes de combinaison des conséquences et de leur vraisemblance. |
| Partie prenante | Personne ou organisation susceptible d’affecter, d’être affectée ou de sentir elle-même affectée par une décision ou une activité.  Note : Un décideur peut être une partie prenante. |
| Risque | Effet de l’incertitude sur l’atteinte des objectifs. |
| Risque résiduel | Risque subsistant après le traitement des risques.  Note 1 : Un risque résiduel peut inclure des risques non identifiés.  Note 2 : Un risque résiduel peut également être appelé « risque maintenu ». |
| 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 au domaine d’application. |
| Traitement des risques | Processus destiné à modifier un risque. |
| TRICK Service | Outil d’appréciation des risques de la société itrust consulting. |
| Vraisemblance | Possibilité que quelque chose se produise.  Note : Dans la terminologie de la gestion des risques, le mot « vraisemblance » est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu’elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée). |

# 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 1 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 et ).

#### 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 inclue 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. Résultats du « brainstorming » destiné à mettre en lumière le niveau d’exposition des actifs aux menaces, vulnérabilités courantes ainsi qu’à une liste de risques génériques.
4. Étude du niveau actuel d’implémentation des spécifications et mesures de sécurité préconisées par les référentiels suivants :
   1. ISO 27001
   2. ISO 27002
5. Analyse qualitative des risques liés aux actifs considérés ;
6. Identification des mesures de sécurité permettant de modifier le niveau des risques pour atteindre le niveau acceptable des risques et estimation des coût d’implémentation de ces mesures ;
7. Validation des résultats ;
8. Validation du plan de traitement des risques ;
9. Résumé et présentation des conclusions.

# Contexte du risque

Cette section documente les critères de base de l’évaluation des risques, la cible et le périmètre de l’appréciation des risques, ainsi que le processus de gestion des risques sous-jacent.

## 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 qualitative des risques par les actifs principaux avec TRICK Service.
3. Évaluation du niveau d’implémentation des mesures de sécurité et estimation des coûts pour atteindre une conformité complète.
4. 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 exigences légales, réglementaires et contractuelles ;
* 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 considérant des catégories d’impact ainsi que des niveaux d’impacts. Lors de l’estimation des impacts, trois critères de sécurité sont considérés pour les actifs à savoir la confidentialité, l’intégrité et la disponibilité. Cependant d’autres aspectes peuvent être envisagés lors de l’estimation comme la perte d’image ou les conséquences légales ou contractuelles des incidents.

Les types d’impacts considérés dans cette analyse sont :

### Critères d’acceptation du risque

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

Table 1: Critères acceptation des risques

## 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 2 : 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. dd/mm/yy 2. dd/mm/yy 3. dd/mm/yy |
|  |  | 1. dd/mm/yy 2. dd/mm/yy 3. dd/mm/yy |
|  |  | 1. dd/mm/yy 2. dd/mm/yy 3. dd/mm/yy |

Table 3: 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 4 : 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 5 : 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 spécifiques

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 : Spécificités 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 A pour les informations détaillées).

### 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

Pour chaque scénario, il revient au consultant en relation avec les responsable métiers d’estimer les risques de manière qualitative l’impact et la vraisemblance du scénario afin déterminer le risque. Pour ce faire, les échelles d’impact et de vraisemblance suivantes seront utilisées :

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

Les résultats de l’analyse des risques sont exprimés en utilisant une matrice des risques. Cette matrice permet de représenter de manière graphique le niveau de risque atteint par l’organisation en précisant le nombre d’actifs concernés par ce niveau de risque et ce en fonction de la valeur de l’impact et de sa vraisemblance. Des informations détaillées quant au risque pour chaque actif, présentant le niveau d’impact et la vraisemblance sont reporté dans l’Annexe A : Détails de l’analyse des risques.

Figure 2: Matrice des risques

### 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 3 and Figure 4) et d’autre part quels scenarios ou quel type de scenarios sont les plus à même de conduire à ces risques (Figure 5 and Figure 6)

Figure 3: Evaluation des risques par actif

Figure 4: Evaluation des risques par type d’actif

Figure 5: Evaluation des risques par scénario

Figure 6: Evaluation des risques par type de scénario

## 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 3.2.3).

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 inclue 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.

## 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 27002 à la fin de la phase.
* **Le coût moyen annuel de la phase** (considérant le coût de set-up, la durée de vie et la maintenance annuelle).
* **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

## 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 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 des risques

Cette phase correspond au processus d’acceptation du risque résiduel et à celui et concomitamment à celui d’approbation que le risque actuel a été réduit à ce niveau d’une manière adéquat. Cette décision inclue donc l’acceptation du plan de traitement et l’engagement de mettre en œuvre les ressources nécessaires à son effectuation dans les délais établis par ce plan.

# Boucles de rétroaction du processus d’appréciation des risques

## Communication sur les risques

Le présent rapport ou des éléments spécifiques de celui-ci sont utilisés pour communiquer sur les risques. La stratégie de communication sous-jacente n’est cependant pas partie intégrante de ce rapport.

## Surveillance des risques et revue des risques

Ce processus n’est pas partie intégrante de ce rapport. La surveillance des risques et la revue de ceux-ci consistent à mettre à jour ce rapport de manière régulière, au moins annuellement, ou en cas de changement significatif du périmètre ou identification de risques importants non encore considérés.

# 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 15 : 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 B : État d’implémentation des normes et bonnes pratiques considérées*

## 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 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 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 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 27002 pendant les différentes phases d’implémentation

# Annexe A : Détails de l’analyse des risques

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

* De l’impact quand la menace se produit sur l’actif ;
* De la probabilité annuelle d’occurrence de la menace.

Le niveau d’importance d’une paire actif-menace est calculé en multipliant l’impact maximal et la probabilité de la paire.

# Annexe B : État d’implémentation des normes et bonnes pratiques considérées

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 (500 €) et d’un jour externe (1000 €, 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)