|  |
| --- |
| *Inclure votre logo ici* |
| Nom de l’organisation |
| Titre du projet |
| Rapport d’appréciation et de traitement des risques |

Informations générales

|  |  |
| --- | --- |
| Numéro de séquence | … |
| Version | 0.1 |
| État | Brouillon |
| Approuvé par | … |
| Date d’approbation | dd/mm/yyyy |
| Classification | Confidentiel/Restreint/Interne/Publique |

Liste de distribution

|  |  |  |  |
| --- | --- | --- | --- |
| Destinataire | Date | Canal | Raison |
| … | dd/mm/yy | Choisir | Choisir |

Historique

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Auteur | Modifications |
| 0.1 | dd/mm/yy | … | Rapport exporté de TRICK Service |
|  |  |  |  |
|  |  |  |  |

Groupe de travail

|  |  |
| --- | --- |
| Nom | Entité |
| *Nom des personnes du groupe de travail* | … |

Approbations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom | Rôle | Responsabilité | Date | Signature |
| … | Choisir | Choisir | dd/mm/yy |  |
| … | Choisir | Choisir | dd/mm/yy |  |

Sommaire analytique

Contexte

Le présent rapport inclut les résultats de l’appréciation et du traitement des risques effectué par …. L’appréciation des risques a été menée avec l’aide de l’outil TRICK Service développé par itrust consulting.

Envergure

…

Résultats et limitations

…

Plan de traitement du risque

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

Phase 1 : cette phase correspond au … trimestre de l’année … et implémente … mesures pour une charge de travail de … jours internes et de … jours externes ;

Phase 2 : cette phase correspond au … trimestre de l’année … et implémente … mesures pour une charge de travail de … jours internes et de … jours externes ;

….

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

Le présent document inclut un rapport sur la gestion des risques de … sur la période d’activité ….

## Objectifs du document

Le rapport décrit la démarche et présente les résultats de l’appréciation et du traitement des risques mené par ….

## Cadre d’application

L’appréciation des risques couvre les risques portant sur ….

## Audience

Ce rapport est adressé à …

## Structure de ce document

Le rapport est structuré en plusieurs chapitres :

* Le chapitre 2 décrit la démarche et présente les résultats de l’appréciation et du traitement des risques.
* Le chapitre 3 renseigne sur le niveau de conformité par rapport aux normes ISO/IEC 27001 et ISO/IEC 27002.
* 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, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences.
2. ISO/IEC 27002, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information.
3. ISO/IEC 27005, 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’étude

L’appréciation et le traitement des risques a été réalisée en suivant le processus de gestion des risques en sécurité de l’information ISO/IEC 27005 (voir figure ci-dessous).



Figure 1 : Processus de gestion des risques ISO/IEC 27005

La démarche suivante a été considérée :

1. Description du domaine d’application et des limites de l’appréciation des risques ;
2. Identification des actifs qui font partie du domaine d’application ;
3. Analyse de base sur l’exposition à des menaces et vulnérabilités typiques ainsi qu’à des spécificités de risques ;
4. Identification et analyse des mesures de sécurité existantes ;
5. Analyse qualitative des risques liés aux actifs considérés faisant partie du domaine d’application ;
6. Identification de mesures de sécurité modifiant le niveau de risques et estimation des coûts d’implémentation ;
7. Validation des résultats de l’appréciation des risques ;
8. Validation du plan de traitement des risques ;
9. Résumé et présentation des conclusions.

## Établissement du contexte

Ce processus vise à spécifier les critères de base, le domaine d’application et l’organisation du processus de gestion des risques.

### Considérations générales

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

1. Identification de risques de base 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 actif avec TRICK Service.
3. Identification des mesures de sécurité existantes et estimation des coûts pour finaliser la mise en place des mesures en cours d’implémentation et de nouvelles mesures identifiés.
4. Priorisation des mesures de sécurité en vue d’établir un plan de traitement des risques.

### Critères de base

#### Critères d’évaluation des risques

Les risques sont évalués en considérant :

* L’importance des informations pour assurer le fonctionnement de l’activité afférente au domaine d’application de l’analyse des risques ;
* Les exigences légales, réglementaires et les obligations contractuelles ;
* Les trois aspects de sécurité (confidentialité, intégrité, disponibilité).

#### Critères d’impact

L’impact d’un incident de sécurité est estimé selon des catégories d’impact et suivant des niveaux d’impact.

Les trois volets de la sécurité, la confidentialité, l’intégrité, et la disponibilité sont considérés.

Les types d’impacts considérés dans cette analyse sont :

#### Critères d’acceptation du risque

Les critères d’acceptation du risque sont les suivants :

Tableau 1 : Seuil d’acceptation des risques

### Caractéristiques, contraintes et planification

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

Tableau 2 : Considérations générales sur l’envergure de l’analyse de risque

## Appréciation des risques

Ce processus se décompose en trois phases distinctes permettant d’identifier, d’analyser et d’évaluer les risques.

### Plan des réunions

L’appréciation des risques a été réalisée pendant des réunions d’experts. Le tableau suivant énumère les différentes entrevues qui ont été organisées dans le contexte de l’appréciation des risques.

|  |  |  |
| --- | --- | --- |
| Service | Participants | Date(s) entrevue(s) |
| Service HR | Monsieur X, Madame Y | Dd/mm/yyyy, dd/mm/yyyy |
| … | … | … |
|  |  |  |
|  |  |  |
|  |  |  |

Tableau 3 : Liste des réunions d’experts dans le contexte de l’appréciation des risques

### 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 ;
2. Identification des menaces, des vulnérabilités et des spécificités des risques (brainstorming) ;
3. Identification des mesures de sécurité existantes (voir Annexe B) ;
4. Analyse des impacts que des pertes de confidentialité, d’intégrité et de disponibilités peuvent avoir sur les actifs considérés (voir les détails de l’analyse des risques dans l’Annexe A).

#### Identification des actifs

Le tableau suivant fournit l’inventaire des actifs considérés pendant l’appréciation des risques.

Note : Ce tableau contient déjà l’indication du niveau de risque tel qu’il est estimé au chapitre suivant.

Tableau 4 : Liste des actifs appartenant au domaine d’application de l’analyse des risques

Le tableau suivant énumère tous les actifs qui n’ont pas été considérés pendant l’appréciation des risques.

Tableau 5 : Liste des actifs non considérés appartenant au domaine d’application de l’analyse des risques

#### Brainstorming

Avant d’analyser les risques, il est important d’identifier les menaces, vulnérabilités et spécificités de risques auxquelles le domaine d’application est exposé. La liste des menaces, vulnérabilités et spécificités de risques abordées ont été cartographiées selon la méthode MAGERIT.

L’échelle suivante a été utilisée pour exprimer l’exposition du domaine d’application de l’analyse des risques :

|  |  |
| --- | --- |
| Exposition | |
| **Symbole** | **Description** |
| - - | Très faible |
| - | Faible |
| N | Normale |
| + | Importante |
| + + | Très importante |

Tableau 6 : Échelle de niveau d’exposition

##### Cartographie des menaces

Une vulnérabilité peut seulement devenir un risque s’il existe des menaces qui l’exploitent. Ainsi il est très important de connaître les menaces auxquelles on est exposé. Le tableau suivant donne un aperçu de cette cartographie et des niveaux d’expositions.

Tableau 7 : Cartographie des menaces

…

##### Liste 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. Le tableau suivant donne un aperçu de la liste des vulnérabilités et des niveaux d’expositions.

Tableau 8 : Liste des vulnérabilités

…

##### Spécificités 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 du domaine d’application. Cette évaluation considère non seulement la force et la fréquence de la menace, mais aussi le niveau de vulnérabilité des actifs ciblés.

Tableau 9 : Spécificités des risques

…

### Analyse des risques

L’analyse des risques inclut plusieurs phases :

1. Le choix de la méthodologie.
2. L’estimation des conséquences selon une échelle définie.
3. L’estimation des probabilités d’occurrences selon une échelle définie.
4. L’estimation du niveau de risque (voir Annexe A pour le détail).

#### Scénarios de risques et échelles de probabilité et d’impact

Dans la prochaine étape, les risques ont été qualifiés avec la méthode TRICK d’itrust consulting pour 8 scénarios de risques génériques. Ces risques sont des scénarios d’attaque qui reprennent les menaces et vulnérabilités essentielles en relation avec les 3 critères de sensibilité de l’information : Confidentialité, Intégrité, et Disponibilité.

Le tableau suivant présente les scénarios de risques considérés pendant l’analyse des risques.

Tableau 10 : Scénarios de risques considérés

Les tableaux suivants présentent les échelles de probabilité et d’impacts utilisées pour apprécier la vraisemblance d’occurrence et les conséquences d’un risque.

Tableau 11 : Échelle de probabilité d’un scénario de risque

Tableau 12 : Échelle d’impact d’un scénario de risque

#### Résumé du niveau actuel des risques

Les niveaux de risques par actifs, type d’actif, scénarios de risques et type de scénario de risque sont résumés dans les figures suivantes.

Figure 2 : Risk Heat Map

Figure 3 : Nombre de risques par actif

Figure 4 : Nombre de risques par type actif

Figure 5 : Nombre de risques faibles, moyens, hauts, critiques par scénario de risque

Figure 6 : Nombre de risques faibles, moyens, hauts, critiques par type de scénario de risque

### Évaluation des risques

Cette phase permet de comparer les résultats de l’analyse des risques avec les critères d’acceptation du risque fixés avec les parties prenantes (voir ch. 2.1.2).

Les risques évalués comme non-acceptables doivent être modifiés en définissant un plan de traitement des risques.

## 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 décideurs de l’organisation.

### Plan de traitement des risques

Afin de traiter les risques identifiés lors de ce projet et qualifiés pour un traitement, une liste d’actions destinées à être implémentées a été dressée. 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. La mise en œuvre de cette liste d’action permettra de réduire les risques à un niveau acceptable.

#### Caractéristiques du plan de traitement des risques

Le tableau suivant 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 % à la fin de la phase.
* Le coût moyen annuel de la phase en considérant le coût d’implémentation, la durée de vie et la maintenance annuelle des mesures de sécurité.
* La planification des ressources : les charges de travail en jour-homme et le coût en kilo-euros de toutes les mesures de sécurité de la phase (pour la charge de travail interne, la charge de travail externe, l’investissement, la maintenance interne, la maintenance externe, les coûts additionnels de maintenance et finalement le coût total (... €/jour pour le personnel interne et … €/jour pour le personnel externe, incluant le coût de gestion interne).

Tableau 13 : Résumé des caractéristiques des phases d’implémentation

#### Le détail du plan de traitement des risques

Le tableau suivant donne la liste complète des mesures de sécurité planifiées à être implémentées pour traiter les risques identifiés comme non-acceptables. Cette liste est regroupée par phase d’implémentation. Cette liste est appelée, suivant ISO/IEC 27001, le plan de traitement des risques. Elle contient un numéro séquentiel, une référence vers la norme/bonne pratique d’où la mesure de sécurité provient, une description de ce qui reste à faire, 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.

Tableau 14 : Plan de traitement du risque selon TRICK Service

## Acceptation des risques

L’acceptation du risque n’est pas couverte par ce rapport. Il consiste à accepter les risques résiduels et à en assumer la responsabilité. Implicitement, cette décision inclut l’acceptation du plan de traitement des risques, c’est-à-dire l’engagement financier et la délégation des charges afin d’assurer que le plan pourra être mis en œuvre comme planifiée.

La décision doit être formellement enregistrée.

## Communication relative aux risques

Le présent rapport ou des parties du présent rapport sont utilisés pour échanger des informations relatives aux risques. La stratégie de communication ne fait pas partie du présent rapport.

## Surveillance et revue des risques

Cette phase n’est pas incluse dans ce rapport, mais elle consiste à mettre à jour ce rapport, annuellement, et en cas de changements ou de découverte de risques significatifs.

# Niveau d’implémentation ISO/IEC 27001 et ISO/IEC 27002

## Méthodologie

Dans ce chapitre le taux et le coût d’implémentation pour les mesures de sécurité, provenant des normes considérées et qui n’étaient pas complètement implémentées, sont estimés.

Pour chacune des mesures de sécurité, nous indiquons :

* La référence ;
* Le domaine (et son titre) ;
* Le statut (AP : applicable, NA : non applicable, OB : obligatoire) ;
* 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. |

Tableau 15 : Échelle d’implémentation des mesures de sécurité

* La charge de travail interne, indiquant combien de jours de travail interne sont nécessaires pour mettre en œuvre la mesure ;
* La charge de travail externe indiquant combien de jours de travail d’une personne externe sont nécessaires pour mettre en œuvre la mesure ;
* L’investissement indiquant quel budget est à prévoir en supplément des ressources internes et externes pour implémenter la mesure ;
* La durée de vie (lifetime) de la mesure ;
* La charge de travail interne pour maintenir la mesure ;
* La charge de travail externe pour maintenir la mesure ;
* L’investissement annuel à faire pour maintenir la mesure ;
* Le coût annuel calculé à partir des paramètres précédents (en tenant compte du coût moyen d’un jour interne (… €) et d’un jour externe (… €, ce taux incluant la coordination avec les ressources internes).

Le tableau complet des mesures et des estimations se trouve en Annexe B du présent rapport.

## Niveau de conformité

Cette section présente le résultat des estimations du taux de conformité vis-à-vis aux exigences des normes ISO/EC 27001 et ISO/IEC 27002. Les numéros représentent les différents chapitres de la norme. Les graphiques suivants donnent la moyenne du taux de conformité pour chaque chapitre.

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

Figure 8 : Taux de conformité ISO/IEC 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 :

* la référence (Réf) ;
* le titre ;
* le statut/état (AP : applicable, NA : non applicable, OB : obligatoire) ;
* le taux d’implémentation actuel (TI) (indiquant l’estimation de l’application actuelle de la mesure déterminée lors de l’audit, exprimé en pourcentage) ;
* la charge de travail interne (CTI), indiquant combien de jours de travail interne sont nécessaires pour mettre en œuvre la mesure ;
* la charge de travail externe (CTE) indiquant combien de jours de travail d’une personne externe sont nécessaires pour mettre en œuvre la mesure ;
* l’investissement (INV) indiquant quel budget est à prévoir en supplément des ressources internes et externes pour implémenter la mesure ;
* la durée de vie (LT), de la mesure (si 0 est indiqué, l’outil prend par défaut 5 ans) ;
* la charge de travail interne pour maintenir la mesure (MI) ;
* la charge de travail externe pour maintenir la mesure (ME) ;
* l’investissement annuel à faire pour maintenir la mesure (MR) ;

Le coût annuel calculé à partir des paramètres précédents (en tenant compte du coût moyen d’un jour interne (…°€) et d’un jour externe (…°€, ce taux incluant la coordination avec les ressources internes).

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