Aruba Cloud

Gestion du risque pour la sécurité des informations

SOMMAIRE

1 TERMES ET DÉFINITIONS 2
2 LES PRINCIPALES NORMES DE RÉFÉRENCE 5
2.1 ISO/IEC 27001 Standard 5
2.2 ISO/IEC 27002 Standard 5
2.3 ISO/IEC 27005 Standard 6
3 MÉTHODE DE GESTION DES RISQUES POUR LA SÉCURITÉ DES INFORMATIONS 7
4 LE PROCESSUS DE GESTION DES RISQUES 8
4.1 PHASE 1 – Context Establishment 8
4.1.1 Identification des services, des processus et des macro-processus 8
4.1.2 Identification des assets 9
4.1.3 Lien macro-processus – assets 9
4.2 PHASE 2 – Risk Analysis 9
4.2.1 Évaluation des impacts 9
4.2.2 Identification et valorisation des assets 9
4.2.3 Analyse des menaces et évaluation des probabilités d'occurrence 10
4.2.4 Analyse des contre-mesures 10
4.3 PHASE 3 – Risk Evaluation 11
4.3.1 Méthode et modèle du risque 11
4.3.2 Exigences de sécurité applicables et niveau de conformité 11
4.3.3 Calcul des risques élémentaires inhérents et résiduels 11
4.4 PHASE 4 – Risk Treatment 12
4.4.1 Analyse du risque accepté 12
4.4.2 Résultat de l'analyse : risque résiduel AS-IS 12
4.4.3 Analyse des gaps et choix des contre-mesures à mettre en œuvre 12
4.4.4 Plan de Traitement du Risque – Rationalisation des interventions 12
5 FRÉQUENCE D'ANALYSE 13

Aruba S.p.A.
Via San Clemente 53 - 24036 Ponte San Pietro (BG) – n° de TVA: 01573850516
https://www.arubacloud.com - https://www.arubacloud.fr - https://www.arubacloud.es

1 TERMES ET DÉFINITIONS

Le présent chapitre contient certaines des définitions considérées comme importantes pour la représentation du modèle de calcul et de gestion du Risque pour la Sécurité des Informations.

BIA (Business Impact Analysis) **:**

Analyse des impacts économiques, réglementaires et réputationnels pour le Business liés à la perte de Confidentialité, d'Intégrité et de Disponibilité des informations relatives à un processus/service donné et à l'interruption de ce dernier.

Disponibilité :

Garantir que les systèmes d'information et les données requises soient disponibles pour l'utilisation lorsqu'ils sont nécessaires.

Gestion du risque pour la sécurité des informations :

Ensemble d'activités et de processus de business destinés à identifier, mesurer, limiter et surveiller les risques liés à la perte de Confidentialité, d'Intégrité et de Disponibilité (CID) des données et des services.

Impact :

La conséquence négative pour l'entreprise si une ou plusieurs menaces se réalisent.

Incident :

Un évènement lié à la sécurité informatique ayant une probabilité significative de compromettre les opérations de business et/ou de menacer la sécurité des informations.

Intégrité :

Désigne la protection des données et des informations contre les modifications d'un contenu, accidentelles ou volontaires.

Menace :

La cause potentielle (délibérée et accidentelle) d'un incident qui peut endommager un système ou une organisation en générant des impacts sur la **Confidentialité, l'Intégrité et la Disponibilité** des informations.

Les menaces peuvent être :

- De nature « informatique » - elles provoquent des impacts négatifs sur l'entreprise à travers :
  - l'utilisation du système d'information ou de ses composantes (ex : attaque par des hackers) ;
  - la réalisation d'activités de gestion du système d'information (ex : dommages par un personnel interne) ;
- De nature « non informatique » - elles provoquent des impacts négatifs sur le système d'information de l'entreprise à travers :
  - Des impacts directs sur la fourniture des services du système d'information (ex : catastrophes naturelles, interruption des services d'assistance) ;

- Des effets sur les modalités de gestion du système d'information (ex : modalités de mise en œuvre des processus IT).

Pour caractériser les risques associés à chaque menace, il est nécessaire de connaitre :

- Les vulnérabilités des composantes du système d'information, à savoir là où les menaces peuvent se concrétiser ;
- L'exposition des composantes à la menace, à savoir la facilité avec laquelle la menace peut se concrétiser (par exemple, un serveur qui présente un service web aux clients est davantage exposé aux attaques véhiculées par Internet) ;
- Les types de conséquences, étant donné que certaines menaces peuvent être à leur tour « vecteurs » d'autres menaces (par exemple, l'accès non autorisé à un serveur web peut permettre à un intrus de voler des données, mais également de les supprimer, de les altérer, de réaliser des fraudes, etc.).

Possibilité ou probabilité d'occurrence :

La possibilité d'occurrence d'une menace désigne la probabilité qu'une menace se réalise sur une ou plusieurs composantes IT, pour provoquer un impact négatif pour l'entreprise, sur une certaine période.

Risque pour la sécurité des informations (appelé ci-dessous également « risque »)

Il s'agit du produit entre la probabilité que se réalise une menace et l'impact causé à l'entreprise concernant les assets impliqués dans l'analyse. En fonction du moment de mesure, le risque se différencie en :

- Risque potentiel ou risque inhérent (**rRp**) :

  Représente le risque maximal auquel est soumis un certain asset en termes de possibilité de réalisation d'une menace pouvant avoir un impact en cas de perte de Confidentialité, d'Intégrité ou de Disponibilité des informations. Toutes les composantes qui se rapportent au service dans l'analyse contribuent à la détermination du risque inhérent : les processus, les applications, les données, les infrastructures et, non des moindres, les facteurs humains.

  Il est essentiellement représenté par une valeur, différemment calculée selon les méthodes appliquées, résultant de la somme de toutes les menaces possibles auxquelles est soumis un asset, en tenant compte des probabilités d'occurrence respectives et des impacts relatifs.

  En d'autres termes, il s'agit du risque auquel un asset peut être exposé en tenant simplement compte de sa nature et des menaces liées à celui-ci. À titre d'exemple, prenons le cas d'un ordinateur exposé sur le réseau public sans aucune mesure de protection.

- Risque résiduel ou final (**rRf**) :

  Représente le risque observé sur un service à la suite de l'application des contre-mesures visant à entrainer une réduction du risque inhérent.

- Risque Final Acceptable (**rRfa**) :

  Représente la limite maximale de risque acceptable par l'Organisation.

Toutes les valeurs de risque exposées ci-dessus doivent être considérées comme dynamiques, car elles varient au fil du temps, puisqu'elles sont influencées, par exemple, par les éléments suivants :

- Évolution des menaces ;
- Modification des niveaux de service requis ;
- Variation des dispositions légales ou des règlements de référence ;
- Changements organisationnels pouvant avoir des effets sur les faiblesses ou sur la probabilité que se réalise les menaces, ou modifier les impacts conséquents ;
- Renforcement ou Affaiblissement des contre-mesures de sécurité.

Risques Élémentaires :

Il s'agit des risques informatiques pour la sécurité des informations associés à chaque asset et à chaque scénario de risque.

Confidentialité :

Il s'agit de la protection des données et des informations afin de limiter les risques liés à l'accès ou à l'utilisation non autorisée des informations.

RPO (Recovery Point Objective) :

Perte de données admissible, il s'agit de la durée qui s'écoule entre la dernière sauvegarde des données d'un processus et la survenance de l'évènement ayant provoqué l'arrêt du processus.

RTO (Recovery Time Objective) :

Délai après un incident au cours duquel :

- Le Produit ou le Service doivent reprendre, ou
- L'activité doit reprendre, ou
- Les ressources doivent être récupérées.

Scénario de Risque :

Union de deux ou plusieurs menaces permettant la classification de celles-ci.

Vulnérabilité :

Faiblesse intrinsèque d'un processus, d'un service, d'un asset qui, si elle est exploitée par une ou plusieurs menaces, permet la violation des objectifs de Sécurité des Informations (Confidentialité, Intégrité et Disponibilité). Il peut s'agir de :

- Réseaux non segmentés ;

- Utilisation de protocoles privés de protection cryptographique ;
- Systèmes d'exploitation non régulièrement mis à jour ;
- Bases de données avec données « sensitive » non cryptées ;
- Définitions de virus non mises à jour ;
- Accès physiques sans surveillance ;
- Absence de systèmes anti-incendie automatiques ;
- Insuffisance des systèmes d'énergie supplémentaire ;
- Etc.

2 LES PRINCIPALES NORMES DE RÉFÉRENCE

Les principales normes adoptées pour garantir la conformité des activités réalisées aux best practices internationales dans le domaine de la sécurité sont celles décrites aux paragraphes suivants.

2.1 ISO/IEC 27001 Standard

La norme ISO/IEC 27001:2013 constitue, en tant que norme internationale de sécurité, un vrai modèle de référence pour l'évaluation du niveau de sécurité des informations capable d'analyser aussi bien les composantes technologiques que celles organisationnelles qui contribuent à définir un Système de Gestion de la Sécurité des Informations (SGSI).
La norme définit les conditions d'un SGSI et aide à identifier, à gérer et à réduire la variété des menaces auxquelles les informations sont régulièrement soumises. Cette norme fixe également les contrôles de sécurité à adopter pour protéger les informations en sécurisant les parties concernées, y compris les clients de l'organisation.

2.2 ISO/IEC 27002 Standard

La norme ISO/IEC 27002:2013 définit les lignes directrices et les principes généraux destinés à mettre en œuvre un Système de Gestion de la Sécurité des Informations adapté au sein d'une Organisation.
En particulier, la norme ISO/IEC 27002:2013 constitue, en tant que norme internationale de sécurité, un vrai modèle de référence pour l'évaluation des aspects organisationnels, procéduraux, technologiques et règlementaires de la sécurité d'un système d'information réalisée dans le but de :

- Effectuer un examen critique des services et des fonctionnalités que le système en question dispose déjà ou devra disposer ;
- Mettre en évidence les vulnérabilités du système ;
- Indiquer les actions opportunes pour atteindre le niveau de sécurité défini dans les objectifs.

Nous précisons que l'ISO/IEC 27002 identifie les contrôles de sécurité qu'une organisation devrait prendre en compte, mais ne remplace pas l'activité d'Analyse des Risques proprement dite.

2.3 ISO/IEC 27005 Standard

L'ISO/IEC 27005 décrit le processus de gestion du risque en matière de sécurité des informations et les actions associées, en soutenant les principes généraux contenus dans l'ISO/IEC 27001.

La norme – conforme à la norme ISO 31000 – a pour objectif d'aider les entreprises à gérer le risque relatif à la sécurité des informations de manière similaire à la façon dont elles gèrent les autres types de risque.

La Figure 1 représente le schéma proposé par l'ISO/IEC 27005:11 de processus de gestion du risque dont s'inspire le modèle adopté et développé par le Groupe Aruba.

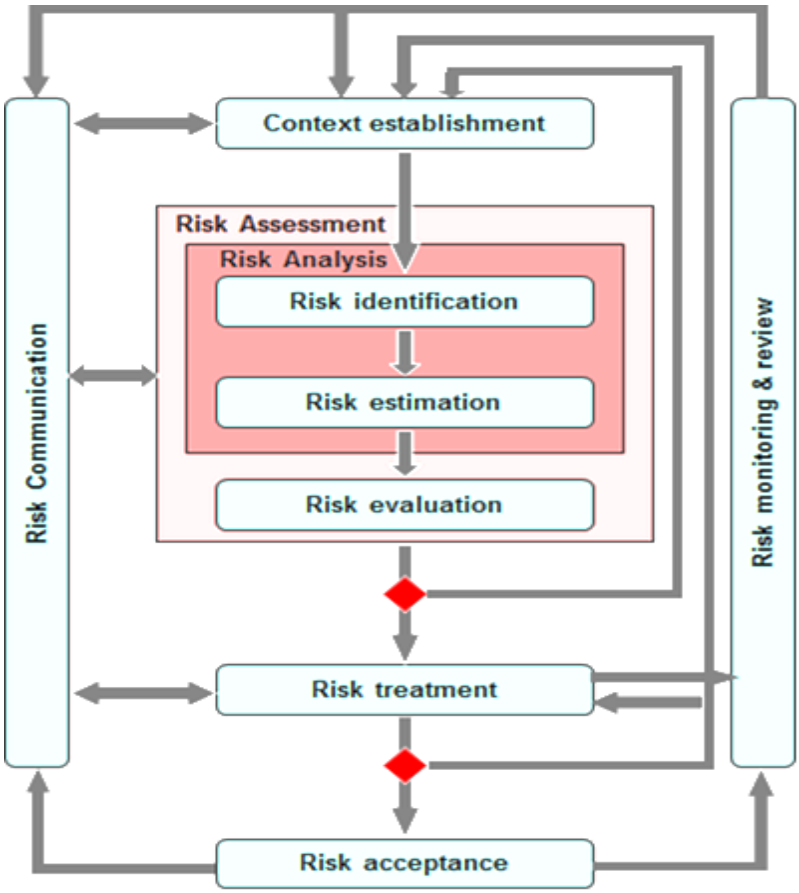

Figure 1 – ISO/IEC 27005 : Processus de gestion du risque

3 MÉTHODE DE GESTION DES RISQUES POUR LA SÉCURITÉ DES INFORMATIONS

Pour le Groupe Aruba S.p.A, l'information représente un patrimoine dont la gestion attentive est stratégique pour la protection et le développement du business d'entreprise.

Dans ce contexte, un risque informatique peut être défini comme tout évènement incertain pouvant compromettre une ou plusieurs des trois principales propriétés suivantes du patrimoine informationnel de l'entreprise :

- **Confidentialité** (les données sont accessibles aux personnes non autorisées) ;
- **Intégrité** (les données peuvent subir des modifications non autorisées et être altérées) ;
- **Disponibilité** (le système d'information n'est pas utilisable) ;

selon les niveaux de gravité dépendant principalement du type des informations impactées.

L'évaluation du risque est effectuée en tenant compte des impacts possibles de type :

- Économique ;
- Réglementaire ;
- Réputationnel.

La gestion des risques relatifs à la sécurité des informations est un processus qui permet d'évaluer les interrelations entre les assets, les menaces et les vulnérabilités concernant une certaine organisation. Ce processus analytique a pour objectif d'identifier les risques associés aux vulnérabilités et aux menaces rencontrées sur les assets et de fournir les bases pour définir un programme de sécurité efficace.

Les catégories de risque prises en considération doivent être en accord avec les typologies applicables au contexte. Par conséquent, les risques pris en considération peuvent dériver aussi bien de menaces internes, externes ou environnementales, que d'actes délibérés, de gestions organisationnelles inadéquates ou de négligences de chaque risque.

La valeur du risque est considérée comme la fonction de la valeur des assets dans ce contexte, de la valeur des menaces et des vulnérabilités.

Les résultats de l'analyse des risques sont documentés et incluent :

- Une identification claire des risques fondamentaux ;
- Une évaluation des impacts potentiels que chaque risque identifié pourrait avoir sur le business ;
- Un plan d'actions recommandées pour réduire les risques et les ramener à un niveau acceptable.

Le Groupe Aruba établit un modèle d'analyse de type qualitatif, car il est capable de fournir à court terme un niveau de connaissance élevé des risques majeurs ICT impactant l'environnement technologique de référence.

La méthode adoptée est :

- Utilisée par le Groupe afin d'estimer la valeur des informations dans les processus de compétence et le niveau de risque auquel elles sont soumises, pour permettre l'identification des mesures de protection adéquates ;
- Applicable même en cas de développement de nouvelles solutions d'infrastructure ou d'application ayant un impact sur la sécurité des données gérées. Dans ce cas, la méthode permet d'évaluer la criticité des données et les menaces auxquelles elles sont exposées, en permettant aux fonctions responsables de l'analyse des risques, dans les processus de développement et d'obtention des systèmes d'information, de mettre en œuvre les mesures de protection adéquates pour réduire au maximum les vulnérabilités.

L'évaluation des risques et l'analyse des corrélations entre assets, menaces et contre-mesures sont effectuées à l'aide d'un outil développé en interne, alimenté avec les informations collectées au cours des rencontres spécifiques avec les différents acteurs impliqués dans les processus faisant l'objet de l'analyse.
La méthode utilisée permet de réaliser un modèle d'entreprise où sont décrits tous les éléments de base nécessaires aux analyses successives, leurs caractéristiques, leur structure hiérarchique et les connexions relatives.

4 LE PROCESSUS DE GESTION DES RISQUES

Nous décrivons ci-dessous les principales phases du modèle d'analyse pour la gestion des risques relatifs à la sécurité des informations adopté et appliqué par le Groupe Aruba S.p.A.

4.1 PHASE 1 – Context Establishment

La définition du contexte d'analyse prévoit la modélisation de la réalité d'entreprise ainsi que l'identification des principaux services de business, processus, macro-processus et assets impliqués.

Pour l'identification des ressources, comme le suggère la norme ISO/IEC 27005 « Information technology – Security techniques – Information security risk management », deux catégories distinctes ont été considérées :

- **Ressources primaires** – informations, processus, macro-processus et services de business ;
- **Ressources secondaires ou assets** – hardware, software, personnel, network, localisation et organisation.

4.1.1 Identification des services, des processus et des macro-processus

Pour l'identification des services et des processus de l'Organisation, les assets organisationnels publiés et mis à disposition par le biais de l'instrument de communication interne de l'entreprise ont été pris comme points de référence initiaux.
Par la suite, les différents processus qui participent à la fourniture des services sont regroupés en macro-processus spécifiques pour le contexte analysé.

4.1.2 Identification des assets

Afin de garantir une bonne identification des propres assets, il convient de procéder par étape :

1. **Identification des catégories** d'assets informationnels (ex : hardware, software, location, etc.), selon la classification définie dans la norme ISO/IEC 27005 ;
2. **Pondération des catégories** d'assets informationnels en fonction de la stratégie de sécurité de l'entreprise et des exigences commerciales, légales et contractuelles ;
3. **Identification des dépendances** entre les catégories d'assets recensées.

4.1.3 Lien macro-processus – assets

Après avoir identifié les assets, il convient de définir les dépendances entre ces derniers et les macro-processus.

Ces dépendances permettent d'associer à chaque catégorie d'assets les valeurs d'impact CID (déterminées par les entretiens de BIA), ce qui permet de calculer les risques informatiques élémentaires associés à chaque asset.

4.2 PHASE 2 – Risk Analysis

4.2.1 Évaluation des impacts

L'évaluation des impacts (Business Impact Analysis) est effectuée, conformément à la méthode adoptée et aux principales normes internationales (ISO 27005, ISO 22301), par les référents de business.
Grâce à un instrument développé en interne pour la collecte des informations, les Responsables des services de l'entreprise évaluent, lors de la phase d'entretien de BIA, la perte de Confidentialité, d'Intégrité et de Disponibilité des informations gérées dans leur propre zone de compétence en termes d'impact économique, réglementaire et réputationnel, selon des échelles d'évaluation bien définies.

Les différents processus, comme indiqués lors de la PHASE 1, sont par la suite regroupés en macro-processus spécifiques pour le contexte analysé. Les impacts associés à ces macro-processus sont calculés comme le « *worst case* » des différents impacts des processus qui les composent.

4.2.2 Identification et valorisation des assets

L'identification des assets est la base de départ sans laquelle il n'est pas possible de procéder à une gestion bonne et efficace de la sécurité de l'entreprise. En effet, l'inventaire est le point de départ pour la classification des assets de l'entreprise et l'analyse du niveau de risque auquel ils sont exposés.

L'objectif de cette phase opérationnelle est celui de garantir l'élaboration, ou la formalisation conformément aux méthodes déjà existantes, de l'inventaire des assets informationnels considérés par l'entreprise comme étant « mission critical » afin d'atteindre ses propres objectifs de business, de respecter ses propres obligations contractuelles et, enfin, de respecter les normes et la législation auxquelles sont soumises les activités.
La valeur centrale d'un asset est normalement représentée par les informations (ou données) que le système traite, en laissant la tâche aux autres assets de les élaborer et de les protéger.

Dans cette logique, la valeur est attribuée, lors des entretiens de BIA, pour chaque asset et pour chacune des dimensions CID (confidentialité, intégrité et disponibilité) de sécurité applicables au contexte.

En utilisant les informations collectées au cours des entretiens de BIA, il est donc possible d'associer à chaque asset les impacts dérivant des macro-processus qui les utilisent.

4.2.3 Analyse des menaces et évaluation des probabilités d'occurrence

La méthode utilisée dans le processus de gestion des risques pour la sécurité des informations définit un passage ponctuel pour déterminer les menaces qui concernent les assets dans le périmètre. Les menaces représentent tous les éléments ou évènements pouvant endommager un asset.
L'objectif de cette activité est d'identifier les menaces et les vulnérabilités qui insistent sur les assets identifiés et intégrés dans le processus d'analyse et de gestion du risque, ainsi que d'évaluer les probabilités d'occurrence de celles-ci.
Pour garantir l'exhaustivité de la liste des menaces, nous avons pris comme point de référence la liste des menaces de la norme ISO/IEC 27005, à laquelle il convient d'ajouter les considération présentées et publiées par l'ENISA en aval de ses études en la matière.
Les différentes menaces sont successivement regroupées en scénarios de risque réalistes pour le contexte analysé.

4.2.4 Analyse des contre-mesures

L'objectif de cette activité est d'identifier les contre-mesures considérées comme nécessaires pour couvrir les scénarios de risque sur les assets identifiés à l'étape précédente.
Pour garantir l'exhaustivité de la liste, le Groupe Aruba S.p.A adopte une liste de contre-mesures basée sur les best practices de la norme ISO/IEC 27001:2013 Annexe A. Les évaluations, en fonction du type de service analysé, peuvent être enrichies pour des thématiques spécifiques par l'analyse de contrôles supplémentaires suggérés par des autorités comme l'ENISA, l'AgID, le NIST, etc.
Après avoir défini la liste des contrôles de sécurité, ceux-ci ont été cartographiés par rapport aux scénarios de risque, sur lesquels ils peuvent agir en termes de réduction de la probabilité d'occurrence des menaces qui les composent ou de l'impact.
Les contre-mesures ont été divisées en :

- **Réactives** (r), destinées à réduire l'impact ;
- **Préventives** (p), destinées à réduire la probabilité d'occurrence.

4.3 PHASE 3 – Risk Evaluation

4.3.1 Méthode et modèle du risque

La valeur du risque est considérée comme la fonction $R = f(A, M, V)$, où A est la valeur des assets dans ce contexte, M la valeur des menaces et V les vulnérabilités.

Lors de la PHASE 2 du processus de gestion des risques pour la sécurité des informations, il a été possible de définir le modèle de risque (*Threat Modeling*). Ce dernier représente un processus permettant d'identifier les menaces et les vulnérabilités potentielles, d'évaluer leur probabilité dans le cas spécifique, de les mettre sur une échelle de priorité, et de réduire le risque qu'elles deviennent réalité en mettant en œuvre des contre-mesures adéquates.

Après avoir défini le contexte de base, le processus de *Threat Modeling* consiste à :

- Dresser une liste des possibilités d'attaque/de vulnérabilité prévoyant les manières possibles de compromettre la Confidentialité, l'Intégrité et la Disponibilité des données ;
- Évaluer quelles sont les attaques/vulnérabilités les plus probables, écarter les plus improbables ou celles qui sont presque impossibles à remédier, et appliquer des contrôles sur toutes les autres, ou des contre-mesures pouvant être techniques ou procédurales.

4.3.2 Exigences de sécurité applicables et niveau de conformité

En aval de l'identification des exigences de sécurité considérées comme applicables dans le cadre de l'analyse (voir paragraphe « Analyse des contre-mesures »), il convient d'effectuer une évaluation du niveau de couverture des exigences relatives aux 14 catégories identifiées dans la norme ISO/IEC 27001:2013 Annexe A.

Le degré de conformité de chaque contre-mesure est exprimé selon une échelle de valeurs bien définie qui va de 0, en cas de contre-mesure inexistante, à 4 pour une contre-mesure complètement mise en œuvre.

Pour l'analyse du niveau de conformité des contrôles exigés par l'Annexe A de la Norme ISO/IEC 27001:2013, il convient d'utiliser les informations et les preuves collectées au moyen d'activités d'assessment spécifiques réalisées en interne.

4.3.3 Calcul des risques élémentaires inhérents et résiduels

Au cours de cette phase, il convient de calculer la valeur des risques de sécurité élémentaires CID inhérents et résiduels (AS-IS, planifiés et TO-BE) associés au service analysé.

Le calcul des risques élémentaires inhérents pour chaque asset et pour chaque scénario, associé selon les logiques décrites précédemment, est effectué en prenant en compte la probabilité d'occurrence des différents scénarios de risque et l'impact potentiel que ceux-ci pourraient entrainer.

Une fois les risques inhérents déterminés, pour obtenir les risques résiduels (AS-IS, planifié et TO-BE), il convient de prendre en compte les valeurs associées, lors de la phase d'audit interne, aux contre-mesures de sécurité nécessaires

pour contraster les scénarios de risque identifiés, aussi bien en termes de réduction de la probabilité d'occurrence des menaces qui les composent que de réduction de l'impact.

4.4 PHASE 4 – Risk Treatment

4.4.1 Analyse du risque accepté

L'un des concepts fondamentaux pour le risk management est le risque accepté. Ce terme désigne de manière générale les risques qu'il n'est pas pratique ou possible de traiter pour certaines raisons, et qui sont simplement acceptés.

Par conséquent, l'objectif de cette activité est de définir un critère sur la base duquel les couples menace-asset qui présentent un faible risque peuvent simplement être acceptés. Par conséquent, en dehors des cas particuliers, il convient de définir un niveau en dessous duquel un certain risque est simplement considéré comme un coût et n'est donc pas traité.

4.4.2 Résultat de l'analyse : risque résiduel AS-IS

Le travail d'analyse du risque et l'évaluation de celui-ci en prenant en compte les contre-mesures appliquées (risque résiduel), est effectué en réalisant les activités suivantes :

- Assessment des contrôles de sécurité concernant les best practices de l'Annexe A de la Norme ISO/IEC 27001:2013 ;
- Analyse des impacts en cas de perte de disponibilité, de confidentialité et d'intégrité des informations pour les services dans ce contexte ;
- Analyse des vulnérabilités et des menaces sur les assets ;
- Évaluation du risque tel quel de la sécurité des informations et identification d'une échelle de priorité.

4.4.3 Analyse des gaps et choix des contre-mesures à mettre en œuvre

En aval du travail d'analyse effectué, afin de concentrer les éventuels risques/issues importants dans le cadre des services fournis par le Groupe Aruba S.p.A et/ou dans l'optique de poursuivre l'amélioration continue du SGSI, il convient de traiter les données obtenues des analyses effectuées dans l'outil de Risk Analysis afin d'identifier les zones de risque pour lesquelles définir les interventions de sécurité opportunes.

Pour identifier les actions d'amélioration et réduire les risques, une gap analysis est définie à chaque fois afin d'évaluer la distance entre le niveau d'application actuel des contre-mesures de sécurité et le niveau maximal applicable.

4.4.4 Plan de Traitement du Risque – Rationalisation des interventions

Les actions identifiées dans la gap analysis sont par la suite regroupées en initiatives conceptuelles spécifiques et documentées dans le Plan de Traitement du Risque.

5 FRÉQUENCE D'ANALYSE

Le processus de gestion des risques pour la sécurité des informations doit être effectué tous les 12 mois, ou avant en cas d'évènements significatifs comme, à titre d'exemple mais de manière non exhaustive :

- Nouveaux assets qui font partie du domaine du Risk Management ;
- Nouvelles menaces présentes aussi bien en dehors qu'au sein de l'organisation et qui n'ont pas été évaluées ;
- Possibilité que de nouvelles ou davantage de vulnérabilités puissent être exploitées par les menaces ;
- Révision des vulnérabilités déjà identifiées pour déterminer lesquelles pourraient être davantage exposées à des menaces nouvelles ou qui reviennent ;
- Augmentation des impacts ou des conséquences des menaces sur les assets, de la vulnérabilité et des risques qui, s'ils sont regroupés, déterminent un niveau total de risque inacceptable ;
- Incidents de sécurité particulièrement graves.

De plus, il est possible de réaliser des activités d'analyse avec une fréquence différente, par exemple pour la conformité à des normes ou à des exigences de certification particulières.