Entreprise : JSN

Mise en conformité RGPD - Proposition commerciale

Classification, RGPG et Sécurité du Groupe SVLDC

MAY Nathan ; ECHEVERRIA Sébastien ; CORDELOIS Jonathan
08/02/2019

Historique du document

	N° Révision	Créateurs		Actions
		Dates	Noms	
1.	1.0	01 février 2019	MAY Nathan	Création du document
2.	2.1	01 février 2019	ECHEVERRIA Sébastien	Intégration de la partie « Cartographie »
	2.2	01 février 2019	MAY Nathan	Intégration de la partie « Classification »
	2.3	01 février 2019	CORDELOIS Jonathan	Intégration de la partie « Étude des risques »
3.	3.0	05 février 2019	MAY Nathan	Finalisation du document

Table des matières

1. Table des matières

2. Contexte

2.1. Le Groupe SVLC

Le Groupe SVLDC est un groupe de sociétés d'intérim spécialisé dans les métiers du transport. Le siège social de la société mère ainsi qu'une dizaine d'agences sont basées en France. Le Groupe SVLDC détient 2 filiales dont les métiers sont complémentaires, une est basée en Suisse, l'autre est basée en Espagne. Le Groupe SVLDC emploie près de 1'000 collaborateurs, et en 2018, a travaillé avec plus d'une centaine de clients et a accompagné plus de 25'000 intérimaires.

Des échanges d'informations sont quotidiennement réalisées entre les agences, les filiales et le siège du Groupe et un certain nombre d'infrastructure sont mutualisées.

Avec l'application de la Réglementation Générale sur la Protection des Données (RGPD) à caractère personnel, le Groupe souhaite conduire différents audits afin d'évaluer son niveau de conformité et les actions à mener à court/moyens terme.

Il existe actuellement très peu de documentation technique : Aucune politique de sécurité, aucune charte, aucuns schémas techniques à jour…

Pour rappel, le Groupe SVLDC n'étant pas un Organisme d'Importance Vital (OIV), il n'est pas soumis à des réglementations spécifiques.

2.2. Les besoins

2.2.1. Méthode de cartographie

Proposez une démarche de cartographie du Système d'Information client. Cette démarche doit permettre de réaliser l'inventaire des différents composants du SI et notamment ceux qui concourent directement au traitement de données à caractère personnel. Cette cartographie servira notamment à établir la cartographie des traitements de données à caractère personnel.

- Questions à se poser : Quel périmètre, quelles vues, quels outils, quels moyens, etc.
- Bonus : en exposant la démarche que vous souhaitez mettre en œuvre dans le contexte exposé, proposez un déroulement de mission type auquel vous associerez pour chaque étape identifiée une charge en jour-homme

2.2.2. Démarche de classification

Proposez une échelle de classification de l'information pertinente composée de 3 ou 4 niveaux. Ces niveaux seront conditionnés par des échelles intermédiaires permettant de hiérarchiser les risques selon leur niveau d'impact et de vraisemblance. Cette échelle permettra de classifier les risques pouvant présenter des impacts potentiels sur la vie privée afin de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données concernées. En matière de données à caractères personnel, le RGPD distingue les données sensibles, nécessitant une analyse d'impacts au niveau de leurs traitements, des autres données.

2.2.3. Démarche d'étude des risques

Proposez une méthode d'étude des risques sur la vie privée. En effet, pour chaque traitement de données sensible, une étude d'impact doit être réalisée.

- Bonus : en exposant la démarche d'analyse que vous souhaitez mettre en œuvre dans le contexte exposé, proposez un déroulement type auquel vous associerez pour chaque étape identifiée une charge en jour-homme. Le nombre d'analyses d'impact est estimé à une dizaine.

2.2.4. Mesures de sécurité techniques et organisationnelles

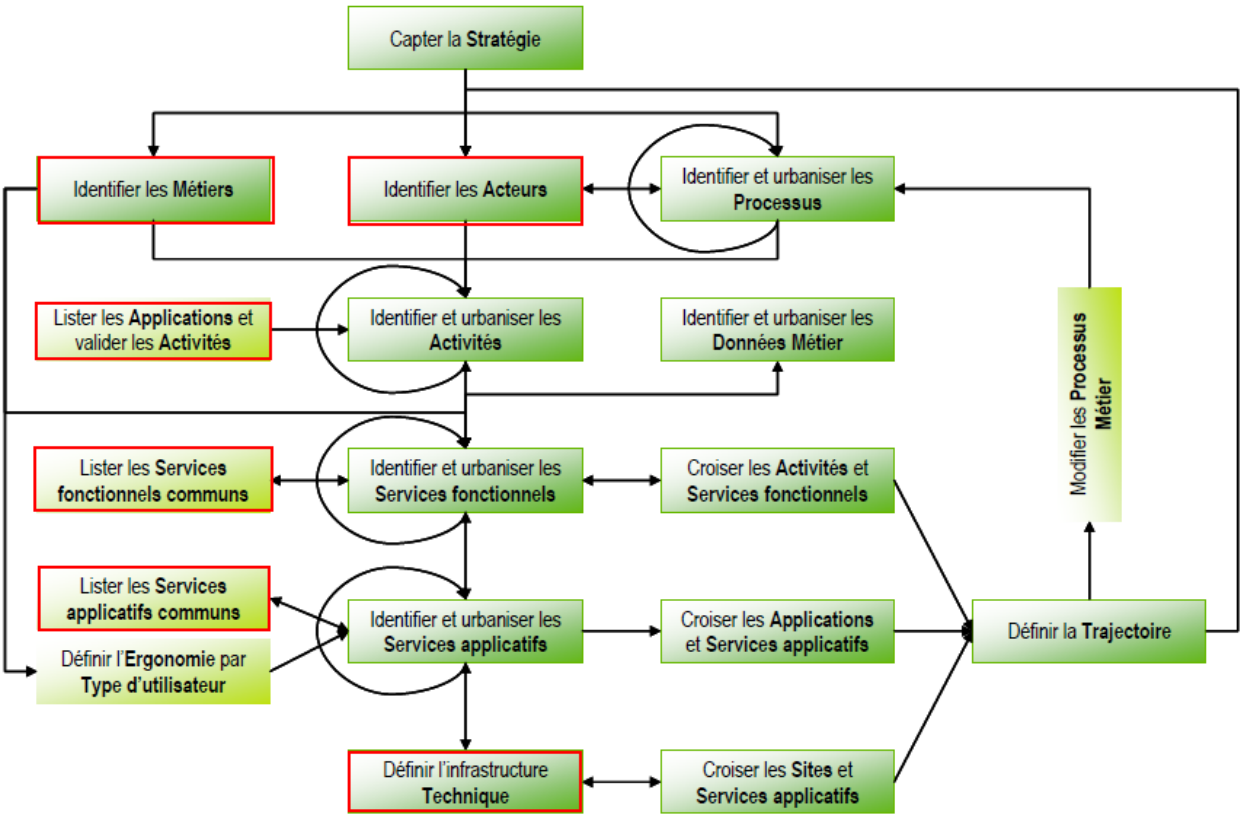
Proposez des mesures de sécurité techniques et organisationnelles sur la base des trois traitements identifiés et détaillés, proposez des mesures de sécurité adaptées là où le niveau de sécurité garanti par les mesures existantes est jugé améliorable.

- Activité/Traitement 1 : gestion des clients et intérimaires
- Activité/Traitement 2 : vidéosurveillance du personnel
- Activité/Traitement 3 : gestion de la paie

3. Méthode : L'urbanisation

Afin de réaliser la cartographie de votre entreprise, nous nous appuieront sur les principes de l'urbanisation.

L'élaboration de la cartographie est un cycle itératif qui permet de modéliser la cible d'urbanisation du SI. Les activités du cycle de cartographie sont présentées dans le schéma ci-dessous :



Nous vous proposons dans un premier temps d'effectuer un état des lieux de votre entreprise, cela correspond aux blocs entourés d'un cadre rouge sur le schéma.

Urbaniser, c'est organiser la transformation progressive et continue du système d'information visant à le simplifier, à optimiser sa valeur ajoutée et à le rendre plus réactif et flexible vis à vis des évolutions stratégiques de l'entreprise, tout en s'appuyant sur les opportunités technologiques du marché. L'urbanisme définit des règles ainsi qu'un cadre cohérent, stable et modulaire, auquel les différentes parties prenantes se réfèrent pour toute décision d'investissement dans le système d'information.

La démarche d'alignement stratégique et d'urbanisation d'un Système d'Information vise à répondre à 4 objectifs majeurs :

- Synchroniser les actions du Système d'Information avec la stratégie de l'Entreprise, afin de renforcer la valeur d'usage du Système d'Information et en faire un atout pour l'Entreprise
- Rendre le Système d'Information « lisible » pour favoriser le dialogue et la communication avec les directions métiers, les Maîtrises d'ouvrage (MOA) et les Maîtrises d'œuvre (MOE)
- Disposer d'un Système d'Information agile, capable d'évoluer rapidement et en toute sécurité tant d'un point de vue métier que technique
- Contribuer à la maîtrise des coûts informatiques

Urbaniser le Système d'Information, c'est répondre positivement aux enjeux suivants :

- Positionner le Système d'Information de Production par rapport au Système d'Information Interne de l'Entreprise
- Aligner les priorités d'investissements sur le Système d'Information de Production par rapport aux objectifs stratégiques
- Clarifier les responsabilités sur les différentes zones du Système d'Information que ce soit en termes de MOE ou MOA
- Etablir et communiquer des règles d'urbanisme pour le Système d'Information de Production
- Evaluer les opportunités technologiques du marché
- Définir un plan de progrès pour le Système d'Information de Production
- Contribuer au choix de solutions et faciliter leur intégration dans le Système d'Information

Les bénéfices attendus d'une approche urbanisée du Système d'Information sont principalement :

- Un alignement facilité du Système d'Information sur la stratégie de l'entreprise et une contribution significative à l'apport de valeur
- Une réduction de la complexité et un renforcement de la cohérence
- Une meilleure préparation des décisions sur l'évolution du Système d'Information (impacts, risques, valeur apportée...)
- Une diminution de la redondance applicative, mutualisation des outils informatiques, réduction des coûts d'intégration
- Une réduction du coût des projets du Système d'Information et des processus en favorisant une optimisation globale
- Une définition claire des rôles et responsabilités des différents acteurs.

3.1. Prestation proposée : Cartographie croisée

Nous avons identifié **12 service**s interne au sein de votre société SVLDC. Nous vous proposons une cartographie croisée de votre entreprise.

La charge de travail est proportionnelle aux nombres de service de votre entreprise.

Nombre et type de service identifié :

- Service RH
- Service Marketing
- Service Compta
- Service Paye
- Service DSI
- Service Commercial
- Service Généraux
- Service Filiale 1
- Service Filiale 2
- Service Direction Générale
- Service Formation
- Service Juridique
- Acteurs et service Externe (fournisseurs)

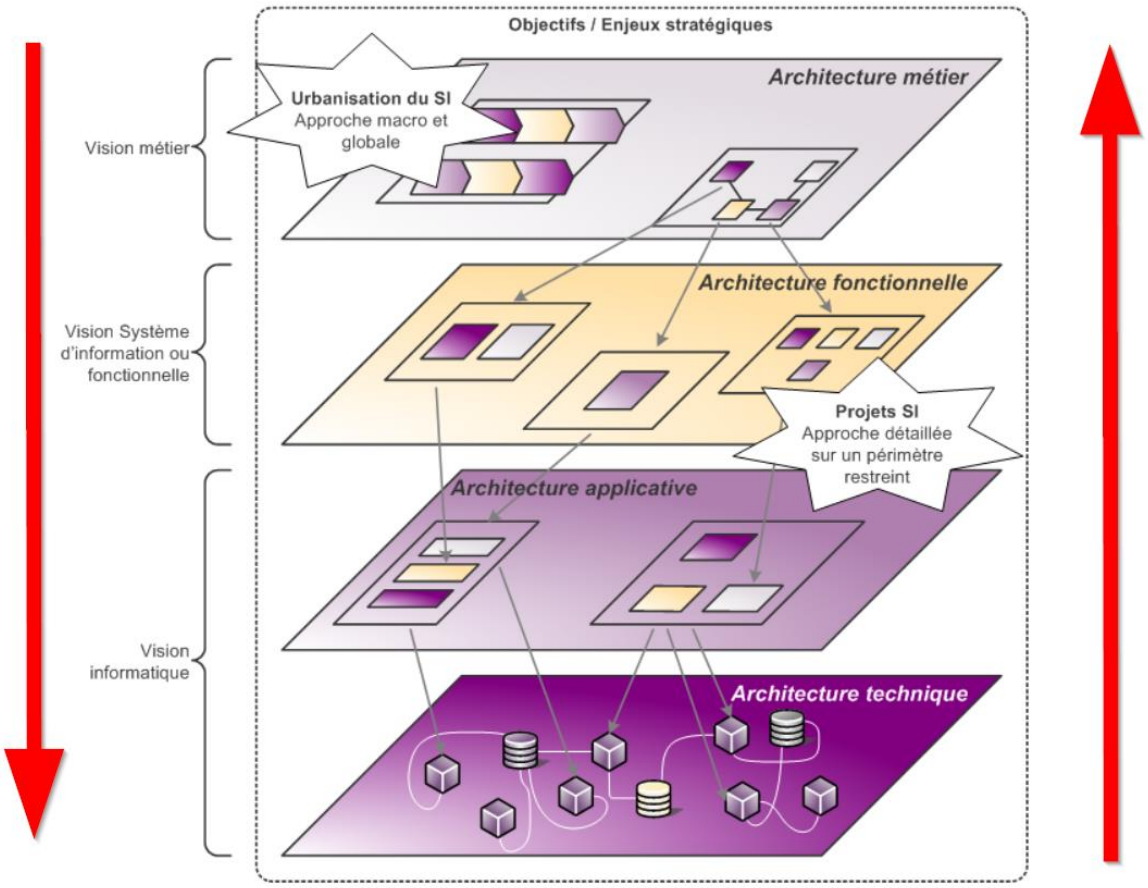
Deux de nos collaborateurs seront chargés d'effectuer la cartographie de votre entreprise et de vous fournir le livrable « Audit de la cartographie » à la fin de la prestation.

Il sera composé de différente vue :

- **Vue métier** : cartographie des processus métiers de l'organisation.
- **Vue fonctionnelle** : description des fonctionnalités (services) offertes par le système d'information pour supporter les processus métiers.
- **Vue applicative** : description de l'ensemble des éléments du système informatique implémentant les services urbanisés sous forme d'éléments logiciels.
- **Vue technique** : description de l'infrastructure de fonctionnement des éléments logiciels du système informatique.

Nos experts auront chacun leur périmètre défini afin de ne pas effectuer deux fois le même travail, il y aura un périmètre métier et un périmètre technique.

Des points de synchronisation seront effectuées à intervalle régulier, 2 points par semaine, afin de pouvoir croisée leur travail et fournir une cartographie exhaustive de votre entreprise.



3.2. Charge de travail

En moyenne, il faut 0,5 j/h pour un entretien, cela comprend :

- Phase de préparation
- Phase d'entretien
- Phase de rédaction et remise du livrable : compte rendu

3.2.1. Phase 1 : Workshop

Un workshop sera lancé pendant la phase de lancement du projet. Il aura pour objectif :

- Gérer le projet :
- Identifier et communiquer à tous les acteurs
- Mettre en place une gestion de la disponibilité des acteurs
- Mettre en place une gestion de la documentation

Nous planifierons et organiserons une réunion de lancement avec les acteurs (direction et directeurs métiers) : total de 2 j/h

- Phase de préparation réunion
- Phase Réunion
- Livrables :
  - Compte rendu réunion
  - Plan de missions : accord sur les missions, le périmètre du projet et les livrables signé par les deux parties
  - Accord financier signé par les deux parties

Le workshop aura une charge totale de 2 j/h

3.2.2. Phase 2 – entretiens directeurs de métier

Nous vous proposons de commencer un état des lieux des métiers avec leur directeur respectif.

Nous recommandons deux entretiens avec les directeurs métiers, la charge totale des entretiens avec les directeurs métiers est de 2 x 0,5 x 12 = 12 j/h

Un PV de recette sera fourni à la fin de cette phase, il comprendra un bilan et les comptes-rendus des entretiens.

3.2.3. Phase 3 – entretiens avec les « key-users »

Les entretiens avec les directeurs vont nous permettre d'identifier les key-users des activités métiers (les gestionnaires des activités).

Des entretiens avec les key-users permettrons de modéliser les activités métiers de l'entreprise et ainsi la réalisation de la cartographie de la vue métier.

En moyenne, on estime à 3 key-users ou activité par métier.

Nous préconisons deux entretiens groupés par métier, la charge totale est de 2 x 0,5 x 12 = 12 j/h

Un PV de recette sera fourni à la fin de cette phase, il comprendra un bilan et les comptes-rendus des entretiens.

3.2.4. Phase 4 – entretiens technique avec la DSI

En parallèle des entretiens des gestionnaires d'activité, Nous vous proposons d'établir un état des lieux de l'architecture technique.

deux entretiens avec le directeur du service d'information sont nécessaires, la charge totale est de 2 x 0,5 = 1 j/h

Un PV de recette sera fourni à la fin de cette phase, il comprendra un bilan et les comptes-rendus des entretiens.

3.2.5. Phase 5 – Audit des ressources techniques

Les entretiens avec le directeur du service informatique permettront d'identifier les gestionnaires des ressources informatiques.

4 entretiens groupé seront nécessaires soit 4x 0,5 = 2 j/h au total pour cette phase.

Un PV de recette sera fourni à la fin de cette phase, il comprendra un bilan et les comptes-rendus des entretiens.

3.2.6. Phase 6 – Rédaction Audit

Cette phase correspond à la rédaction et à l'envoi du livrable final, le rapport d'audit de la cartographie, décrit plus haut dans la proposition.

Cette phase comprend :

- Rédaction de la cartographie
    - Fusion et mises en forme des informations
    - Création des différentes vues
- Rédaction du rapport d'audit

La charge est de 5 j/h

3.2.7. Phase 7 – Clôture

Organisation d'une réunion de clôture.

- Planifier et organiser une réunion de clôture avec les acteurs (direction et directeurs métiers) : total de 1 j/h
    - Phase de préparation réunion 0,25 j/h
    - Phase Réunion 0,5 j/h
    - Livrables : total de 0,25 j/h
        - Compte rendu réunion
        - Bilan

La charge totale est de total de 1 j/h

3.2.8. Total

La charge totale, comprenant les 7 phases, est de (2 +12+12+1+2+5) = 35 j/h

3.3. Macro planning

Phases	
Workshop	2 j
Entretiens directeurs de métier	12 j
Entretiens avec les « key-users »	12 j
Entretiens technique avec la DSI	1 j
Audit des ressources techniques	2 j
Rédaction Audit	5 j
Clôture	1 j
Total	32 J

3.4. Devis

Lots	Livrables	Nbr de J/h	Coût Horraire	Coût Total € HT
Lots 1 cartographie	Plan de missions CR Interne et externes PV recette entretiens Cartographie 4 vues Bilan	35	800	28000

4. Démarche de classification

4.1. Définition : Classification

Classification des données : " Processus de catégorisation cohérente des données sur la base de critères spécifiques et prédéfinis, afin qu'elles puissent être utilisées et protégées plus efficacement. Le processus de classification facilite la localisation et la récupération des données, point très important lorsqu'il s'agit de la gestion des risques, de la conformité et la sécurité, ou encore l'adaptation aux réglementations telle que GDPR et PCIDSS " (*Définition ANSSI*)

Les catégories : Elles sont définies par : (les != vues possibles)

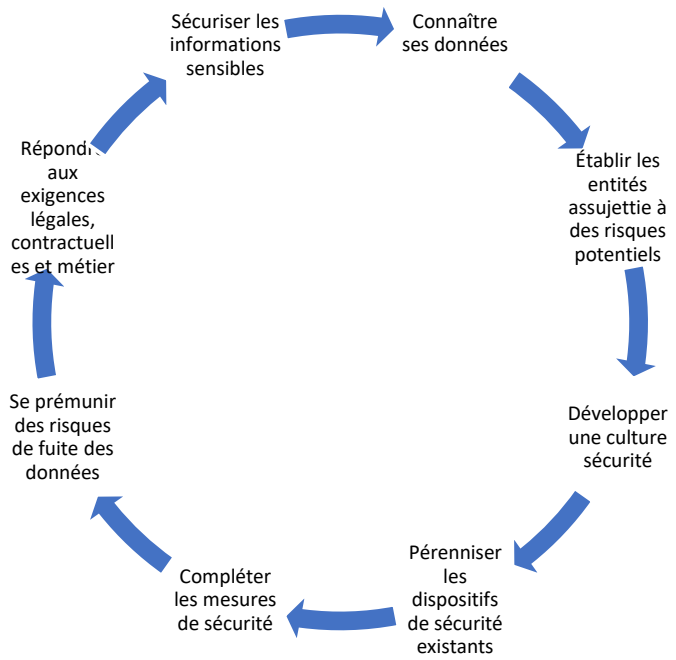
- Niveau de sensibilité
- Division métier

---> Une donnée = Un cadre réglementaire, légal ou de sécurité

Echelles de classification : (France)

- Très secret
- Secret
- Confidentiel
- Restreint
- Non protégé

4.1.1. Les apports de la classification des données

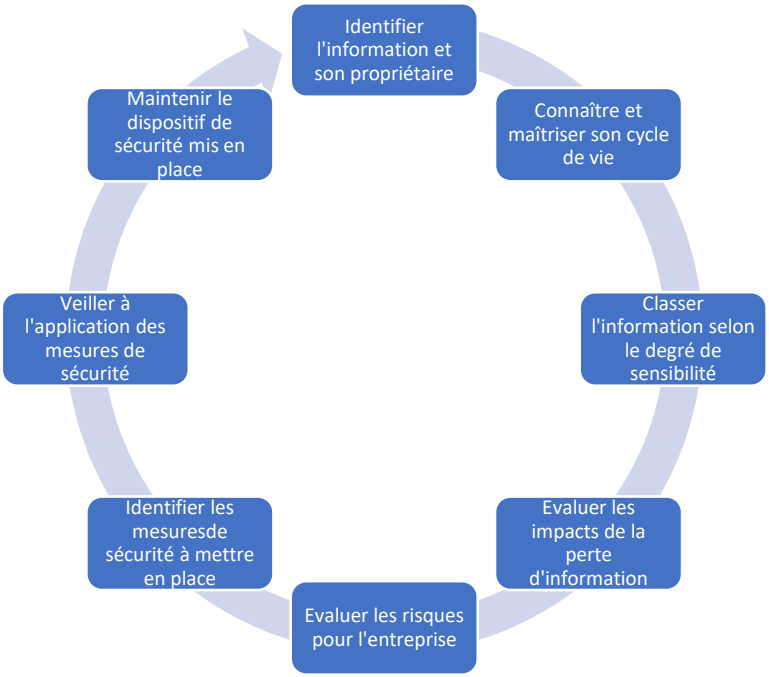


La classification des données permet de connaître la sensibilité et la criticité de vos informations et choisir les dispositifs de sécurité adaptés pour assurer leur protection.

La classification est une activité nécessaire pour la gestion des risques de sécurité dans l'entreprise, en effet, elle permet de choisir les scénarios de risques les plus pertinents qui peuvent affecter la capacité de l'entreprise afin de réaliser les objectifs de sécurité fixés en amont et les évaluer avec précision.

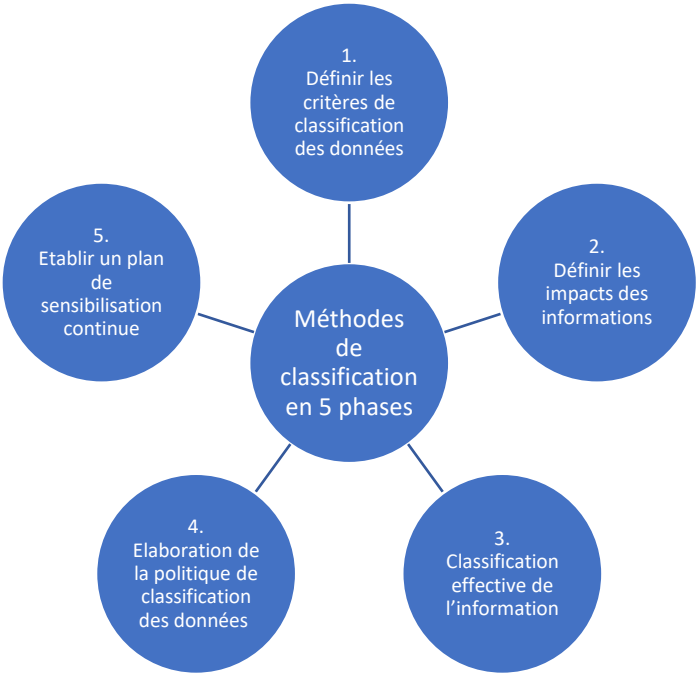
4.1.2. Comment classifier l'information ?

L'approche clé pour une démarche réussie de classification des données, consiste à considérer de bout en bout le cycle de vie de l'information, depuis sa création jusqu'à son archivage ou sa destruction, et considérer les besoins de sécurité (Confidentialité, Intégrité, Disponibilité) à chaque étape du cycle de vie.



4.2. Méthodologie de classification de l'information

Pour effectuer la classification des données il est nécessaire de suivre une méthodologie rodée et pragmatique. Cette dernière doit garantir le bon déroulement du projet et permettre de bien cerner les informations à classifier.


1.
Définir les critères de classification des données
2.
Définir les impacts des informations
3.
Classification effective de l'information
4.
Elaboration de la politique de classification des données
5.
Etablir un plan de sensibilisation continue
Méthodes de classification en 5 phases

4.3. Phase 1 : Elaboration de la politique de classification des données

Après la collecte, la classification et l'analyse des informations obtenues dans les précédentes phase, il sera nécessaire de formaliser dans une « politique de classification », les différentes règles et mesures de sécurité à appliquer afin d'assurer leur protection adéquate.

Cette dernière énoncera des règles de classification et proposera une approche de mise en œuvre des différentes mesures de protection pour chaque niveau de classification et à chaque étape du cycle de vie de l'information.

Voici un exemple de règles à appliquer à chaque niveau de classification dans le cas du « stockage des données sur des supports externes » :

Cas d'utilisation		**Échelles de classifications**			
		Public	**Restreint**	**Confidentiel**	**Secret**
Stockage des données sur des supports externes	**Règles de sécurité**	Marquage des fichiers	• Sensibilisation des collaborateurs à l'utilisation de supports externes sécurisés • Marquage des fichiers	**Outre les règles des données de type « interne » :** • Utilisation des supports externes éligibles par l'entreprise • Suppression des données immédiatement après leur utilisation • Chiffrement des données • Utilisation des supports de stockage avec des mécanismes de protection des données	**Outre les règles des données de type « Confidentiel » :** • Création de partition virtuelle

4.3.1. Partie 1 : Définir les critères de classification des données

La classification des informations a pour but de garantir la sécurité des données. Elle se définie selon 3 critères :

- La confidentialité,
- La disponibilité,
- L'intégrité de l'information.

Voici pour chaque critère, une échelle de classification :

Échelle de confidentialité		
Confidentialité	**Besoin**	**Niveaux d'impact**
Secret	Données pouvant causer de grave dommage au Groupe SVLDC en cas de divulgation publique.	4
Confidentiel	Données pouvant nuire sérieusement au Groupe SVLDC en cas de divulgation publique.	3
Restreint	Données non transmissible aux personnes externe au Groupe SVLDC. Une fuite de ces données peut nuire à l'entreprise.	2
Public / Non protégé	Données pouvant être rendues public, n'ayant aucun impact pour le Groupe SVLDC.	1

Échelle d'intégrité		
Confidentialité	**Besoins**	**Niveaux d'impact**
Élevé	La perte de l'intégrité des données de cette catégorie est intolérable. Une altération de ces données aurait un impact élevée pour le Groupe SVLDC	3
Moyen	Une altération des données aurait un impact important pour le Groupe SVLDC	2
Faible	La perte d'intégrité des données de cette catégorie est tolérable, l'impact pour le groupe SVLDC est faible voire inexistant	1

Échelle de disponibilité		
Confidentialité	**Besoins**	**Niveaux d'impact**
Élevé	L'indisponibilité des données de cette catégorie est inacceptable, l'impact est très élevé pour le Groupe SVLDC	3
Moyen	La tolérance d'indisponibilité des données de cette catégorie est moyenne, le Groupe SVLDC court un impact important.	2
Faible	L'indisponibilité des données de cette catégorie est acceptable, le Groupe SVLDC court un impact faible.	1

4.3.2. Partie 2 : Définir les impacts des informations

Les impacts de la perte de confidentialité, de disponibilité ou d'intégrité de l'information sont **reliés**. Ces impacts peuvent présenter pour l'entreprise des défis pour sa conformité légale réglementaire et contractuelle, ses opérations quotidiennes, sa réputation ou ses finances.

Par exemple, la divulgation d'une information confidentielle peut impliquer une perte de confiance dans l'entreprise ou encore des poursuites judiciaires entrainant des pertes financières considérables.

Voici un exemple d'une concrète des impacts possible :

Impacts	1 : Nul	2 : Modéré	3 : Significatif	4 : Très grave
Conformité	Aucun impact juridique	Possibilité de provoquer un faible nombre de contentieux individuels vis-à-vis de clients, fournisseurs, partenaires.	Peut être considéré comme une infraction au RGPD	Peut être considéré comme des infractions systématiques au RGPD
			Possibilité de provoquer de nombreux contentieux avec des clients, fournisseurs, partenaires.	Possibilité de provoquer un grand nombre de contentieux avec des clients, fournisseurs, partenaires.
Opérationnel	Aucun impact organisationnel	Possibilité de bloquer fortement, de façon non planifié, pendant plus d'1/2 journée et moins d'1 journée le travail de plus de 25% des utilisateurs habituels des applications métiers.	Possibilité de bloquer fortement, de façon non planifié, pendant plus de 24h et moins de 72h de plus de 25% des utilisateurs des applications métiers.	Altération totale d'un traitement crucial/majeur pour le Groupe SVLDC susceptible de provoquer un arrêt ou pendant une durée de l'ordre de 3 jours ou plus.
			Susceptible de créer une surcharge temporaire de travail importante pour éviter une dégradation significative de la qualité de service rendu.	Susceptible d'avoir un impact sur les conditions de travail d'un pourcentage important des utilisateurs.
			Susceptible de créer des mouvements sociaux limités.	Susceptible de créer des mouvements sociaux graves.
Réputation	Aucun impact sur l'image	Médiatisation dans la presse privée, bouche à oreille négatif	Médiatisation dans la presse publique	Médiatisation nationale durable
Financier	Coûts < 1 000€	Coûts > 100 000€	Coûts > 1 000 000 €	Coûts > 10 000 000 €

Les critères choisis devront être redéfinis avec la direction du Groupe SVLDC.

L'analyse des impacts devra tenir compte :

- Du **niveau de granularité** adéquat : Préférer les groupes d'information (dossier du personnel, dossier des clients…) contenant l'information classifiée, plutôt que la donnée élémentaire (nom du collaborateur).
- De **l'étape du cycle de vie** : Considérer le flux de l'information depuis sa collecte (en entrée) par le processus considéré, son traitement par les opérations du processus, jusqu'à son transfert (en sortie) vers les processus en aval.
- De la **vision globale à l'échelle de l'entreprise** : Il est nécessaire d'adopter une dualité dans l'approche d'analyse de la classification.

La prise en compte de ses subtilités est importante pour la pertinence des résultats de classification et la pérennité des dispositifs de sécurité envisagés.

4.3.3. Phase 3 : Plan de déploiement de la politique de classification

Le plan de déploiement reprendra les informations contenues dans la politique de classification des données. Il permet la mise en pratique des mesures de sécurité validées par l'entreprise et aborde le maintien de la classification. Il s'appuie notamment sur les activités suivantes :

a) Déterminer les paramètres de déploiement

- Responsable des mesures de sécurité identifiées ;
- Echéances de déploiement
- Ressources nécessaires

b) Déterminer les rôles et responsabilités minimum pour la classification des données

- Les propriétaires de l'information ;
- Le responsable du suivi et du maintien de la classification
- La liste des parties prenantes impliquée dans la revue de classification;

c) Etablir un plan de sensibilisation continue

Il sera nécessaire de prévoir un programme de sensibilisation et de formation pour s'assurer que les collaborateurs soient conscients de la nécessité d'éviter les comportements à risque.

Cette sensibilisation portera sur les impacts d'une fuite de données, les règles de classification à observer…

4.4. Phase 2 : Classification effective de l'information

4.4.1. Préparation et planification

Dans un premier temps il faudra réaliser une planification des ateliers de classification des données en coordination avec les principaux services concernées en identifiants les interlocuteurs qualifiés.

Le premier objectifs des ateliers est le recueil des informations essentielles de chaque services afin d'établir une cartographie précise de ces dernières. Par la suite, il s'agira d'identifier les informations essentielles aux activités ou processus considéré, puis assister et challenger les interlocuteurs dans l'évaluation des besoins de sécurité pertinents.

Après l'identifications des informations essentielles et leur flux au sein du processus ou de l'activité considérés, les paramètres suivant doivent être identifiés :

Le nom de l'information : Pertinent et explicite, pour une identification unique au sein de l'entreprise.

- **Le nom de l'information** : Pertinent et explicite, pour une identification unique au sein de l'entreprise.
- **Le propriétaire de l'information** (Data Owner) : le responsable de la gestion de l'information.
- **Le format de l'information** : Donnée électronique ou format papier essentiellement.
- **Les responsabilités liées à l'information** : Propriétaire, entités qui y accèdent et droits d'accès.
- **L'impact que l'information peut avoir sur l'entreprise** : Opérationnel, financier, conformité, réputation.
- **Ses besoins de sécurité** : En termes de confidentialité, disponibilité, intégrité.
- **Les canaux de diffusion** : Les SI sollicités, les systèmes et réseaux par lesquels l'information transite.
- **Les règles de marquage applicables** : Lois et règles applicables à l'information.
- **Le cycle de vie de la donnée** : Durée de vie en tant que donnée courante, avant archivage.
- **Le support de stockage** : Format de conservation (Base de données, application, salle d'archive, …)
- **La conservation** : Les raisons de conservation et la période de rétention.
- **Le procédé de destruction de l'information** : nécessité ou non de mise en rebut, de recyclage…
- **Les mesures de sécurité appliquées dans l'entreprise** : règles d'authentification, de cryptage, de conservation d'intégrité, de traçabilité appliquées à la donnée.

4.4.2. Déroulement des ateliers

Les ateliers de classification des données est la partie la plus important du projet.

Une fois les données appréhendées, il est nécessaire d'exposer les échelles de classification utilisées aux collaborateurs et responsables. Dans un second temps, une évaluation d'impacts sera menée, cela contribuera à la compréhension des besoins de sécurité et permettra de faciliter la collecte des données relatives aux informations sensibles du Groupe SVLDC.

4.4.3. Analyse et consolidation

Une fois les données recueillies dans le « recueil des données », une analyse est nécessaire afin de consolider ces dernières et ressortir les éléments de décision attendus. Cette analyse nous permettra :

- D'épurer les paramètres collectés,
- D'identifier les redondances/incohérences,
- De mettre en évidences les actifs supports les plus sollicités
- De mettre en évidences les risques opérationnels

4.5. Devis :

Phases	Livrables	Nbr de J/h	Coûts horaire (HT)	Tarifs (HT)
Phase 1 : Elaboration de la politique de classification des données	• Rapport des critères de classification des données • Rapport des impacts des informations • Politique de classification • Optionnel : Plan de déploiement de la politique de classification	**6**	800 €	4800 €
Phase 2 : Classification effective de l'information	• Recueils des informations essentielles par service • Analyse et consolidation des informations	**12**		9600 €
Phase 3 : Clôture	• Bilan • Recettage	**1**		800 €
			Total	**15200 €**

4.6. Macro planning

Phases	Planning
Phase 1 : Elaboration de la politique de classification des données	6j
Phase 2 : Classification effective de l'information	12j
Phase 3 : Clôture	1j
Total	19j

5. Démarche d'analyse d'impacts

5.1. Le contexte du traitement

- Définir le rôle chaque parties prenantes
- Identifier la finalité du traitement
- Identifier qui effectue ce traitement et sur quel processus métier il intervient
- Identifier les supports (matériel, logiciels, papiers)
- Identifier les canaux de transmission (mail, courrier, scan, impression)
- Indiquer les raisons pour laquelle ce traitement doit être protéger (légal, sectorielle, besoins etc.)
- Identifier les sources susceptibles de compromettre ce traitement (personnes internes, personnes externes, facteurs divers (sinistres, intempéries, etc.))

5.2. Gestion de la gravité

Les évènements redoutés ou risques possibles dans le contexte de l'entreprise en définissant une gravité pour chacun d'entre eux

- Identifier les impacts, conséquences potentielles (pertes, voles, récupérations de données, traitement corrompu ou modifié, etc.)
- Déterminer la gravité pour chacun d'eux en fonction de la gravité et de l'impact (1 à 4)
- Déterminer la gravité pour chacun d'eux en fonction du préjudice (1 à 4)
- Calculer la gravité en fonction des deux critères définis précédemment

Événements redoutés	Caractère identifiant des DCP[23]	Impacts potentiels les plus graves	Caractère préjudiciable des impacts potentiels	Mesures existantes ou prévues	Gravité maximum
1. Indisponibilité des processus légaux	*4. Maximal*	✓ *Diffusion non maîtrisée de DCP* ✓ *Impossibilité d'exercer ses droits* ✓ *Blocage de procédures d'achats*	*2. Limité*	*Aucune mesure prévue pour réduire la gravité*	*3. Important*
2. Modification du traitement	*4. Maximal*	✓ *Propositions commerciales non sollicitées*	*1. Négligeable*	*Aucune mesure prévue pour réduire la gravité*	*2. Limitée*
3. Accès illégitime aux DCP	*4. Maximal*	✓ *Usurpation de compte* ✓ *Exploitation à des fins commerciales*	*3. Important*	*Toutes les données sont nécessaires*	*4. Maximal*
4. Modification non désirées des DCP	*4. Maximal*	✓ *Commandes non satisfaites*	*1. Négligeable*	*Sauvegardes et récupération dans la journée*	*2. Limitée*
5. Disparition des DCP	*4. Maximal*	✓ *Obligation de se réinscrire* ✓ *Perte d'avantages*	*1. Négligeable*	*Sauvegardes et récupération dans la journée*	*2. Limitée*

5.3. La vraisemblance

Il s'agit ici d'identifier les menaces potentielles et d'estimer la vraisemblance. Pour ce faire :

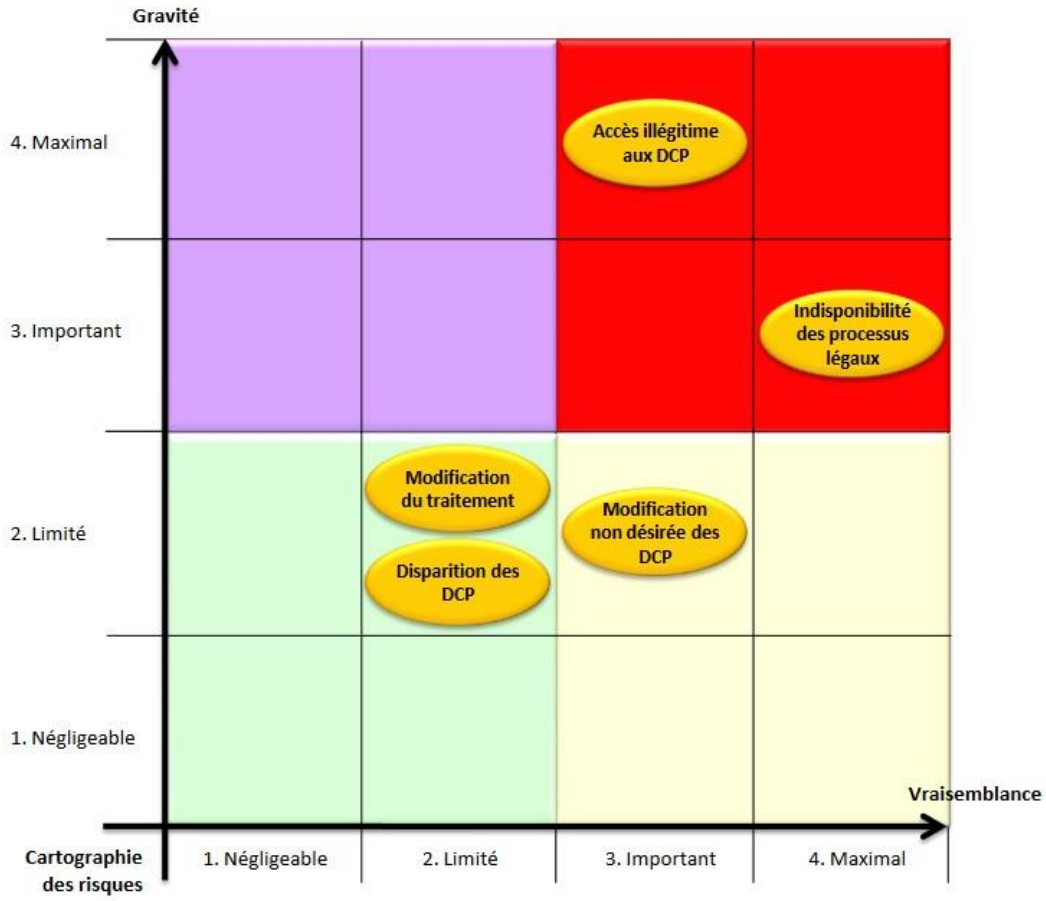
- Identifier les vulnérabilités du support utilisé (papier (vol), disque (copie du disque), clé USB (perte), mail (interception) avec une gravité (négligeable, Limité, Important, Max)
- Identifier la capacité à exploiter les vulnérabilités (droits d'accès, proximité, accès physique, compétences etc.…) avec une gravité (1 à 4)
- Calculer la vraisemblance (en additionnant par ex) les deux points précédents)

Événements redoutés	Menaces les plus vraisemblables	Vulnérabilités des supports	Capacités des sources de risques	Mesures existantes ou prévues	Vraisemblance maximum[26]
1. Indisponibilité des processus légaux	✓ *Détérioration d'un matériel (ex. : destruction d'un serveur)* ✓ *Usage anormal d'un logiciel (ex. : maladresse en manipulant les fichiers)* ✓ *Départ d'une personne (ex. : démission de celui qui connait les procédures)* ✓ *Disparition d'un canal papier (ex. : changement de procédures)*	*4. Maximal*	*3. Important*	*Aucune mesure prévue pour réduire la vraisemblance*	*4. Maximal*
2. Modification du traitement	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*
3. Accès illégitime aux DCP	✓ *Vol d'un matériel (ex. : vol d'un PC portable dans le train)* ✓ *Détournement d'usage d'un logiciel (ex. : usage à titre personnel)* ✓ *Modification d'un logiciel (ex. : propagation d'un virus)*	*3. Important*	*3. Important*	*Aucune mesure prévue pour réduire la vraisemblance*	*3. Important*
4. Modification non désirées des DCP	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*
5. Disparition des DCP	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*	*[sans objet]*

5.4. Création de la matrice

Identifier tous les risques e qui peuvent intervenir sur ce traitement et les classer dans une matrice

- Lister tous les risques identifiés précédemment
- Les classer dans une matrice cartographie des risques
- Pour les risques dont la gravité et la vraisemblance sont élevées, proposer des solutions pour réduire l'un des deux facteurs



Les actions à mettre en place dépendent du niveau de gravité et de vraisemblance. Ces actions sont réparties de la façon suivante :

Niveau de gravité	Niveau de vraisemblance	Actions
Élevé	Élevé	Prévoir des mesures avant, pendant et après sinistres et diminuer leur gravité et/ou leur vraisemblance.
Élevé	Faible	Privilégier des mesures de prévention pour diminuer leur gravité ou leur vraisemblance.
Faible	Élevé	Privilégier des mesures de récupération pour diminuer la vraisemblance
Faible	Faible	Ces risques doivent être traitées au cas par cas. Le traitement des risques plus élevés devrait interagir avec ces risques.

5.5. Actions pour traiter ce risque

Identifier les risques pour laquelle la vraisemblance et la gravité sont les plus élevées, et définir une action pour traiter ce risque. Trois Mesures sont possibles :

- Minimiser
- Informer
- Mettre en place des actions, procédures pour traiter les risques en agissant sur les 4 niveaux.

Afin de réduire / minimiser les risques, nous devons agir si possible sur la vraisemblance et sur la qualité. Pour ce faire, nous devons agir sur les 4 niveaux décrit précédemment. Si nous ne pouvons agir sur le niveau le plus haut, nous agissons sur le niveau du dessous.

- Eléments protéger
- Impacts
- Sources
- Médias

Réestimer la gravité et la vraisemblance des risques. Certains risques peuvent ainsi être repositionnés, d'autres peuvent être acceptés.

Pour identifier lesquels peuvent être acceptés, nous utiliserons ce tableau :

Niveau de gravité	Niveau de Vraisemblance	Actions
Élevé	Élevé	Ces risques doivent être obligatoirement pris en compte
Élevé	Faible	Peuvent être négligé s'il est impossible de réduire la gravité et la vraisemblance est faible
Faible	Élevé	Peuvent être négligé s'il est impossible de réduire la vraisemblance et la gravité est faible
Faible	Faible	Peuvent être négligé

6. Charges de travail et livrables

6.1. Récupération des analyses

Récupérer toutes les données provenant de l'étude cartographique afin d'identifier les parties prenantes, les opérateurs et la finalité des traitements, etc.) (1 jr/h)

Réunion pour identifier tous les supports, les canaux de transmission ainsi que les raisons de protéger ces données. Ce temps prend en compte la préparation de la réunion, le déroulement, une phase d'analyse des échanges ainsi que le compte-rendu de celui-ci. (1 jr/h)

6.2. Etude d'impact (5 à 10 jr/h)

Aujourd'hui, le groupe SVLDC ne dispose d'aucune cartographie et n'a jamais effectué d'analyse de traitement par service. Nous devons attendre que cette cartographie complète soit faite pour effectuer une analyse d'impact.

Une fois les traitements identifiés et la nature des données récoltées, nous définirons des scénarios possibles pour chacun d'eux et les conséquences éventuelles. Nous estimons à une journée l'étude de l'impact par traitement.

Cette analyse sera modélisée dans le document « Audit d'impact » dans le but de :

- Conserver la disponibilité des processus
- Eviter l'altération du traitement
- Contrôler la gestion des données personnelles

6.3. Analyse des risques (4 jr/h)

A partir du tableau réalisé, nous allons définir les vulnérabilités potentielles, lié aux supports, ensuite aux sources des risques.

A l'issu de quoi, nous estimerons la vraisemblance qu'un risque peut intervenir, noté de 1 à 4 ainsi que de la gravité. (3 jr/h)

Cette phase sera accompagnée d'une « matrice de risques », permettant d'identifier les traitements à risques et de définir plus rapidement des mesures préventives avec des actions avant, pendant ou après sinistre. (1 jr/h)

6.4. Clôture (2 jr/h)

Une réunion de fin de projet sera organisée pour restituer ces informations. Des fiches d'analyses d'impacts et de risques vous seront transmis avec les actions et les ponts de vigilance indiqué.

Nous vous apporterons, par notre expérience, des actions mesures pour la gestion de vos traitements. Nous vous proposons, lorsque c'est nécessaire des actions immédiates, lorsqu'un risque majeur et imminent et constaté.

7. Macro planning

Lots Analyse impacts	Livrables à rendre	Nombre Jr/h
Analyse	Compte-rendu Plan d'action et d'analyse	2 jr/h
Etude d'impacts	Audit d'impacts	5 à 10 jr/h
Analyse des risques	Matrice de risques Politique de gestion des risques	6 jr/h
Clôture	Compte-rendu Fiches de risques	2 jr/h

Phases	Planning
Phase d'analyse	1j
Entretiens directeurs de métier	1j
Récupération cartographie	1 j
Audit d'impact et rédaction	5 - 10j
Analyse des risques	3j
Rédaction matrice des risques	1j
Clôture	2j
Total	18 jours

8. Mesures de sécurité techniques et organisationnelles