EGE Ecole de Guerre Economique

Les enjeux du Cloud pour les TPE / PME : Une approche par les risques liés aux données

Présenté par :

Aïda SYLLA
Imad LAAROUSSI
Achille MOUNDANGA
Brice de Rosier WILLYBIRO NGUTTU

Décembre 2022
MBA Exécutif « Management de la Cybersécurité et Gouvernance des Systèmes d'Information »

“ Data is the new oil ”

Clive Humby a British mathematician in 2006


GUERRE
ÉCONOMIQUE
SOUS LA DIRECTION
DE CHRISTIAN HARBULOT,
LUCIE LAURENT
ET NICOLAS MOINET
QUI
EST
L'ENNEMI ?
CENTRE DE RECHERCHE 451
EGE École de Guerre Économique
nouveau monde

P

Préambule

Trois entretiens ont été menés dans le cadre de ce mémoire. L'intégralité des entretiens se trouve en *(Annexe 1).*
En voici quelques extraits :

« … on peut commencer à faire confiance au fournisseur Cloud pour avoir des niveaux de sécurité au moins sur les couches basses de l'infrastructure qui sont généralement plus élevées que ce que la moindre entreprise fera elle-même dans son Data Center. Mais il faut éviter de se faire des illusions. Ce n'est pas parce qu'on est dans le cloud qu'on n'a pas de responsabilités sur ses données. »
« …ce n'est pas parce que tu es dans le Cloud que tu ne vas pas faire de backup. »
« …le tiers auquel je confie ma donnée, je ne lui confie jamais ma donnée entière. Je lui confie, pour le stockage, que de la donnée chiffrée et je reste maître de mes clés de chiffrement et mes algorithmes. Et là on arrive à une réduction assez significative du niveau de risque. »
« …Absolument pas ! Si elles en avaient conscience, on n'aurait tout simplement pas autant de victimes d'attaques par ransomware qui se retrouvent mises à genoux pendant des semaines… Le ransomware n'en est qu'un exemple, mais il illustre en fait un manque de conscience sur l'importance de la donnée et de sa valeur. »
« Quand les assureurs auront vraiment cherché progressivement à toucher le tissu des TPE/PME en termes de cybersécurité, ils ne vont pas avoir d'autre choix que de développer leur niveau d'exigences minimums. »
« …D'autres n'ont pas forcément conscience du fait que la donnée est déjà un actif immatériel en soi et qu'il y a déjà une valeur. »
« Les TPE/PME n'ont pas forcément de RSSI. Elles ne vont pas gérer nécessairement leur informatique elles-mêmes. Elles vont passer par des ESN, ce qu'on appelle des infogéreurs. C'est d'ailleurs la raison pour laquelle l'ANSSI se préoccupe autant de la sécurité des ESN. C'est pour ça aussi que les ESN sont prises en compte dans la version 2 de la Directive NIS. C'est parce qu'elles sont le sang et le cœur battant de l'informatique de beaucoup de TPE/PME et donc d'une grosse partie du tissu économique. »
« Le RGPD le souligne très bien, ce n'est pas parce qu'on confie ses données à un infogéreur qu'on est exempt de responsabilités sur tout ce qui pourrait arriver à ses données. »
« …il y a une nécessité pour les grandes entreprises/organisations comme pour les plus petites d'aborder le choix du Cloud provider sous l'angle des risques et de la compliance. »
« …on a un enjeu aussi quand on a un risque à ne pas pouvoir revenir sur ses choix et sur la liberté de ses choix. Cette liberté est essentielle pour une entreprise qui ne veut pas créer une dépendance énorme avec des frais de migration. C'est une question de sensibilité et de conscience. Ce qui ne nous coûte pas à l'entrée va nous coûter à la sortie. »
« On voit qu'il y a un coût qui augmente, qui a déjà augmenté et qui augmente de manière très rapide. Et donc le risque, il est surtout la maîtrise des coûts, aujourd'hui c'est quelque chose de fondamentale. »
« ….. Mais le fait d'aller vers un label, c'est faire le choix des acteurs qui respecteront les plus hauts degrés de confiance »
« …Il est extrêmement compliqué d'avoir une assurance complète sur la non-application du Cloud Act car in fine ce sont des juges américains qui l'appliquent, juges pour la plupart élus... »

«Chaque jour qui passe révèle notre déficit de souveraineté.»

"Each passing day reveals our lack of sovereignty."

Table des matières

Table des figures

Table des tableaux

Partie 1 – Introduction au Cloud computing, définitions et concepts

1. Brève histoire du cloud (4)

Les prémices du Cloud remonteraient vers 1960, avec Joseph Carl Robnett Licklider, l'un des créateurs d'ARPANET (un des premiers Internet) en expérimentation par l'armée et les chercheurs des universités américains. Les architectes réseaux schématisent cet accès par un nuage. En anglais, on le désigne alors par « The cloud ».

On a officialisé la naissance de l'internet le 12 mars 1989 par l'anglais Tim Berners-Lee. Il est à l'origine de l'invention du World Wide Web (protocole HTTP HyperText Transfer Protocol) et du HTML (la technologie des pages web), clef de voûte du cloud computing.

Dans les années 2000, les hébergeurs web font leur apparition et sont capables d'héberger des applications dans leurs locaux informatiques.

En 2006, les géants Google et Amazon reprennent le terme de "Cloud computing". Les premières applications à y être déployées sont le courrier électronique, les outils collaboratifs, le CRM1 (Customer Relationship Management), ainsi que les environnements de développement et de test.

Pour d'autres chercheurs, l'invention du cloud revient entièrement à Amazon qui, en 2000, louait ses serveurs avec le système "à la demande", à d'autres entreprises. En quelque sorte, c'est une optimisation de l'espace serveur non alloué à d'autres ressources informatiques.

Le recours aux technologies Cloud computing se développe à mesure que les besoins augmentent, la covid-19 a été un accélérateur dans le développement du cloud à travers le télétravail.

2. Définition (5)

Pour définir le Cloud computing selon le NIST (National Institute For Standard and Technology), le Cloud computing possède 5 caractéristiques essentielles, 3 niveaux de services et 4 modèles de déploiement.

Les 5 caractéristiques essentielles :

- Le service doit être en libre-service à la demande
- Il doit être accessible sur l'ensemble d'un réseau
- Il doit y avoir une mutualisation des ressources
- Il doit être rapidement élastique (adaptation rapide à une variation du besoin)
- Le service doit être mesurable (mesure et affichage de paramètres de consommation)

Le NIST présente 3 modèles (traditionnels) de service (Iaas, Paas, SaaS), avec l'évolution du cloud d'autres modèles se sont ajoutés dont le FaaS et le CaaS pour ne citer que ces deux-là ; 4 modèles de déploiement (public, privé, Hybride, multicloud).

3. Intérêt du cloud

Il s'agit de l'intérêt du cloud c'est-à-dire dans quel contexte cela s'inscrit et pourquoi cela se développe.
Les 3 mouvements conjugués qui ont poussés au développement du Cloud sont :

- Le cycle de développement de nouveaux produits est 2 fois plus rapide qu'il y a 10 ans. Il est donc nécessaire

de développer les applications supportant ces innovations 2 fois plus vite.

- Pour s'adapter à cela, les méthodes de développement ont évolué du classique développement en cycle en V (avec des étapes se succédant, besoins/ spécifications fonctionnelles, développement et mise enproduction avec une durée de 6 mois à 2 ans pour un projet), au développement des méthodes agiles le cycle complet (le développement est divisé en cycles de 3 semaines à 6 semaines avec une mise en production d'une partie des fonctionnalités au bout de chaque cycle de développement). Ce qui s'appelle aujourd'hui le DevOPS (c'est-à-dire l'intégration des développements et des opérations). Et en rajoutant la sécurité, cela est devenu le DevSecOps.

-Le développement de l'internet et des outils liés à ceux-ci a permis de créer des applications web accessibles via un simple navigateur avec des serveurs que l'on peut utiliser selon les besoins (notion de scalabilité).

4. Ecosystème du Cloud computing

Les éléments pouvant constituer l'écosystème du cloud sont entre autres :

Datacenter :

Datacenter signifie centre des données en anglais. L'objectif d'un Datacenter est d'héberger les sites web, les applications et les données pour les rendre accessibles aux utilisateurs. C'est dans ces bâtiments hautement sécurisés que sont gérés les équipements informatiques qui permettent de stocker, d'analyser et de traiter les données.

Il faut savoir que pour assurer efficacement son rôle d'hébergement et de mise à disposition des données et des applications, le Datacenter s'appuie sur différentes techniques qui garantissent la continuité d'activités et la tolérance aux pannes.
Cela commence par la gestion d'énergie pour alimenter les infrastructures informatiques mais aussi les dispositifs de refroidissement pour éviter aux serveurs toute surchauffe.
On a aussi les techniques de redondance en cas de panne des équipements et bien évidemment l'aspect sécurité qui est aussi un point central du Datacenter.

Sécurité physique du Datacenter :

Il faut savoir que le Datacenter est un site hyper sécurisé, vous ne pouvez pas rentrer comme ça et accéder aux serveurs et aux données hébergés. On passe généralement par un sas d'accès où l'identité est vérifiée, moyennant un badge d'accès par exemple plus la vérification de l'empreinte digitale, pour voir si la personne a bien les autorisations nécessaires. Le poids peut être aussi pesé à l'entrée et la sortie, le poids sera repassé pour être sûr que la personne n'embarque rien. De façon générale, un badge est nécessaire avec les autorisations spécifiques. Il y a aussi des caméras qui surveillent les différentes parties du Datacenter. L'ensemble du site est supervisé et une équipe tourne 24h/24, 7j/7 pour surveiller les différentes salles où l'on retrouve des alertes dès qu'une anomalie est détectée, par exemple au niveau du système de refroidissement ou coupure d'énergie, alerte incendie, mais aussi vol, intrusion etc.

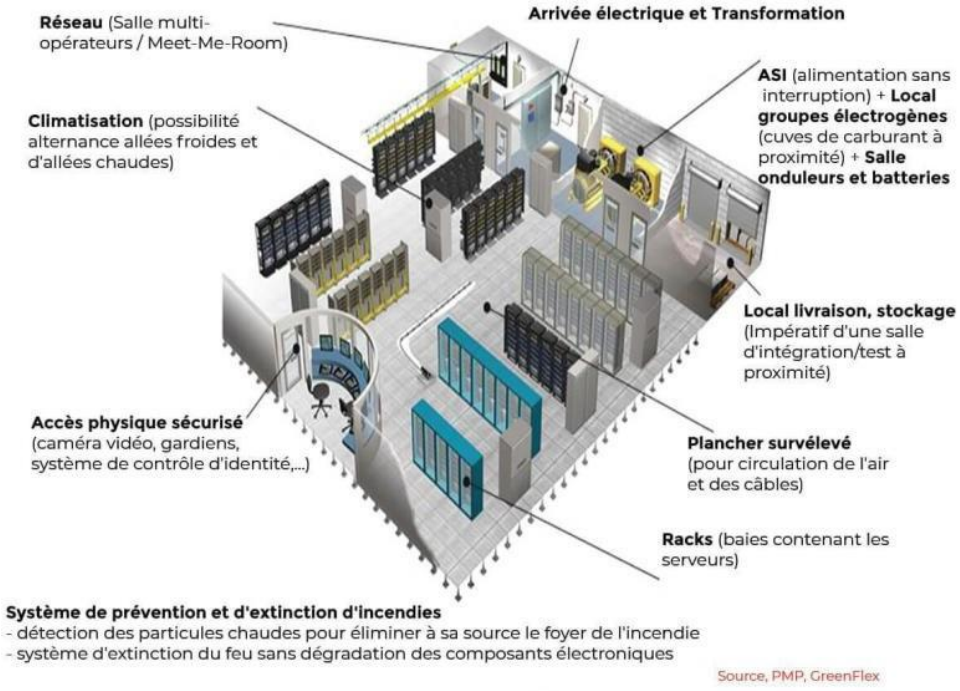


Figure 1 - Architecture d'un Datacenter (6)

Virtualisation :

La virtualisation est une des composantes du Cloud computing, elle permet d'optimiser les ressources informatiques et donc, de réduire les coûts et d'augmenter l'agilité de l'organisation.

La virtualisation consiste à faire fonctionner sur une même machine physique, plusieurs systèmes (OS) comme s'ils fonctionnaient sur des machines physiques distinctes. Son logiciel, appelé hyperviseur 1 (VM Ware) et hyperviseur 2 (VirtualBox) a pour fonction d'assurer entre autres :

- Assure le contrôle du processeur et des ressources de la machine hôte
- Alloue à chaque VM (Machine virtuelle) les ressources dont elle a besoin
- S'assure que ces VM n'interfèrent pas l'une avec l'autre.

Middleware :

L'expression middleware est une combinaison des termes « middle » signifiant milieu et « software » logiciel.
Le middleware est une couche « intermédiaire » technique qui se positionne entre l'OS et la couche applicative. Il joue également un rôle d'intermédiaire entre les différentes applications. Le but, c'est de permettre aux développeurs de se concentrer sur le métier de l'application lors de sa construction sans pourtant penser à toutes contraintes extérieures. C'est donc au Middleware de faire communiquer toutes ces applications hétérogènes qui n'ont pas été prévues pour interagir ensemble en natif.
Le Middleware fournit des services requérants permettant de faire circuler les données entre applications.

En résumé, trois points à souligner :

- Le middleware peut se situer au milieu des plusieurs sites physiques,
- Le Middleware permet aux données de transiter d'un site à l'autre,
- Le Middleware permet de réaliser des échanges asynchrones, c'est-à-dire deux applications n'ont pas

besoin d'être démarrées simultanément pour communiquer (ce qui veut dire que si une application B n'est pas disponible à un moment donné, le Middleware gardera les données et les lui transmettra dès que la liaison serait rétablie.

Il joue donc un rôle essentiel dans l'écosystème du cloud hautement distribué comme les micro-services, la mise en mémoire cache pour l'accès rapide aux données et aussi la messagerie pour le transfert rapide des données.

Cluster computing :

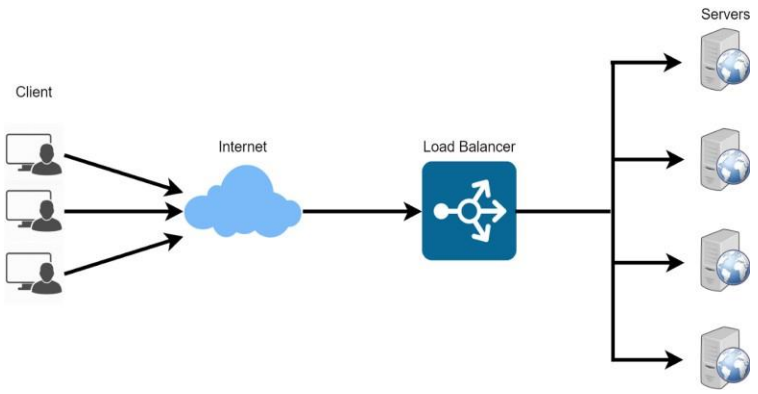


Figure 2 - Architecture simplifiée du cluster computing

Cluster signifie en français groupe ou grappe. Il désigne un groupe de serveurs vue de l'extérieur comme un seul et même serveur logique (machine virtuelle).

Le cluster répond à un double besoin :

- D'une part, les demandes de traitement d'application en augmentation constante auxquelles un seul serveur ne peut difficilement répondre,
- D'autre part une demande forte de haute disponibilité des applications.

C'est ce besoin de haute disponibilité qui amène à la redondance des serveurs pour garantir à la fois la continuité des services et pour se prémunir des pannes.

Le cluster Computing consiste également à connecter plusieurs ordinateurs pour résoudre de grands problèmes. Ainsi le fonctionnement des clusters permet de profiter d'une ressource de traitement de données centralisée. Un client dialogue avec le groupe de serveurs comme s'il s'agissait d'une seule machine ; ceci grâce à l'équilibrage de charge (load balancer) dans le Cloud computing.

Serverless (sans serveur) :

Un serverless désigne un ensemble de services qui sont proposés par les fournisseurs de cloud et qui nous permettent de s'abstenir de la gestion des machines. Les services varient en fonction des fournisseurs car la plupart proposent à leurs clients des services de bases de données et de stockage ou de plates-formes de type FaaS (Function-as-a-Service), comme : Cloudflare Workers, Stockage de fichiers, API, etc.

Concept du serverless computing :

Le concept de serverless est apparu en premier avec l'offre Lambda d'Amazon Web Service (AWS) en 2014. Depuis le catalogue des serverless s'est étendu et aujourd'hui plusieurs fournisseurs de services cloud en proposent : Microsoft avec Azure function, Google avec Google cloud function, IBM Cloud Functions et OVH cloud avec

OpenFaaS.

Le serverless est un modèle dans le cloud computing dans lequel le client peut créer, exécuter ses applications sans avoir besoin de se soucier de la partie infrastructure et notamment de la partie serveur, d'où le nom de serverless.

La particularité du serverless est très simple, le développeur a juste besoin d'une chose, fournir son code et tout le reste est à la charge du fournisseur de services cloud (fini les problématiques de stockage, de load balancing et d'autres problématiques réseaux, etc.). Le modèle serverless va donc faire abstraction de toute la partie infrastructure pour le développeur. Et, le développeur va donc pouvoir se concentrer sur son travail de développement.

Évidemment, il y a des principes à suivre avant d'entrer dans le modèle serverless. Il est demandé au développeur de repenser la conception de son code. En effet, le code d'exécution n'est plus celui de toute l'application. Le code d'application doit être alors décomposé en plusieurs fonctions. Chaque fonction a un seul et unique but, et l'ensemble de ces fonctions forment l'application. C'est pourquoi, on associe souvent au serveless les termes function as a service "FaaS".

API (Application programming interface) :

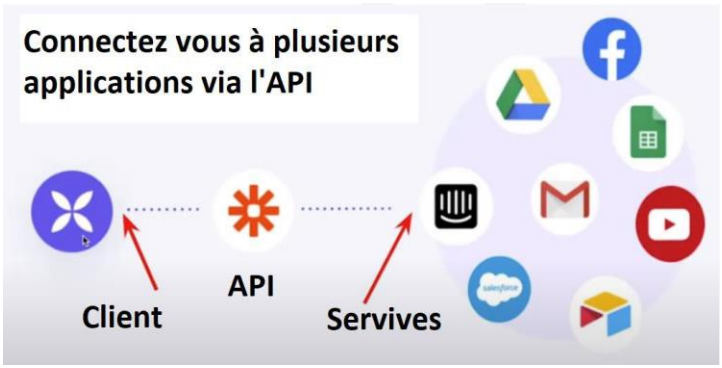


Figure 3 - Architecture d'API

En français le terme API signifie « Interface de programmation d'application », elle permet de connecter un logiciel ou service à un autre logiciel ou service dans le but d'échanger des données et des fonctionnalités. Il s'agit donc de faire dialoguer facilement plusieurs applications (consommatrice de service et productrice de ce service).
Il est à noter que sans les API, les "no code1 " n'existeraient pas. C'est grâce au modèle de FaaS plus précisément à l'utilisation des fonctionnalités du serveless que la technologie du "no code" est rendue possible. L'API simplifie le développement d'applications cloud-native (application développée et accessible dans le cloud) et permet une distribution continue et une flexibilité accrue.

DNS (Domain Name System) :

Lorsqu'on souhaite accéder à un site web, on utilise ce qu'on appelle un nom de domaine (par exemple www.google.com ou www.bsi-consulting.fr ou www.ege.fr). Sauf que dans la pratique, le navigateur n'a pas besoin de ce nom de domaine, il a besoin de savoir à quel serveur se connecter, donc l'adresse IP (Internet Protocol) du serveur sur lequel il va chercher les pages web. L'adresse IP, c'est justement un numéro d'identification qui va être attribué à chaque machine connectée sur internet (par exemple pour www.bsi-consulting.fr l'adresse IP est 16X.XXX.XXX.XXX ou pour www.ege.fr 10X.XXX.XXX.XXX).

C'est là qu'intervient le DNS (Domain Name System). Les serveurs DNS sont tout simplement des serveurs chargés de faire la correspondance entre les noms de domaine et les adresses IP. Grâce aux serveurs DNS, les internautes

n'ont pas à mémoriser les adresses IP. A savoir que le nom de domaine et l'adresse IP sont uniques.

Figure 4 - Illustration simplifiée DNS (7)

Quelques technologies génériques du cloud :

D'un côté se trouvent les technologies classiques VM et de l'autre les technologies microservices ou container qui font abstraction du sous-jacent infrastructure. L'intérêt des microservices est de permettre de passer d'un cloud public à un autre facilement puisque l'on s'abstrait. On trouve donc :

- Les VM ou les containers si on est en microservices
- Les outils de configuration
- Les outils de déploiement type Terraform
- Les outils de loadbalancing type Traefik
- Les outils de sécurité : IngressController, les services mesh, …

Outils de publication en ligne, premières tendances vers le cloud (8) :

- Messagerie : O365, Zimbra
- Outils d'édition : O365
- Outil collaboratif : O365 (Sharepoint), Tixeo
- Vidéo conférence : Zoom, Webex, Tixeo
- Applications métiers : toutes les applications en Saas : ERP (SAP, Oracle) / CRM (Salesforce, Hubspot, Cegid,) SCM, RH etc...

5. Types de Cloud Computing

On distingue les modèles de Cloud computing suivants : Public, privé, Hybride, communautaire et multicloud.

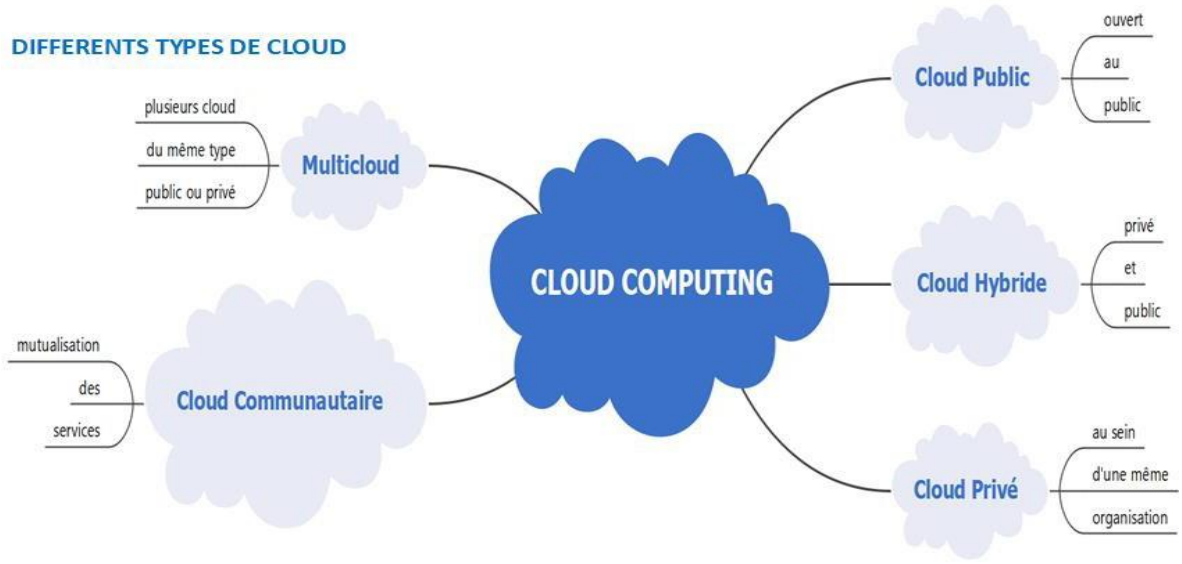


Figure 5 - Différents types de cloud

Cloud public (ouvert au grand public) :

L'infrastructure est dédiée à plusieurs clients et hébergée chez le fournisseur de service Cloud. Les clients consomment les services du Cloud public sans se soucier de l'emplacement géographique de leurs données.
Côté clients, pas besoin d'investissement initial car ils sont facturés à la demande pour consommer les services alloués. A contrario ce type de service demande des investissements lourds pour le fournisseur du Cloud.

Le Cloud public offre beaucoup de flexibilité, il est souvent moins cher qu'un Cloud privé pour le même service. Cependant, le Cloud public est moins sécurisé et inquiétant au niveau de la protection des données confidentielles.

Cloud privé (au sein d'une même organisation) :

L'infrastructure est dédiée à un seul client et adaptée à ses besoins. La gestion de celle-ci peut se faire soit en interne soit externalisée (Cloud privé virtuel) chez un hébergeur. Les entreprises qui s'orientent vers les Cloud privés le font généralement pour des raisons d'intégration et d'exigence de sécurité pour leurs données et applications critiques. Ce type de solution permet aux entreprises de mieux contrôler leurs données et applications situées géographiquement dans le périmètre de l'entreprise.

Le choix du lieu d'hébergement par l'entreprise dans le même pays peut s'expliquer par la problématique d'extraterritorialité (litiges juridiques dus aux différentes législations dans chaque pays hébergeur).
L'adoption du Cloud privé exige un investissement, des charges de maintenance, des compétences et des locaux appropriés pour les clients, sans compter les problématiques sécuritaires et de contrôles de données. A noter que, le Cloud privé exige d'énormes efforts en cas d'évolution des besoins.

Cloud hybride (Privé et public) :

Il s'agit d'un mélange entre les deux formes précédentes : certaines applications qui contiennent de données confidentielles ou critiques, par exemple, peuvent être stockées sur des Cloud privés, tandis que les autres sur des Cloud publics.
Le Cloud hybride permet donc de bénéficier des avantages de ces deux types de Cloud et correspond à une utilisation selon la criticité des données.

Cloud communautaire (mutualisation des services) :

C'est le partage des ressources numériques, de serveur ou de stockage au sein d'une communauté de collectivité ou d'acteurs publics qui caractérise le Cloud communautaire.
Ce choix peut aussi s'expliquer par les besoins de :

- Gouvernance partagée ou maîtrise de l'utilisation de données publiques,
- Sécurité,
- De fédération des serveurs, etc.

Grâce aux économies d'échelle réalisées, le Cloud communautaire apporte des bénéfices importants pour les collectivités.

MultiCloud :

Le Multicloud désigne l'utilisation des plusieurs Cloud du même type, gérés par différents fournisseurs.

En pratique, on utilise le multicloud parce qu'il n'existe pas de Cloud ultime qui répondrait à tous les besoins. Avec le multicloud, l'entreprise va choisir le Cloud qui répond au mieux à ses besoins. Elle peut prendre tel fournisseur parce que son IaaS est le moins cher, ou tel fournisseur pour son offre de CaaS plus performant ou s'inscrire à telle offre de PaaS qui correspond à tel besoin spécifique de ses développeurs.

6. Différents modèles de services de Cloud (On-Premise, IaaS, CaaS, PaaS, FaaS, SaaS)

En fonction des acteurs et des usages, on distingue les différents modèles de services de Cloud computing : **IaaS, CaaS, PaaS, FaaS, SaaS.**

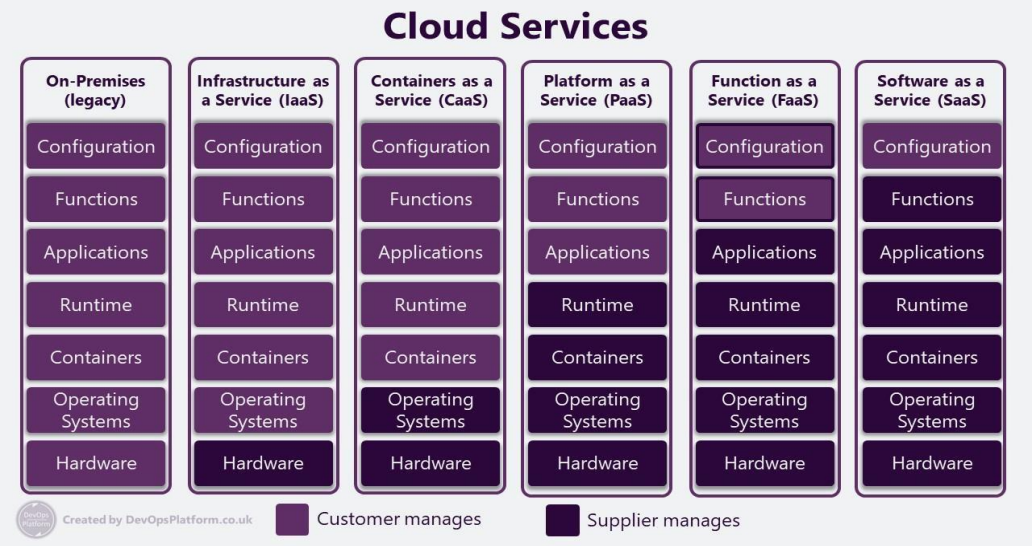


Figure 6 - Différents modèles de services Cloud
Source : *https://www.proen.cloud/en/blogs/enterprise-will-invest-on-cloud/*

Sur site (On-Premises) :

Le modèle sur site dit On-Premise est l'approche traditionnelle de la gestion des ressources informatiques. Cela sous-entend que l'entreprise contrôle la totalité des services informatiques et à l'entière responsabilité des infrastructures (données, serveurs, réseaux …) sans oublier le coût réel d'acquisition (ensemble des dépenses et des frais liés aux achats et à l'utilisation des équipements, des logiciels …).

Infrastructure en tant que service (IaaS) :

L'ensemble de l'infrastructure est externe à l'entreprise. Au lieu d'acheter le matériel directement, l'IaaS fournit l'infrastructure de Cloud computing, y compris les serveurs, les réseaux, les systèmes d'exploitation et le stockage via la technologie de la virtualisation.

Avec ce modèle, l'hébergeur du Cloud est responsable de la disponibilité des services et de la protection de données. Le client à l'entière responsabilité de la gestion des ressources informatiques (système d'exploitation et logiciels) dans le but de concevoir, déployer et exécuter ses applications.

Containers as a Service (CaaS) :

Conteneurs en tant que Service est l'un des acronymes de service Cloud qui propose une virtualisation basée sur des conteneurs.

Le CaaS permet à l'hébergeur du Cloud de fournir l'infrastructure, le système d'exploitation, le démon de conteneur (processus s'exécutant en arrière-plan), l'orchestration et d'autres ressources de calcul qui en découlent. Il met à la disposition de l'entreprise un environnement de programmation sans restriction relative. Il revient à l'entreprise de définir ses propres conteneurs (langages de programmation, environnement d'exécution, outils et frameworks).

Plateforme as a service (PaaS) :

La Plateforme "en tant que service" est une solution externe qui met à la disposition du client une suite logicielles et des outils d'intégration et de suivi.

Le PaaS est très utilisé pour le développement d'applications. Le fournisseur Cloud fournit l'infrastructure, les systèmes d'exploitation, les logiciels et gère le déploiement et l'hébergement des applications. Quant aux clients, ils utilisent la plateforme pour concevoir, développer et déployer les applications et assurer leur maintenance une fois mises en ligne.

Le client n'a plus à se préoccuper des coûts financiers liés à l'infrastructure et aux dépenses d'achats des logiciels, car la plateforme garantit la compatibilité des outils utilisés.

Function as a service (FaaS) :

Le FaaS englobe une partie des fonctionnalités de la technologie serverless basée sur un modèle de serveur à la demande. Il permet de gérer les fonctions de l'application sans que le client se préoccupe de la gestion de l'infrastructure.

Les fonctions sont de petits morceaux de code qui effectuent des actions singulières, un niveau plus petit que les microservices. Par exemple, les fonctions peuvent inclure la lecture, l'écriture, la mise à jour ou la suppression. Le client ne paie que pour l'exécution du code, si le code n'est jamais appelé, aucune charge financière ne serait retenue.

Software as a Service (SaaS) :

Le logiciel en tant que service enlève la majorité de la responsabilité aux clients. Les providers du Cloud fournissent l'infrastructure, les logiciels, les applications et les fonctions sur Internet. Les clients disposent normalement d'une sélection limitée d'applications et de fonctions à utiliser. SaaS comprend un large éventail de services bien connus et couramment utilisés tels que Dropbox, Office 365, Google Workspace, SAP, Service Now, Zoom, Outlook, etc. C'est le cas par exemple d'une location de logiciel de comptabilité en ligne chez un prestataire externe.

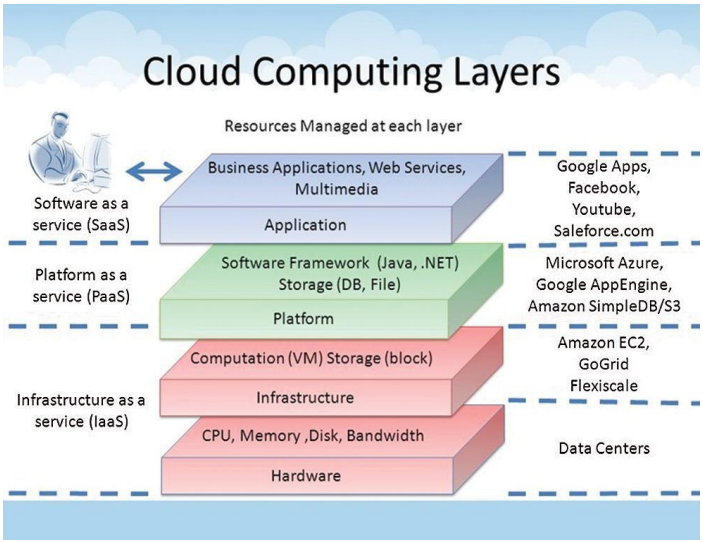


Figure 7 - Architecture du Cloud computing (9)

7. Atouts et Inconvénients des modèles de cloud

Atouts :

En cette année 2022, le cloud est devenu un outil incontournable, en voici quelques avantages.

- Rentabilité (pour de petits déploiements car au-delà c'est à discuter)
- Puissance
- Rapidité et simplicité
- Accessibilité et Archivage gratuit
- Gouvernance des données au niveau de l'entreprise
- Hébergement d'applications et de services
- Le Cloud computing facilite le télétravail

Inconvénients du Cloud computing :

- Problématique de la sécurité liée à l'environnement du cloud
- La dépendance

- Le Cloud computing n'est pas fiable à 100 %
- Les problèmes de connectivité peuvent créer des temps d'arrêt inattendus
- Des fonctionnalités offertes sont parfois insuffisantes
- L'interdépendance crée la vulnérabilité
- Le Cloud computing oblige une entreprise à se réinventer
- Le logiciel de sécurité, indispensable pour la protection des données
- Modification de la gouvernance d'entreprise
- Les garanties de disponibilité peuvent être très coûteuses
- La transition vers le Cloud computing prend beaucoup de temps.

Tableau récapitulatif d'atouts et inconvénients de modèles des services Cloud :

	Atouts	Inconvénients	Exemples
IaaS	Pas de frais d'infrastructure, Administration et Personnalisation, Flexibilité et évolutivité, Maintenance à la charge du fournisseur, Capacité de stockage infini, Sécurité.	Sécurité multi-locataire Dépendance au Provider Cloud Besoin d'un administrateur système Problème d'interopérabilité	AWS, Cisco Metacloud, Google Compute Engine (GCE) DigitalOcean, Linode, Microsoft Azure, Rackspace
CaaS	Compatibilité complète avec Kubernetes, Utilisation des conteneurs dans les Cloud Privés, publics et Hybrides, Portabilité élevée (Docker, Kubernetes), Services évolutifs, facturation à l'usage	Pas de support logiciel pour kubectl et Kubernetes, Technologie récente (limites), Risque de sécurité (externalisation des données), L'exploitation difficile des applications multi-conteneurs pour les multi-Cloud.	Amazon EC2 Container service (ECS), Google Container Engine (GKE), Microsoft Azure Container Service (ACS)
PaaS	Développement et déploiement d'applications (simples et rentables), Personnalisation d'applications, hautement disponible. Pas d'infrastructure nécessaire, Environnement hétérogène.	Sécurité de données, Problème d'intégration et de compatibilité (ancien système), Limitation des langages, Impossible de personnaliser Pas de personnalisation de la configuration des VM.	Amazon Web Elastic Beanstalk,Azure, Force.com (Salesforce), Google App Engine & Red Hat OpenShift, Heroku, Windows, etc.
FaaS	Service à la demande (vous ne payez que ce que vous consommez), Scaling automatique, Diminution du coût de la gestion de l'infrastructure, Possibilité de coder dans plusieurs langages différents, Une architecture agnostique (interopérabilité).	Dépendance aux fournisseurs du Cloud, Location de serveur, Des limitations techniques, Une technologie encore jeune, Ne convient pas aux tâches lourdes et complexes comme du traitement vidéo ou des ressources allouées en permanence.	AWS Lambda d'Amazon, Azure Logic App (Développement d'application No Code en quelques clics), Google Cloud Functions, IBM Cloud Functions, Microsoft Azure Functions (Open Source), OpenFaaS (Open Source).

SaaS	Pas d'installation et plus de licence, Migration, Accès à plusieurs travail collaboratif, sauvegarde automatique, Mises à jour automatiques, Déploiement rapide et mobilité, Facilité de stockage et récupération des données sur le Cloud, Avantage concurrentiel (accès aux dernières applications), vitesse élevée et grande performance.	Stockage non localisé, Logiciel limité, Dépendance des prestataires et problème d'Interopérabilité, Manque de service support d'intégration, Personnalisation minimale, Limitation des caractéristiques. Sécurité & Confidentialité : confiance à l'éditeur	Adobe Photoshop, Cisco Coffreo, DocuSign, Google Workspace, KeePass, Malwarebytes,Office 365, Oodrive, PayPal, Sage, Salesforce, TikTok, Webex, Whatsapp, WordPress.

Tableau 1 - Récapitulatif d'atouts et inconvénients de modèles des services Cloud

8. Risques de sûreté et sécuritaires du Cloud

En opérant dans le Cloud, les entreprises s'exposent à des risques tels que le déni de service, les logiciels malveillants, les cyberattaques, l'espionnage, les violations et pertes de données. Ces risques peuvent avoir des conséquences graves pour l'entreprise, notamment en termes de confidentialité et de sécurité des données. Il est donc important que les entreprises prennent toutes les mesures nécessaires pour minimiser ces risques.

Le manque de services ou de conseils informatiques empêche les petites entreprises de profiter pleinement des technologies du cloud et les rend vulnérables aux risques cyber. Elles doivent être conscientes des risques potentiels liés à l'utilisation des technologies du cloud afin d'éviter d'être pénalisées pour non-conformité.

Quelques risques cyber

Déni de service (10) :

Les petites entreprises ont pour habitude de s'orienter vers un cloud public, or ce dernier est généralement multilocataire. Les attaques sur les ressources utilisées par un ou plusieurs autres locataires peuvent également affecter vos opérations en perturbant votre activité et causer l'arrêt sur l'ensemble du réseau.
Exemple : Le 21 octobre 2016 DynDNS a été victime de cyberattaque, ce qui a rendu indisponible plusieurs sites web importants tels que Twitter, PayPal et Ebay pour une période prolongée d'un peu plus d'une dizaine d'heures sur toute la côte Est américaine. Il s'agissait d'une puissante attaque DDoS de plus de 1 téraoctet par seconde, brisant le record mondial de la plus puissante attaque DDoS.

Shadow IT "Informatique parallèle" :

Le shadow IT désigne l'utilisation d'équipement numérique pour ne pas dire informatique seulement, et de logiciels par les employés de l'entreprise sans l'accord du département Informatique. Sans précautions nécessaires, les employés et les gestionnaires ont tendance à contourner l'équipe IT et à télécharger des applications tierces telles que les SaaS qui permettent d'effectuer des tâches aléatoires comme, convertir des fichiers (JPEG en fichiers PDF), enregistrer des fichiers vidéo ou la messagerie instantanée).
Souvent, les fichiers sensibles sont téléchargés sur des serveurs cloud inconnus pour être simplement convertis en différents types de fichiers.

Bien que le BYOD (Bring your Own Divice) "apportez son propre matériel" permette aux entreprises d'économiser de l'argent sur l'équipement informatique, il augmente également les risques de sécurité dans le Cloud. Certaines de ces actions ne sont pas détectées la plupart du temps, il suffit qu'une seule donnée sensible soit diffusée au grand

public ou tombe entre les mains de la concurrence pour nuire à la réputation de l'entreprise. Les dispositifs volés, perdus ou mal utilisés peuvent également représenter un risque pour la confidentialité des données.
L'absence d'accords ou de contrat légal de niveau de service avec les fournisseurs de Cloud computing sont également des risques à prendre en compte.

Vol de données (11):

Ce type de pratique survient quand des pirates informatiques volent des informations d'identification de compte pour accéder aux applications et systèmes sur le Cloud, et représente l'un des risques les plus courants.
A titre illustratif, c'est le cas d'une divulgation en 2019 des données de la société de communication californienne VoIP (téléphonie IP), compromettant 7 millions de journaux d'appels et 6 millions de SMS ou plus récemment en 2021 d'une fuite massive des données de profil concernant 2,8 milliards d'utilisateurs de Facebook.

Perte de données :

Pour mieux comprendre, la perte de données s'explique par l'indisponibilité ou la destruction partielle ou complète d'information. Cela peut se produire par effacement accidentel, écrasement ou actions malveillantes de la part d'utilisateurs ou de pirates.

Exemple (12) : La société Codespaces victime d'attaque cyber, offrait l'hébergement en ligne de code source, n'est plus. Le service a été fermé après qu'un pirate eût pris le contrôle de l'interface d'administration et détruit un certain nombre de données hébergées par les clients. Pendant que l'équipe de Codespaces tentait de reprendre la main, en voulant changer les mots de passe, le pirate a réagi en détruisant des données. D'après l'équipe de Codespaces, la majeure partie de leurs données, de leurs backups, leurs données de configuration des serveurs virtuels et leurs backups hors-site ont été partiellement ou totalement détruits.

Non-conformité réglementaire :

Dépourvus de conseils juridiques spécialisés, les petites entreprises sont confrontées aux problématiques de déchiffrement des règles de protection des données, peu importe le pays dans lequel réside l'entreprise. Si les entreprises ne sont pas conformes aux différentes réglementations telles que le **HIPAA** (Health insurance Portability and Accountability Act), l'**HDS** (Hébergement de données de santé), le **PCI-DSS** (Payment Card Industry Data Security Standard), le **SOX** (Sarbannes-Oxley), le **RGPD** (Règlement Général de Protection des Données) et autres citées plus loin, alors de lourdes amendes pourraient leur être infligées.

La conformité aide les entreprises à établir une feuille de route pour déterminer la manière dont les données vont être stockées et protégées. Elle permet de définir qui doit avoir accès aux données et de déterminer les règles d'autorisations.

Exemple : En 2019, le Département de la Santé et des Services sociaux des États-Unis et l'« Office for Civil Rights » (OCR) ont annoncé le règlement d'une amende de 2,5 millions de dollars par la société CardioNet, basée en Pennsylvanie, en vertu de la loi HIPAA. La raison est la divulgation non autorisée de renseignements médicaux électroniques protégés et non sécurisés. Cela fait suite à une enquête de cinq ans concernant le vol de l'ordinateur portable d'un employé dans un véhicule contenant 1391 dossiers de patients.
Bref, la société CardioNet ne disposait pas d'un système d'analyse des risques, ni de processus de gestion des risques suffisants au moment du vol. Il s'agit de la première amende de ce genre et qui implique un fournisseur de services de santé sans fil. À noter que CardioNet est l'un des principaux fournisseurs de services mobiles de télémétrie cardiaque ambulatoire.
Source : Conformité HIPAA et phishing : les attaques entraînent d'énormes amendes HIPAA – TitanHQ

Menaces internes :

Les menaces internes sont traduites comme étant des actes intentionnels ou non intentionnels des employés partageant des données sensibles susceptibles d'exposer l'entreprise à des risques juridiques, financiers et opérationnels.
Cela comprend les individus négligents ou imprudents, ceux mal intentionnés (espionnage, la vengeance et le profit) ainsi que les cybercriminels.
Généralement ce type de risque est causé par des collaborateurs internes à l'entreprise.

Exemple 1 : Les vols de données sont plus fréquents lors du départ d'un employé. C'est le cas d'un vendeur qui quitte l'entreprise pour un concurrent et qui peut facilement télécharger des données clients à partir d'une application CRM sur le cloud. Ce type d'attaque est plus difficile à détecter que le vol de documents papiers.

Exemple 2 : Un employé mécontent divulgue des données matérielles et immatérielles à la concurrence « Brevets, licence, contrat ».

L'utilisation de plus en plus fréquente du Cloud computing fait apparaître de nouveaux risques de sécurité, augmentant ainsi l'intérêt des criminels à trouver de nouvelles vulnérabilités et exposant les utilisateurs à voir leurs données compromises. Dans la partie "Donnée", nous aborderons les enjeux liés à cette problématique, tant au niveau national ou international.

9. Les Acteurs du Web

Acteurs du Web dans le monde :

Sur le marché mondial, les 3 géants principaux du cloud qui font tous les types de cloud sont :

- Amazon Cloud services
- Google avec CGP
- Microsoft avec Azure

IBM et Oracle sont à considérer sur cet échiquier.
Depuis fin 2019, ces différents acteurs se partagent environ 80 % du marché mondial.

Dans d'autres régions du monde, certaines nations possèdent leurs propres géants :

- Chine avec Alibaba, Huawei, Datacloud, Tencent
- Russie avec Yandex

La souveraineté des Etats est menacée par l'hégémonie des 3 principaux clouders et leurs emprises sur l'intelligence artificielle et d'autres domaines numériques.

Acteurs du Web en France :

En France, il existe OVH Cloud, Oodrive, Ikoula, Orange Cloudwatt… qui se partagent le marché national avec les géants cités précédemment.

Principaux acteurs du secteur Cloud Computing :

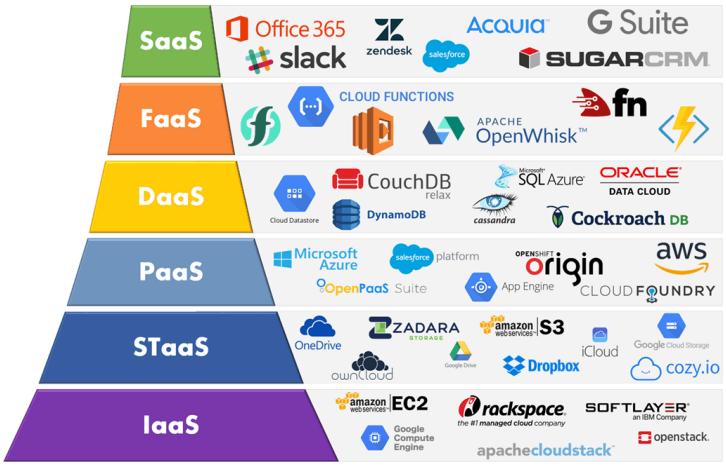


Figure 8 - Quelques acteurs du Cloud Computing

Les principaux acteurs mettent l'accent sur les solutions innovantes de Cloud computing pour renforcer la concurrence. Microsoft, Amazon Web Services, IBM, Alibaba, Oracle et Apple se concentrent sur la mise à niveau de leur portefeuille de produits existants. Ces sociétés fournissent une suite complète de services de Cloud Computing tels que Microsoft Azure, Google Cloud Platform (GCP), AWS Cloud, entre autres. En outre, ces entreprises développent et proposent désormais des solutions basées sur le Cloud avec des technologies innovantes telles que l'IA, le ***ML*** et d'autres pour améliorer leurs produits et fournir des solutions enrichies à leurs utilisateurs.

En 2021, le cloud a encore renforcé sa position de pilier central sur lequel repose le monde numérique, et des analystes prévoient un marché dix fois plus grand d'ici 2030 par rapport à 2020. La dépendance croissante vis-à-vis des technologies du Cloud s'accompagne d'une surveillance accrue à leur égard.

<u>Liste non exhaustive des principales entreprises présentées :</u>

- Amazon Web Services (AWS)
- Alibaba Cloud
- Oracle
- Google Cloud
- IBM Cloud
- iCloud
- Ikoula
- Microsoft Azure
- Numergy
- Orange Cloudwatt
- Outscale
- OVH Cloud
- Rackspace Technology
- SAP (Walldorf, Allemagne)
- TOO (France) Tixeo, Oodrive, Olvid, Scaleway
- VMware

Partie 2 : Les données dans le Cloud

1. Définition de la Donnée (13)

Une donnée est une information brute, sans contexte, un fait sans aucun arrière-plan. Elle ne peut pas être exploitée telle qu'elle. Une donnée brute peut prendre différents aspects. Cela peut être des données numériques, textuelles, ou un mélange de texte et de chiffres, mais aussi un tableau, un graphique…
Afin d'être utilisée et d'avoir une réelle valeur, une donnée doit passer par un processus. A proprement parler, une donnée est un 'input' dans le processus de transformation. Ce qui ressortira de ce processus de transformation, 'l'output', est l'information finale. Les informations sont des « données transformées ».

2. Différents types de données

Avant d'entreprendre un projet d'analyse de la donnée, il faut savoir prendre du recul car c'est une procédure très complexe et relève des compétences d'experts. Quel que soit le format des données, on peut les classer sous deux types : données quantitatives et données qualitatives.

Donnée qualitative

Ce type de données est très important dans la recherche d'expérience comportementale d'un utilisateur et dans la collecte des données d'une personne interviewée (sondage, opinions, doutes sur un produit, etc.).

Donnée quantitative ou numérique

Ce type de données est généralement mesuré, compté et exprimé par des chiffres (combien), ce sont des données issues de statistiques et donc structurées, ce qui signifie qu'elles sont définies et plus stables.
Les données quantitatives peuvent vous informer de ce qui s'est passé et enregistrer certains événements concernant un objet, une personne, etc. Elles sont subdivisées par catégories appelées données discrètes et données continues. Les données dites discrètes sont non divisibles en petite parties, par exemple : un véhicule n'est pas divisible.
Les données continues sont divisibles à l'infini et en petites parties ou qui fluctuent de manière continue, exemple : votre âge, votre poids, une démographie, etc. Les données représentent le carburant pour le fonctionnement des entreprises. Mais quel que soit leur format, les données sont classées en trois catégories : structurées, semi-structurées et non structurées.

Données structurées, non structurées et semi-structurées

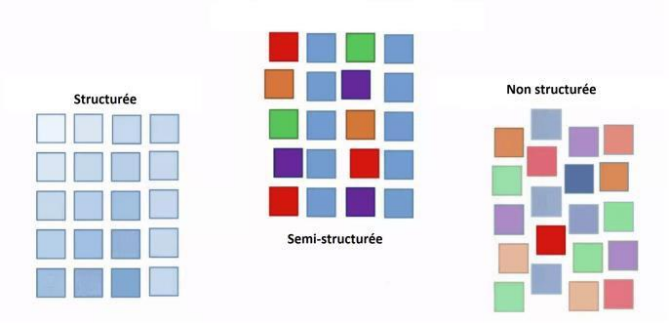


Figure 9 - Données structurées, non structurées et semi-structurées (14)

On peut différencier les données par les questions suivantes : qui, quoi, quand, où et comment ?

- Qui utilisera les données ?
- Quel type de données collecteriez-vous ?
- Quand traiterez- vous les données avant leur stockage ?
- Où stockez- vous les données ?
- Comment les données seront stockées ?

Ce type de questions fondamentales nous guiderons plus bas dans ce mémoire, vers le devenir des données dans le Cloud computing.
La structuration de ces données joue un rôle central dans la sécurité et sûreté des systèmes d'information (la confidentialité des données, l'intégrité des données, la disponibilité, l'authentification, la non-répudiation) et de communication au travers des normes, certifications etc….

Données structurées :
Les données structurées sont des données dont les éléments sont adressables pour une analyse efficace. Elles ont été formatées et transformées en un modèle de données bien défini.
Ces données sont générées par nous ou par les ordinateurs et sont stockées dans des bases de données relationnelles. Elles constituent le moyen le plus simple de gérer les informations.

<u>Les atouts des données structurées :</u>

- Leur traitement est facilité par les algorithmes de Machine Learning.
- Leur traitement est facilité par les utilisateurs professionnels types et qui connaissent le sujet.
- Leur connaissance approfondie n'est pas nécessaire car elles sont accessibles en source ouverte par les utilisateurs professionnels.

<u>Un des inconvénients des données structurées :</u>

- Il repose un manque de flexibilité.

<u>Quelques exemples de données structurées :</u>

- Les statistiques de l'INSEE et les données relatives aux citoyens, comme la naissance et la démographie (quantité).
- Les feuilles de calcul (Excel, logiciel de comptabilité ou de calculs, etc.).
- Une base de données orientée objet est un ensemble de données structurées

Données semi-structurées :
Les données semi-structurées sont considérées comme des données intermédiaires entre les données structurées et non structurées. Celles-ci ne résident pas dans une base de données rationnelle, mais possèdent des propriétés organisationnelles facilitant leur analyse.

Un autre exemple de données semi-structurées par rapport à des données structurées serait un fichier de données client délimité par des tabulations et une base de données contenant des tables CRM (Customer Relationship Management). D'autre part, les données semi-structurées sont plus hiérarchisées que les données non structurées ; un fichier délimité par des tabulations est plus précis qu'une liste de commentaires provenant du compte Instagram d'un client.

Données non structurées :
Une donnée non structurée peut être tout ce qui n'est pas dans un format spécifique (pas organisée de manière prédéfinie, en état brut, difficile à collecter, à traiter et à analyser).

Ces données sont plus nombreuses que les données structurées et se retrouvent partout sur internet plus précisément dans le Big Data d'où le besoin de data science pour les structurer.
Ce sont des données stockées dans des bases de données non relationnelles contrairement aux données structurées. Leur exploitation est un enjeu majeur pour les entreprises. Les informations à en tirer sont multiples et malgré les nombreux programmes informatiques, leurs traitements restent difficiles et complexes.
En fonction des besoins spécifiques de l'entreprise, les données non structurées présentent également des forces et des faiblesses.

Les atouts des données non structurées :
Parmi ces atouts, on retiendra les points suivants :

- Leurs formats natifs permettent d'obtenir une plus grande variété de formats de fichiers dans les bases de données non relationnelles, car quel que soit leurs formats les données peuvent y être stockées. Les professionnels de la donnée peuvent donc analyser les données dont ils ont besoin.
- Leurs accumulations est plus rapide, étant pas prédéfinies, elles peuvent être facilement collecté et rapidement traiter.

Les inconvénients des données non structurées :

- Le principal inconvénient des données non structurées est que leur préparation et leur analyse exigent d'être data scientiste.
- Étant non définies et non formatées, leur utilisation reste difficile par un professionnel standard.

Tableau comparative de la structure des données

Données Structurées	Données Semi-structurées	Données non structurées
Basées sur les tables de base de données relationnelle.	Basées sur XML/RDF.	Basées sur des caractères et des données binaires.
Dépendent du schéma et sont moins flexibles.	Plus flexibles que les données structurées, mais moins que les données non structurées.	Très flexibles et absence de schéma.
Très difficiles de mettre à l'échelle le schéma de base de données.	La mise à l'échelle est plus simple que les données structurées.	Très facile à mettre à l'échelle.
Exemple : base de données relationnelle (MySQL, SAP, Microsoft SQL, etc.).	Exemples : données XML, XHTML, carte heuristique (Mind mapping).	Exemples : Une facture, une donnée de surveillance, des contenues multimédia riches, un e-mail, tout ce qui est son, image, texte, Word, PDF, logs, fichier journal, etc.

Tableau 2 - Comparatif de la structure des données

Conclusion : Les données structurées ne représentent que 5 à 10% de toutes les données informatiques et 20% du total des données des entreprises.

Quel avenir pour les données ?
Indépendamment de votre choix d'utiliser des données structurées ou non structurées, l'intégrité de vos données est indispensable pour qu'elles restent une source fiable. Il est préférable d'utiliser des pratiques de gouvernance des données et des techniques de gestion des données reconnues pour assurer leur intégrité.

Pour résumer une donnée n'est pas une information. Une donnée requiert une interprétation pour devenir une information (données traitées).

3. Données à caractère personnel (DCP)

Définition (15)

Selon la Cnil, une donnée à caractère personnel est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc. Peu importe que ces informations soient confidentielles ou publiques.

A noter : pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.

Attention : s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.

En ce qui relève des données sensibles se rapportant à la vie privée d'une personne physique, nous vous invitons à prendre connaissance de certains exemples :

- L'origine raciale et ethnique
- L'opinion politique
- La croyance et religions
- L'opinion philosophique
- L'appartenance syndicale
- Les données génétiques et biométriques
- Les caractères physiques

Ces données permettent d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

- Si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
- Si les informations sont manifestement rendues publiques par la personne concernée ;
- Si elles sont nécessaires à la sauvegarde de la vie humaine ;
- Si leur utilisation est justifiée par l'intérêt public et autorisée par la Cnil ;
- Si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Données du secteur public :

La notion de « donnée publique » couvre l'ensemble des données qui sont ou devraient être (légalement ou volontairement) publiées ou tenues à disposition du public, et qui sont produites ou collectées par un État, une collectivité territoriale, un organe parapublic, dans le cadre de leurs activités de service public.

Données sensibles du secteur privé (entreprise) :

Pour une organisation quelle qu'elle soit, sont considérées comme données sensibles, les informations ayant une valeur économique et/ou stratégique, dont la fuite, l'altération, l'obtention, la détention, la divulgation ou l'utilisation illicite leur seraient préjudiciables. Elles concernent ces cinq grandes catégories :

- **Les données liées aux personnes :** collaborateurs, partenaires extérieurs, fournisseurs, clients et prospects, (Contrats de services, contrats de travail) etc.
- **Les données liées aux métiers de l'entreprise :** savoir-faire, secrets de fabrication, documents de propriété intellectuelle, méthodes de conception, plans de production, prototypes, (Brevets, licences) etc.
- **Les données stratégiques et organisationnelles :** documents issus des instances de gouvernance, décisions stratégiques, orientations, projets de recrutement, synthèses R&D, etc.
- **Les données économiques et financières :** trésorerie, montages financiers, rémunérations, politiques tarifaires, conditions d'achat auprès des fournisseurs, budgets prévisionnels, etc.
- **Les données juridiques :** toute information liée aux contraintes légales ou de conformité (RGPD, Bâle II, etc.).

Il existe également une loi dite "de blocage" pour la protection des entreprises contre les lois extraterritoriales.

4. Aspects Juridiques de la donnée (catégories de régimes de protection légale des données)

Désignation	Famille juridique	Référence légale
Donnée de la nature militaire, diplomatique, politique, recherche	**Secret de la Défense nationale**	L. 2311-1 du code de la défense, article 409-3 du code pénal ; Instruction générale interministérielle (IGI) 1300 du 30 novembre 2011 sur la protection du secret de la défense nationale
Informations personnelles	**Données à caractère personnel**	Loi N°78-17 du 6 janvier 1978 Informatique et liberté-RGPD (UE-2016)
Informations médicales relatives aux patients	**Données de santé à caractère personnel**	Code de la santé publique RGPD article 6
Données de recherche, données stratégiques et techniques	**Informations relevant du potentiel technique et scientifique de la nation présentes au sein des zones à régimes restrictifs (ZRR)**	Décret 2011-1425 du 2 novembre 2011, arrêté du 3 juillet 2012 et la circulaire. n°3414/SGDSN/AIST/PST du 7 novembre 2012

Secret des affaires, savoir-faire, données confidentielles	**Informations économiques non divulguées**	Directive UE n°2016/943 du 8 juin 2016 (article 39.2 du traité ADPIC du 14 octobre 1994) article 151.1 du code de commerce
Données stratégiques sur support numérique	**Informations sensibles des opérateurs d'importance vitale (OIV)**	Article R.1332-1 et S. du code de la défense en application de l'article 22 de loi de Programme militaire (LPM) n°2013-1168 du 18 décembre 2013
Données numériques essentielles	**Données traitées par les Opérateurs de services essentiels (OSE)**	La directive (UE) 2016/1148 du 6 juillet 2016 dite NIS-Loi n°2018-133 du 26 février 2018
Informations autres que personnelles	**Données non personnelles**	Directive (UE) sur la donnée non personnelle

Tableau 3 - Aspects Juridiques de la donnée (catégories de régimes de protection légale des données) (16)

5. Classification et Protection de la donnée

Classifier les données est une première étape cruciale pour mettre en place une stratégie efficace de sécurité des données. En effet, cela permet d'identifier les zones à risques et ainsi de mieux cibler les mesures de protection à mettre en place.

La protection des données est indéniable pour les entreprises et les États. Ces derniers doivent mettre en place des mesures idoines pour sécuriser leurs données confidentielles, critiques, sensibles afin de se prémunir des actes intentionnels, malveillants… pouvant nuire à leurs activités ou à la sécurité nationale.

Nous avons tendance à dire « je n'ai rien à cacher » ou plutôt à dire « nous avons des données à protéger » exemple : code de carte bancaire, nos informations de santé. Les entreprises doivent protéger leurs données (savoir-faire, brevet, licence, contrat etc…).

Pour protéger ses données, chaque entreprise ou État élabore son système de classement. A savoir, toutes informations (dossiers, documents) liées aux entreprises ou à l'Etat ne sont pas en libre accès, c'est pour cela qu'il faut hiérarchiser des niveaux d'accès aux données car, les enjeux et les risques en cas de fuite ou divulgation non autorisée sont préjudiciables.

Il existe des règles strictes relevant de la défense nationale, mentionnées dans les articles R. 2311-2 et R. 2311-3 du code de la défense qui définissent trois niveaux de classification restreignant l'accès ou la diffusion des documents : Très Secret-Défense, Secret-défense, Confidentiel-Défense.

En dehors de cette classification, il existe un système de classification des données (documents) généralement utilisé par les entreprises. Ce système permet d'attribuer une mention afin de définir la valeur et l'importance des données appartenant à une entreprise, en mettant en place un niveau de protection pour y accorder l'accès.

Voici un des exemples de classification sur quatre niveaux :

NC – Non classifié : Cette mention s'applique uniquement aux informations qui peuvent circuler librement à l'extérieur d'un périmètre donné (un ministère, une entreprise, etc). Ces informations ne justifient d'aucune protection particulière.

C1 – Usage interne : Il s'agit du niveau par défaut. Ce niveau regroupe les informations qui ne doivent être communiquées à personne en dehors de l'organisation.

C2 – Diffusion restreinte : cette mention s'applique aux informations qui ne doivent être communiquées (y compris à l'intérieur du périmètre de l'organisation) qu'aux personnes directement concernées et identifiées. La divulgation

de ces informations pourrait nuire au fonctionnement d'une entité ainsi qu'au bon déroulement d'un projet ou d'une mission.

C3 - Secret : Ce niveau est réservé aux informations rares dont la divulgation à des personnes non autorisées pourrait mettre en péril les intérêts stratégiques de l'organisation, sa sécurité, voire son existence.

Source : Code de la défense - Article R2311-2 - Article R2311-3 (codes-et-lois.fr)

6. Sécurité de la donnée

Un système d'information sécurisé est le fondement de la sécurité de la donnée. Il repose sur les 5 éléments clés suivants :

- La confidentialité des données informatiques
- L'intégrité des données
- La disponibilité des données informatiques
- La non-répudiation
- L'authentification

Par ailleurs, la donnée est représentée sous 3 états et doit être protégée en conséquence :

- Au repos, appelée parfois donnée froide : elle est stockée sur un support à un instant donné et est chiffrée
- En mémoire vive chez l'hébergeur (appelé protection contre le service) ou est en cours de manipulation ou d'utilisation à un instant donné : aucune protection possible à ce jour
- En transit, également appelée donnée chaude : elle se déplace d'un équipement à un autre à un instant donné. Le chiffrement de la donnée se fait en VPN IPSEC ou SSL

Au-delà de cela, un certain nombre de mécanismes de protection de la donnée existe tel que :

- L'authentification des utilisateurs qui peut être simple (login/ mot de passe) ou multi facteur (login/mot de passe + SMS ou email ou mot de passe à usage unique ou code d'authentification unique, empreinte cryptographique avec une clé)
- Mise en place d'un bastion pour gérer les comptes à privilèges
- Un système de provisioning des utilisateurs définissant les droits sur les applications (IAM : Identity Access Management)

Au niveau organisationnel / développement, la protection ultime est l'usage de :

- L'anonymisation : une donnée ne peut être reliée à une personne
- La pseudonymisation qui est un traitement de données à caractère personnel de manière qu'on ne puisse pas attribuer les données à une personne physique sans avoir recours à des informations supplémentaires.

La protection de la vie privée et la sécurité des données sont primordiales dans l'utilisation des services Cloud. Ces données peuvent être la cible de plusieurs attaques.
Malgré les technologies sur lesquelles se basent le Cloud computing, il subsiste des nouveaux risques et des vulnérabilités de sécurité propres au Cloud en plus des risques des environnements traditionnels.

En effet, plusieurs clients partagent les mêmes infrastructures, ce qui conduit aux risques de visibilité des données par d'autres utilisateurs. L'accès au Cloud se fait par les interfaces de gestion basées sur le web, rendant la probabilité d'un accès non autorisé plus élevée en comparaison aux systèmes traditionnels.

De ce qui précède, on peut lister les principales menaces comme suit : abus et utilisation malveillante du Cloud computing, interfaces et API non sécurisés, malveillances internes, problèmes dus au partage de technologie, perte ou fuite de données, détournement de compte ou de service et enfin profil de risque inconnu.

Le Cloud computing est une technologie très prometteuse permettant à ses clients de réduire les coûts d'exploitation, d'administration etc. Tout en augmentant l'efficacité, toutefois, l'adoption de cette technologie reste faible, et cela revient aux problèmes de sécurité en particulier la sécurité des données échangées sur le réseau internet.

Conseils (18)

- Mettre en place une politique stricte de mot de passe
- Mettre en place des accès restreints aux données
- Sauvegarder très régulièrement les données de l'entreprise
- Utiliser un VPN professionnel
- Mettre en place une application de blocage et gestion des flux internet
- Chiffrer les données de l'entreprise
- Sécuriser les postes de travail par un antivirus, etc

La sécurité inclut le chiffrement des données, la gestion des clés, leur masquage ainsi que la surveillance et l'audit.

7. Gestion des données

La gestion des données désigne l'ensemble des pratiques nécessaires à la construction et maintenance d'un cadre/framework pour l'importation, le stockage, l'exploration et l'archivage des données qui sont nécessaires aux activités de l'entreprise.

Contractuellement, il faut prévoir :

- La sauvegarde de la donnée doit également se faire dans le cloud (Exemple : l'incendie du Datacenter d'OVH à Strasbourg)
- La réversibilité qui est la capacité à récupérer facilement ses données pour les porter ailleurs

Support et stockage des données

Pour la bonne conduite de l'activité, les données sont devenues stratégiques pour toute entreprise, leur stockage ou sauvegarde étant un impératif.
Avant tout, il faut prendre en compte la complexité du stockage des données numériques par rapport au stockage sur un support papier. Différents supports de stockage sont à ce titre disponibles sur le marché.
En voici les principaux :

- Le disque dur ordinateur (interne, externe)
- Les serveurs/sur site et ou cloud (disques durs réseaux, serveurs RAID/NAS "Redundant Array of Independent Disks"/ "Network Attached Storage")
- La clé USB "Universal Serial Bus" (support de stockage mobile)

- CD “Compact Disc” et DVD “Digital Versatile Disc” (support de stockage classiques
- PCD (Protein-coated disks, La technologie de disque optique enrobé de protéines)
- HVD (Holographic Versatile Disks, même famille que le DVD pouvant atteindre 50 téraoctets)
- Les cartes mémoires (pour les besoins assez restreints)
- La mémoire vive RAM “Random Access Memory”

Externalisation (19)

Le principe de l’externalisation de service consiste à aider les entreprises à se recentrer sur leur cœur de métier en déléguant certaines opérations à une entité tierce (spécialisée en la matière). L’objectif est de gagner du temps et réduire les coûts de l’entreprise.

Dans le cas d’une entreprise désirant migrer vers le Cloud computing, il serait souhaitable :

- Qu’elle s’entoure des ressources expérimentées afin d’éviter les coûts cachés,
- De prendre les bonnes décisions adaptées à ses besoins,
- De ne pas oublier les aspects sécuritaires et juridiques relevant de la responsabilité partagée.

Dans la même perspective, l’Agence nationale de sécurité des Systèmes d’Informations (ANSSI) a mis en place un guide pour mieux comprendre les enjeux du Cloud computing. Les points suivants y sont évoqués :

- Les avantages et inconvénients,
- Les risques liés à la sous-traitance,
- Les risques liés à la localisation des données,
- Les risques liés aux données à caractère personnel,
- Les risques liés aux choix techniques du prestataire,
- Les risques liés aux interventions à distance,
- Les risques inhérents aux interventions à distance,
- Les risques liés à l'hébergement mutualisé.

Durée de conservation de la donnée

Cette partie s’adresse aux structures publiques et privées qui sont amenées à collecter et utiliser des données à caractère personnel. En finalité, elles devront respecter les règles se rapportant à la conservation, l’archivage et la durée de vie des données traitées, encadrées par le RGPD et le Code du patrimoine.
Selon le traitement, les données personnelles poursuivent un cycle de vie en trois phases.

Conservation en base active :

Il s’agit de la durée nécessaire à la réalisation de l’objectif (finalité du traitement) ayant justifié la collecte/enregistrement des données. Par exemple, dans une entreprise, les données d’un candidat non retenu seront conservées pendant 2 ans maximum (sauf s’il en demande l’effacement) par le service des ressources humaines.
En pratique, les données seront alors facilement accessibles dans l’environnement de travail immédiat pour les services opérationnels qui sont chargés de ce traitement (exemple : le service des ressources humaines pour les opérations de recrutement).

Archivage intermédiaire :

L’archivage intermédiaire concerne :

- Les données personnelles qui ne sont plus utilisées pour atteindre l’objectif fixé « dossiers clos »,
- mais présentent encore un intérêt administratif pour l'organisme (exemple : gestion d’un éventuel contentieux, etc.)
- ou doivent être conservées pour répondre à une obligation légale (par exemple, les données de facturation conservées dix ans en application du Code de commerce, même si la personne concernée n’est plus cliente).
- Ces données peuvent alors être consultées de manière ponctuelle et motivée par des personnes spécifiquement habilitées ;

Archivage définitif :

En raison de leur « valeur » et intérêt, certaines informations sont archivées de manière définitive et pérenne.
À la différence de la conservation en base active, les deux dernières étapes ne sont pas systématiquement mises en place. Leur nécessité doit être évaluée pour chaque traitement, et, pour chacune de ces phases, un tri sera opéré entre les données :

- L’identification de la durée de conservation des traitements
- La définition de la durée de conservation relève de l’analyse de conformité que le responsable doit mener pour son traitement.

Dans certains cas, la durée de conservation est fixée par la règlementation (par exemple, l’article L3243-4 du Code du travail impose à l’employeur de conserver un double du bulletin de paie du salarié pendant 5 ans).
Toutefois, pour de nombreux traitements de données, la durée de conservation n’est pas fixée par un texte. Il appartient alors au responsable du fichier de la déterminer en fonction de la finalité du traitement.
La CNIL fournit un guide de conservation des données, ainsi que le référentiel de durée de conservation relevant du domaine de la santé (20).

Partie 3 : Cadre réglementaire et normatif autour du Cloud

Arrêt des recherches le 12 octobre 2022.

Avant de migrer leurs données dans le Cloud, les TPE/PME doivent comprendre les risques juridiques auxquels elles s'exposent et comment s'en protéger. Elles doivent également parfois répondre aux besoins de mise en conformité à travers le cadre normatif.

Cette partie étant traitée sous l'angle de la donnée, il serait intéressant de rappeler les différents types de données et leur contenu :

- Données publiques : toute donnée dans le domaine public
- Données personnelles : nom, prénom, visage, ADN, numéro de téléphone direct ou indirect, appartenance religieuse, politique et syndicale, adresse IP, Géolocalisation
- Données anonymisées/pseudonymisées : respectivement identifiants séparés des autres données, aucune identification possible. Elles peuvent être mises dans un Cloud public
- Données sensibles : données personnelles, données des agents de l'État, données à portée d'intelligence économique (répond aux exigences SecNumCloud)
- Données classifiées telles que les données relevant de diffusion restreinte, confidentiel, secret (seuls Trustednest de Thales et les Cloud de l'État pour la diffusion restreinte peuvent être dans le Cloud)

D'un point de vue réglementaire, le marché du Cloud présente une incohérence entre les réglementations étrangères, notamment américaines, et européennes.

Afin d'établir un cadre juridique strict concernant les flux de données, plusieurs réglementations ont été mises en œuvre telles que le RGPD depuis 2016 en Union Européenne ou le Cloud Act aux États-Unis.

Quant à la libre circulation des données personnelles, l'invalidation du Privacy Shield (affaire Schrems II) par la Cour de Justice de l'Union Européenne en 2020 a mis en évidence une incompatibilité de la réglementation américaine avec les principes du RGPD.

De ce fait, les entreprises transférant des données personnelles de citoyens européens vers des serveurs d'entreprises non européennes, même localisés en Europe n'ont plus de base légale pour le faire et s'exposent à un risque juridique car les fournisseurs de Cloud internationaux accèdent à leurs données confidentielles. Un exemple d'incompatibilité est que l'un des principes du RGPD assure la sécurité et la confidentialité des données à caractère personnel alors que les fournisseurs de Cloud américains ne peuvent les garantir à l'égard des autorités américaines.

Le cadre réglementaire européen, français, quelques lois étrangères (russes, chinoises et américaines), de même que le cadre normatif français sont abordés dans ce chapitre afin de clarifier les principaux aspects afférents à ces thématiques.

Chapitre 1 - Réglementations EU :

Au sein de l'UE, il n'existe pas de service dédié aux sujets Cloud. Les institutions européennes *(Annexe 2)* interviennent d'une manière plus étendue dans le domaine du numérique, de la cybersécurité et de la sécurité des systèmes d'informations en général. Avec comme objectif principal la régulation du marché du Cloud au sein de l'UE, dans le cadre de la stratégie Cloud computing (adopté le 16 mai 2019) (21).

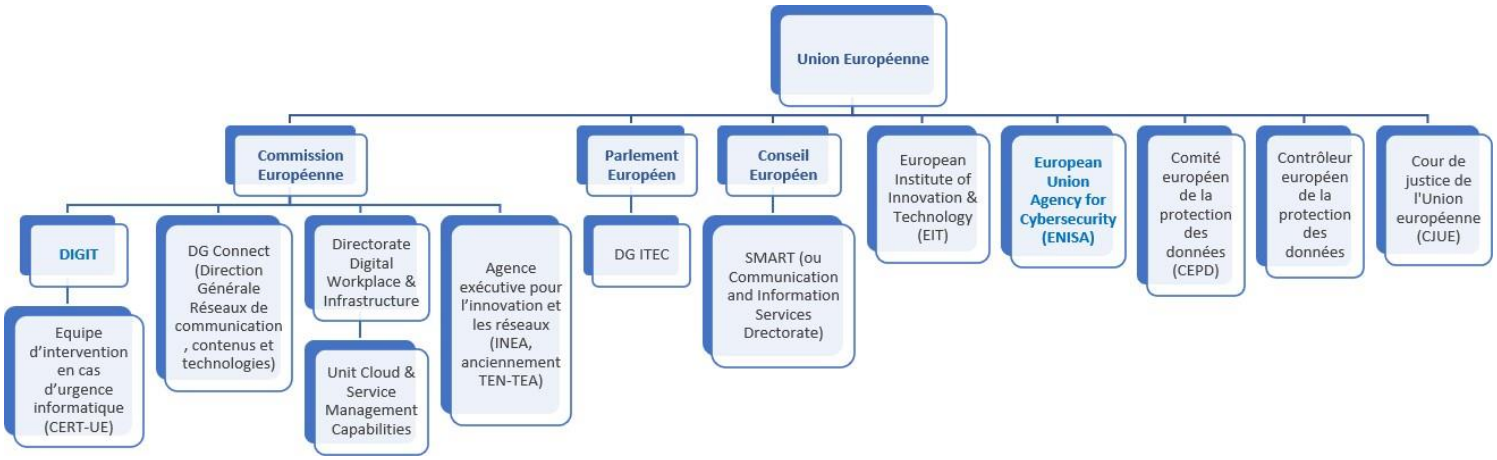


Figure 10 - Organigramme des institutions européennes
Source : Rapport des travaux des auditeurs de la promotion MIE25 de l'école EGE, en collaboration avec l'ANSSI sur « La souveraineté dans les stratégies nationales du cloud en Europe » 2022.

1. Réglementations EU pour les données non personnelles

1.1. Règlement EU 2018 1807 sur la libre circulation des données non personnelles

Définition et objectifs du règlement

Le règlement UE 2018 1807 (22) a été adopté par le parlement et le conseil européens le 14 Novembre 2018 et il est entré en vigueur le 27 Mai 2019.
Il rentre dans le cadre de la stratégie du **marché unique numérique** proposée par l'Union européenne. Le règlement a trois principaux points :

- Permettre une libre circulation des données **non personnelles** au sein de l'Union européenne. Il complète le RGPD qui prévoit ce principe pour les données personnelles.
- Rendre disponible les données pour les autorités compétentes et faciliter leur traitement transfrontalier avec les procédures de coopération entre les autorités.
- Permettre le portage des données afin d'ouvrir le marché de **la concurrence entre les fournisseurs de services informatiques dont le Cloud**.

Le ***CEPD*** est l'autorité responsable de son contrôle au sein de l'***UE***.

Application du règlement

Il s'applique à toutes les données autres que les données personnelles listées par le RGPD : Données non personnelles publiques ou privées. Il vise le traitement des données au sens le plus large, quel que soit le type de système informatique utilisé, qu'il ait lieu dans les locaux de l'utilisateur ou qu'il soit externalisé chez un fournisseur de services. Couvrant tous les niveaux de traitement depuis le stockage des données (infrastructure à la demande) jusqu'au traitement des données sur des plateformes (plateforme à la demande) ou dans des applications (logiciel à

la demande).

Le règlement **ne s'applique pas aux services de traitement des données ayant lieu en dehors de l'Union européenne** ni aux exigences de localisation relatives à ces données.

Il doit être respecté par tous les états membres au sein de l'Union européenne (sauf si une restriction ou une interdiction se justifie par des motifs de sécurité publique) et s'applique aux personnes physiques ou morales qui fournissent des services de traitement de données aux utilisateurs résidant ou ayant un établissement dans l'Union, **y compris à celles qui fournissent des services dans l'Union sans y avoir d'établissement**.

En termes d'exemple d'application, on retrouve les banques. En effet, en plus des données personnelles, elles traitent aussi de nombreuses données non personnelles, il peut s'agir de données pour l'évaluation quotidienne des risques auxquelles elles sont exposées (risques financiers, climatiques...) ou encore de données de clients personnes morales (entreprises). Elles sont très consommatrices du Cloud computing exploitant l'IA. Elles sont donc concernées par le règlement d'abord comme fournisseur de services bancaires mais aussi en tant qu'opérateur de traitement pour leurs besoins.

Sanctions, points forts ou désavantages (concurrentiels)

Parmi les points forts du règlement, on peut noter qu'il **favorise la circulation des données non personnelles** et la croissance du marché européen basée sur les données en **supprimant les règles nationales qui imposaient des exigences de localisation des données**.

L'un de ses points durs, c'est qu'il ne prévoit pas de règles contraignantes pour le secteur privé en ce qui concerne les échanges des données (récupération ou transfert des données à un autre prestataire). Pour les accords conclus entre les entreprises et les prestataires de services, un choix de **l'auto-régulation** a été fait. Mise en place, par exemple, d'un contrat (suivant un modèle établi en amont) pour organiser la manière dont les données seront transférées suite à la demande du client.

Le Secret des affaires « SDA » : Parmi les données non personnelles, on retrouve des données à forte valeur et qui méritent d'être hautement protégées. Ces dernières peuvent comprendre des informations stratégiques ou financières comme elles peuvent contenir des données industrielles représentant le savoir-faire de l'entreprise ou encore ses brevets. Afin de mieux protéger les entreprises européennes face à l'espionnage économique et industriel, le Parlement européen a adopté une directive sur le secret des affaires le 14 Avril 2016. La violation du secret des affaires peut être engagée par l'obtention, la divulgation ou l'utilisation illicite d'informations. Les sanctions sont définies par les lois transposées dans chaque pays membre (Pour la France, voir la partie *1.1 Le secret des affaires (SDA)).*

2. Réglementations EU pour les données personnelles

2.1. Le Règlement général sur la protection des données personnelles (RGPD)

Définition et objectifs du règlement

Le règlement (UE) 2016/679 (23) sur la protection des données personnelles (RGPD) a été initié en 2012. Il a été adopté le 27 Avril 2016 et il est entré en application le 25 Mai 2018.

L'objectif principal de ce règlement est de fournir aux citoyens européens plus de **contrôle sur leurs informations privées** tout en harmonisant les régimes juridiques en matière de protection des données à caractères personnels en Europe. Ses points forts résident en :

- Son **principe d'extraterritorialité** qui, en fonction des situations, permet d'étendre son champ d'application au-delà des frontières européennes.
- Son concept de **« Privacy by Design »** : l'objectif est de garantir que la protection de la vie privée soit prise en compte dès la conception du service ou du produit amené à traiter, utiliser ou collecter des données

personnelles.

- Son concept de **« Privacy by Default »** : L'idée est que le système de protection mis en œuvre soit activé par défaut sans l'intervention de l'utilisateur.

L'autorité de contrôle du RGPD est l'Etat membre dans lequel se trouve l'établissement principal de l'entité. Pour la France, ça sera le CNIL qui en est responsable (Voir partie *2.1 La loi informatique et liberté (loi I&L), le règlement général de protection des données (RGPD)*).

Le règlement donne **pouvoir aux autorités de contrôle à travers l'application de sanctions répressives**. Il met en œuvre aussi un mécanisme de coopération entre les autorités de contrôle qui peuvent mener des actions conjointement et **s'échanger des informations** dans le cas où le responsable du traitement ou le sous-traitant ont **des entités dans plusieurs pays de l'Union européenne**.
Le comité Européen de la Protection des Données pilote le règlement et publie de la documentation dans ce cadre.
Il réunit les autorités de protection nationales et traite les désaccords entre elles.
Il s'assure de l'application uniforme du règlement au sein de l'Union européenne et il est l'émetteur de décisions contraignantes dans le cadre de procédures de sanctions.

Application du règlement

Le RGPD est directement applicable dans tous les pays de l'Union européenne. Il s'applique aux traitements des données comportant des informations ou des données relatives aux **personnes physiques identifiées ou identifiables directement ou indirectement**. Sont visés, les traitements des données à caractère personnel, automatisés en tout ou en partie, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier. Il n'y a pas de distinction si les traitements ont été mis en œuvre par une personne physique ou une personne morale de droit public ou de droit privé.
Les acteurs concernés par le règlement sont ceux qui sont susceptibles de traiter des données à caractère personnel, **qu'ils soient responsables du traitement ou sous-traitants**. Ces derniers sont soumis au règlement, **qu'ils soient établis sur le territoire européen ou pas**.
Le règlement s'applique à ces acteurs à partir du moment où leurs activités de traitement sont liées soit :

- A l'offre de biens ou de services à des personnes concernées au sein de l'Union européenne (Contre rémunération ou gratuitement).
- Au suivi du comportement de ces personnes du moment que le comportement a lieu au sein de l'Union européenne.

Pour les entreprises proposant des services de Cloud computing à des résidents européens par exemple, le règlement s'applique donc pleinement.
La nationalité de la personne concernée n'est pas un critère : Ce sont l'établissement des acteurs impliqués dans le traitement et le territoire dans lequel est fourni le bien ou le service qui comptent.

Sanctions, points forts ou désavantages (concurrentiels)

Parmi les points forts du RGPD, figurent son champ d'application et sa portée extraterritoriale. Il s'applique aux responsables de traitements mais également aux sous-traitants. Les autorités de protection pourront sanctionner directement ces derniers également. **Même si le responsable de traitement ou les sous-traitants sont basés hors de l'Union européenne, le règlement s'applique du moment qu'une personne au sein de l'UE est directement visée par un traitement de données à caractère personnel.**
Parmi les difficultés du RGPD, on note le droit à l'effacement des données plus connu sous l'expression de « droit à l'oubli ». En effet, à la suite de la demande d'une personne - à condition que cette dernière soit légitime - les organisations publiques et privées doivent être en mesure de supprimer définitivement leurs données de leurs systèmes dans un délai de 30 jours. Dans ce cas, les entreprises doivent mener des enquêtes, notamment afin de

vérifier l'existence de délais légaux de conservation des données (Dans le secteur bancaire par exemple qui est soumis à de fortes contraintes, environ 95% des demandes d'effacement sont refusées (24).

Aussi, beaucoup d'entreprises, surtout les TPE et les PME ont du mal à mettre en place une mise en conformité au RGPD. Ceci est dû principalement au manque de ressource, de temps et d'investissement.

Quant aux sanctions et leur application, en fonction de la nature, de la gravité ainsi que de la durée de l'infraction, les autorités de contrôle peuvent prononcer des sanctions administratives comme :

- Un avertissement ou une mise en demeure.
- Une limitation temporaire ou définitive d'un traitement ou la suspension du flux de données.
- La demande de rectification ou la limitation ou l'effacement complet des données.

Ou dans les cas les plus graves, des amendes administratives :

En fonction de l'infraction, jusqu'à 10 à 20 millions d'euros pour une personne,

Ou dans le cas d'une entreprise, jusqu'à 2 à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent**.**

Application du RGPD dans le cas des données mixtes : Lorsqu'un ensemble de données inclut des données non personnelles et personnelles, tel que le dossier fiscal d'une entreprise, mentionnant le nom et le numéro de téléphone du Directeur Général de la société. Dans la plupart des cas, les données sont indissociables et l'application des règlements à chaque type de données (personnelles et non personnelles) devient impossible. Dans ce cas, les règles du RGPD doivent être suivies pour l'ensemble des données.

3. Réglementations EU pour les données mixtes

3.1. La directive européenne Network and Information Security (NIS)

Définition et objectifs du règlement

La directive européenne sur la sécurité des réseaux et des systèmes d'Information (NIS (25) a été adoptée le 7 Juillet 2016. Les États membres avaient jusqu'au 9 Mai 2018 pour la transposer.
Cette directive était le **premier acte législatif adopté au niveau de l'Union européenne dans le domaine de la cybersécurité**. Son objectif était de créer un niveau plus élevé de sécurité des données et des infrastructures au sein de l'Union européenne, particulièrement pour **la protection des infrastructures critiques**.
Le champ d'application de la directive concerne les opérateurs publics et privés. Elle s'adresse aux OSE, ainsi qu'aux FSN. L'objectif principal de la directive est la cyber résilience. En d'autres termes, pour ces opérateurs, elle assure la sécurité des réseaux et des systèmes d'information afin de pouvoir résister (à un certain niveau de confiance donné) à des actions qui peuvent compromettre :

- La disponibilité, l'intégrité ou la confidentialité des données (stockées, transmises ou en cours de traitement).
- Des services dépendants qu'offrent ou rendent accessibles les réseaux ou les systèmes d'information des opérateurs.

L'autorité nationale responsable du contrôle est celle de l'État membre dans lequel l'entité fournit son service. Certains types d'entités (fournisseurs de services DNS, **fournisseurs de services Cloud**…) relèvent de la compétence de l'**État membre dans lequel se trouve leur établissement principal dans l'Union**.

Application du règlement

Les données concernées sont *« les données numériques stockées, traitées, récupérées ou transmises par tout réseau de communication électronique, tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés dont un*

ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques » (26).
Et ceci en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance des réseaux et système d'information des OSE et FSN.
Le règlement doit être respecté par les OSE et les FSN identifiés par les États membres.
La directive liste en amont les secteurs, les sous-secteurs, ainsi que les types d'entités des OSE à définir par chaque État membre.
Les FSN quant à eux sont retenus comme étant des entités fournissant des services normalement contre rémunération, à distance, par voie électronique et suite à la demande d'un utilisateur du service.
Les services Cloud en font partie. Voici les autres types de service à retenir :

- Les services de vente en ligne / de place de marché en ligne
- Les services de moteur de recherche en ligne

Sanctions, points forts ou désavantages (concurrentiels)

Parmi les points forts à retenir du règlement, c'est qu'il permet :

- D'homogénéiser à l'échelle de l'Union européenne **un niveau renforcé de cybersécurité**.
- Garantir la continuité des services essentiels **assurant le fonctionnement de la société et l'économie des pays membres.**
- D'imposer le même niveau de conformité aux **fournisseurs de services étrangers opérant sur le marché européen** comme les GAFAM par exemple.

Suite à l'évaluation de la directive NIS en décembre 2020 (25), voici quelques points d'amélioration relevés et qui ont poussé à la révision de la directive vers une nouvelle version (NIS 2) :

- Le champ d'application devient limité avec l'évolution du secteur numérique et les cyber-menaces.
- La directive manque de clarté quant aux critères et à la liste des OSE.
- Chaque pays membre décide des mesures de sécurité à intégrer dans sa loi transposée de la réglementation. Ainsi, le niveau de maturité risque de varier en fonction des ressources humaines et financières que l'État membre accorde à la réalisation des différentes missions comme la surveillance des OSE. Des différences importantes peuvent apparaître au niveau des obligations d'un pays à l'autre.
- Malgré le caractère dissuasif des sanctions applicables aux violations des obligations prévues par cette directive, certains États membres se sont montrés très réticents à appliquer ces sanctions. Cela pourrait engendrer un écart négatif quant au niveau de cyber-résilience attendu des entités concernées.

Concernant les sanctions, chaque État membre fixe les règles relatives aux sanctions applicables en cas d'infractions aux lois nationales transposées depuis la directive. Ils s'assurent aussi de l'application des mesures mises en place. Selon la directive, *« les sanctions prévues doivent être effectives, proportionnées et dissuasives ».*

NIS 2 (27) **:** Face aux menaces croissantes, liées à la crise COVID-19 et à l'évolution du secteur numérique en général, une nouvelle directive NIS 2 a été approuvée par le COREPER le 22 Juin 2022. Le texte doit encore être voté en session plénière pour être adopté définitivement. Son objectif est d'étendre le champ d'application du NIS et de remplacer cette dernière.

Dans la poursuite du même objectif que la directive NIS, la NIS 2 devrait élargir les secteurs et les sous-secteurs concernés à environ 10 fois plus d'organisations que la première version NIS.

En plus des secteurs listés dans la directive NIS 1, on retrouve l'espace, la recherche et les entreprises de services du numérique ou encore les télécommunications et les administrations publiques que la directive vise particulièrement à intégrer. L'évolution de la directive réside aussi dans la manière de classification des entités, identifiées (Selon un critère de taille au sens de la recommandation 2003/361/CE) comme entités essentielles ou importantes avec des secteurs / sous-secteurs et types d'entités (28). Cette catégorisation se veut plus précise et

classifie les entités selon leur niveau de criticité. Ainsi, les entités identifiées par les États membres seront obligées de suivre les obligations de la directive et surtout d'avertir l'autorité nationale chargée de la gestion des incidents cyber pour tout incident majeur.
A noter que certaines entités font partie d'un registre créé et tenu à jour par l'ENISA comme les fournisseurs de services numériques, de services DNS, de services Cloud ainsi que certains fournisseurs listés en annexe de la directive (28).
Une autre évolution significative concerne les mesures appropriées, à mettre en place pour la gestion des risques en matière de cybersécurité pour ces entités essentielles et importantes. Dans ce cadre et afin de démontrer la conformité aux exigences imposées par la directive, certains États membres peuvent exiger des certifications pour des produits, services ou processus dans le cadre du schéma européen de certification en matière de cybersécurité.

3.2. Data Governance Act / Data Act

Définition et objectifs des règlements Data Governance Act / Data Act

A – Data Governance Act « DGA » (29) ***:*** Le règlement a été adopté en Mai 2022 et il ne sera applicable qu'en Septembre 2023. Son objectif est de favoriser le partage des données personnelles et non personnelles en mettant en place des *structures d'intermédiation*. Trois points sont à retenir pour cet objectif :

- L'accès et la réutilisation de certaines catégories de données particulières détenues par des organismes du secteur public comme les informations commerciales confidentielles ou encore les données personnelles.
- Une certification obligatoire pour les fournisseurs de services d'intermédiation de données.
- Une certification facultative pour les organismes pratiquant *l'altruisme* en matière de données.

B – Data Act (30) ***:*** La proposition législative a été présentée le 23 février 2022 et n'est pas encore votée.
Son objectif est d'encadrer et de faciliter l'usage et la circulation des données, et aussi de renforcer les droits des utilisateurs en termes de droit d'accès aux données générées par des appareils connectés et le droit à la portabilité des données pour la gestion des fournisseurs de services Cloud.
Ainsi, le règlement repose sur cinq axes pour atteindre cet objectif :

- L'accessibilité obligatoire aux données générées par l'utilisation des objets connectés et services connexes. Le but étant de faciliter le partage entre les entreprises et avec[4][5] le consommateur des données.
- L'autorisation de l'utilisation des données captées par les entreprises et par les organismes publics (Le besoin est soumis à justification (31)).
- L'encadrement des contrats entre les fournisseurs de services (Cloud et Edge) et les consommateurs en facilitant les conditions de changement de ces fournisseurs sans frais afin d'encourager la concurrence sur le marché du Cloud.
- L'élaboration de normes d'interopérabilité pour les données.
- La mise en place des garanties contre les accès non autorisés de gouvernements tiers aux données non personnelles contenues dans le Cloud.

Application des règlements

Chaque État membre désigne une ou plusieurs autorités compétentes chargées de l'application et de l'exécution des deux règlements.

Les acteurs concernés pour chaque règlement sont :

A – Data Governance Act :

- Les organismes du secteur public.
- Les fournisseurs de services de partage de données (Services Cloud, Plateforme de partage de contenus, réseaux sociaux…).
- Toute entité qui collecte et traite des données et qui souhaite en faire un usage altruiste.

B – Data Act :
Tous les acteurs privés ou publics du marché de la donnée au sein de l'Union européenne. A savoir :
Les fabricants et les fournisseurs de produits et services connectés recevant, générant ou recueillant des données, les prestataires de ces services, les détenteurs des données, les destinataires des données et les organismes du secteur public.

Sanctions, points forts ou désavantages (concurrentiels)

Les deux règlements prévoient des sanctions, ces dernières seront de la responsabilité des Etats membres. Ils devront déterminer le régime des sanctions applicables aux violations des dispositions de chaque règlement et prendront toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces dernières sont censées être effectives, proportionnées et dissuasives.

Articulation avec le RGPD : Afin d'assurer une bonne articulation autour du RGPD, le DGA et le Data Act nécessitent une gouvernance de la part des autorités de protection des données et une cohérence par rapport aux obligations du RGPD.
En effet, ces deux règlements doivent être appliqués d'une manière intelligente sans porter atteinte à la protection des données personnelles. En cas de conflit avec le DGA par exemple, ce sera le RGPD qui prévaudrait.

4. Cadre européen des certifications et qualifications

4.1. Cybersecurity Act

Définition et objectifs du règlement

Le règlement Cybersecurity Act (32) a été adopté le 12 mars 2019 par le parlement européen et le 7 Juin 2019 par le conseil de l'UE. Applicable depuis le 7 juin 2021, il est obligatoire pour tous les États membres. Ces derniers doivent se mettre en conformité avec les règles impactant leur organisation nationale.

Le premier objectif du règlement est de renforcer la capacité de l'ENISA, en officialisant son mandat permanent. Elle dispose de pouvoirs renforcés afin d'aider les États membres à faire face aux cyber-menaces et constitue le point de référence auprès des institutions de l'UE.

Le deuxième objectif est d'établir un cadre européen de certification de cybersécurité. Via cette certification accordée suite à une évaluation faite par un tiers reconnu, les entreprises ont la possibilité de certifier que leurs produits sont conformes aux normes européennes en matière de cybersécurité.

Application du règlement

Le règlement est applicable directement et ne nécessite pas de transposition en loi locale par les États membres. La mise en place de cette certification est obligatoire pour les États mais reste volontaire pour les entreprises et les organisations, sauf ceux à qui les États membres auraient imposé la certification en appliquant une législation locale.

Trois points sont à retenir pour comprendre l'application de ce règlement : Les modalités d'adoption du schéma de certification, le processus de certification avec ses trois niveaux d'assurance et les acteurs de ce processus.

1 – Les modalités d'adoption d'un schéma de certification sont axées sur cinq étapes :

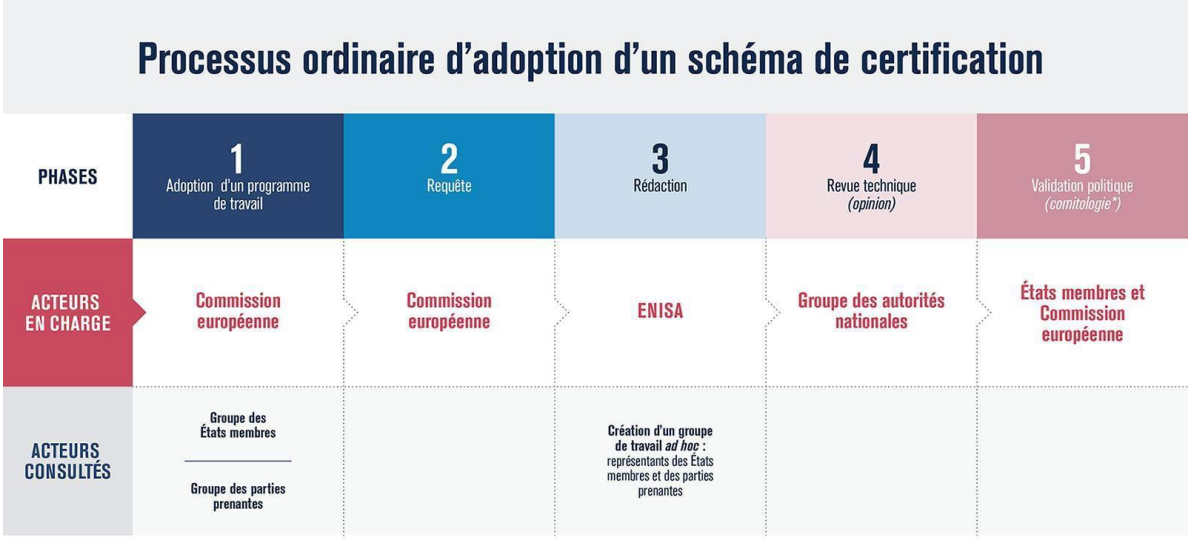


Figure 11 – Le processus pour l'adoption d'un schéma de certification
Source : https://www.ssi.gouv.fr/administration/reglementation/cybersecurity-act/le-cadre-de-certification-europeen/

2 – Trois niveaux d'assurance sont définis. Chaque niveau est caractérisé par son processus de certification, ainsi que sa méthodologie d'évaluation :

Niveau d'assurance	Objectifs de sécurité	Rigueur de l'évaluation
Elémentaire	Les objets grand public (Internet des objets - IOT)	Auto-évaluation des produits par leur développeur
Substantiel	Solutions representant un risque médian. Par exemple les assureurs dans leur couverture du risque des services Cloud	Tests de conformité effectués par un tiers de confiance accrédité (le Conformity Assessment Body – CAB)
Elevé	Solutions representant un risque impliquant des compétenes ou des ressources "significatives" (Véhicules ou dispositifs médicaux connectés)	Des tests de pénétration par un tiers de confiance compétant en plus des test de conformités (réalisé pour le niveau Substantiel) la certification est obligatoirement délivrée par un organisme public, il est le garant des compétences techniques nécessaires pour les tests de pénétration

Figure 12 - Le processus de certification avec ses trois niveaux d'assurance

3 – Plusieurs acteurs sont impliqués dans le processus de certification. Le schéma ci-dessous synthétise leur rôle (détaillés dans le règlement (32)) :

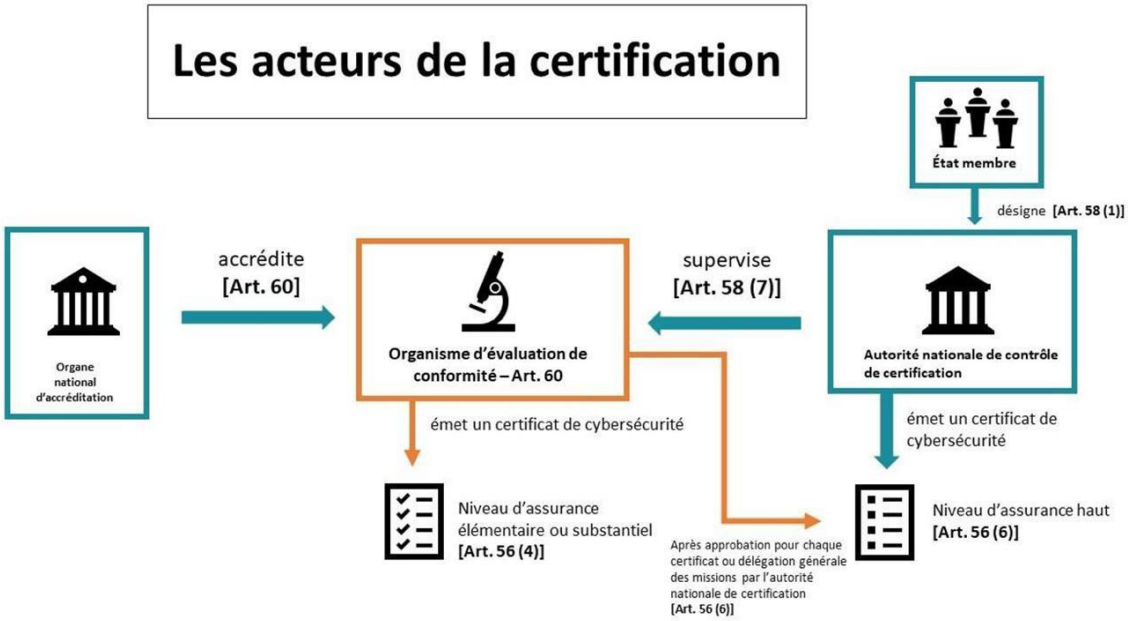


Figure 13 - Les acteurs de la certification
Source : https://www.systancia.com/european-cybersecurity-act/

4.2. Les Schémas européens de certification de cybersécurité pour les services Cloud

Différents schémas de certification cybersécurité existent au sein de l'Union européenne, comme : le C5 (BSI) en Allemagne (33) ; le SecNumCloud (ANSSI) en France (Détaillé en section *4.3 La qualification SecNumCloud*; l'ENS (OC-CCN) (34) en Espagne. Ces schémas ont tous un objectif commun qui est d'assurer un niveau élevé de sécurité des services Cloud. Toutefois, de par leurs exigences et leurs approches distinctes, il en résulte des conditions et des contraintes différentes pour les prestataires de services Cloud qui souhaitent fournir leurs services dans différents États membres de l'UE.
L'objectif du schéma européen de certification de cybersécurité est de supprimer ces différences en uniformisant le marché des services Cloud au sein de l'UE.

Une première version de ce schéma a été établie par l'ENISA le 22 décembre 2020 EUCS (35). Son objectif est de permettre aux prestataires de services Cloud de justifier, selon différents niveaux d'assurance, de la conformité des services fournis par rapport aux exigences mutualisées au sein de l'UE. Et ainsi, de garantir un haut niveau de sécurité pour leurs services.
Le projet est toujours en cours. Suite à la publication de cette première version, de nouvelles demandes ont été soumises à la commission européenne.

En effet, Le Cigref et VOICE ont demandé (via une lettre adressée au commissaire européen Thierry Breton le 23 juin 2022 (36)) à ce que le niveau le plus élevé du schéma intègre l'immunité aux lois étrangères et particulièrement le Cloud Act Américain.

Aussi, une lettre (37) a été adressée à l'ENISA par (OVHcloud et 3DS Outscale, filiale de Dassault Systèmes, paraphée par une trentaine d'entreprises et organisations, dont Oodrive, Clever Cloud ou encore Docaposte, la filiale numérique de La Poste) où ils demandent de ne pas céder sur ce schéma suite aux demandes d'assouplissement des règles de la part des acteurs américains.

De plus, les pays européens ne seraient pas tous d'accord sur certaines exigences (France, Allemagne, Italie et Espagne sont favorables à cette réforme, Pays-Bas, Suède et Irlande sont opposés à cette règle). Le fait de devoir demander des autorisations spécifiques pour l'échange de données entre fournisseurs européens certifiés, et ceux basés en dehors de l'Union européenne, représente une divergence d'avis des États membres.
Selon les pays opposés, ce schéma pourrait présenter une contrainte pour les entités implantées en Europe et ayant des partenaires étrangers (38).

4.3. Cyber resilience Act (CRA)

Définition et objectifs du règlement

Une première version de la législation (39) a été présentée par la commission européenne le 15 septembre 2022. Après examen de ce projet de loi, elle sera adoptée. Cette loi complète le cadre de l'UE en matière de cybersécurité, elle vise à protéger les consommateurs et les entreprises contre les produits contenant des éléments numériques mis sur le marché européen et présentant des défaillances en termes de sécurité. Elle introduit des exigences obligatoires de cybersécurité couvrant à la fois les logiciels et les matériels connectés, tout au long de leur cycle de vie.
Cette loi ne prend pas en compte les produits destinés aux secteurs aéronautique, médical et aux voitures, ces produits étant déjà inclus dans d'autres réglementations. Aussi ne sont pas concernés les services en lignes qui ne sont pas liés à un appareil et les logiciels de services en ligne comme les messageries. Les logiciels fournis dans le cadre d'un service (Ex. Cloud « SaaS ») ne sont pas concernés par cette loi (40).
L'application du règlement et les sanctions sont détaillées en *(Annexe 3).*

5. Stratégie et réglementation du marché numérique EU

5.1. La Stratégie Digital single Market (DSM)

La Stratégie DSM élaborée par la commission européenne (41) a été adoptée le 6 Mai 2015. Elle vise à unir les marchés numériques au sein de l'Europe.
Elle est basée sur 16 initiatives et repose sur les trois piliers suivants :

- Accès : Amélioration de l'accès des citoyens européens aux biens et services numériques.
- Environnement : Création des conditions nécessaires afin que tous les utilisateurs puissent bénéficier d'un accès égal aux services et aux biens disponibles en ligne. Ainsi que des conditions de concurrences équitables, avec un accent sur la protection des données.
- Économie et société : La libre circulation des données numériques afin de maximiser la croissance de l'économie numérique.

Cette stratégie intègre aussi l'initiative européenne sur le Cloud (42), qui se concentrait sur un Cloud scientifique ouvert européen et une infrastructure européenne de données pour traiter en toute sécurité les données en Europe. L'initiative mettait aussi l'accent sur la certification et la possibilité de pouvoir changer de fournisseurs de services Cloud.

5.2. Digital Service Act "DSA" & Digital Market Act "DMA"

Définition et objectifs des règlements

DSA (43) ***:*** Le règlement a été voté par le Parlement européen le 5 juillet 2022 et a été approuvé par le Conseil de l'UE le 18 Juillet 2022. Il devrait entrer en application en 2023.

Son objectif principal est de responsabiliser les plateformes numériques et de lutter contre la diffusion de contenus illicites ou de produits illégaux. Le règlement devrait mieux protéger les droits fondamentaux des utilisateurs européens de ces services, renforcer la surveillance des très grandes plateformes et aider les petites entreprises européennes à se développer.

DMA (44) ***:*** Le règlement a été voté par le Parlement européen le 5 juillet 2022, il devrait être adopté par le Conseil de l'UE le 4 Octobre 2022 et devrait entrer en application en 2024.
Son objectif principal est de limiter (et de corriger) la domination des géants d'internet, particulièrement les (GAFAM), sur le marché numérique européen et de lutter contre leurs pratiques anticoncurrentielles (Combinaison de masse des données des utilisateurs et recours aux algorithmes puissants et inaccessibles). Ainsi, ce règlement devrait créer une concurrence loyale entre les acteurs du numérique en Europe au profit des petites, moyennes et des start-ups européennes qui opèrent sur le marché européen mais qui peinent à capter de la valeur sur ce dernier.

L'application des règlements et les sanctions prévues sont détaillées en *(Annexe 4)*.

Chapitre 2 - Réglementation française

1. Réglementations françaises pour les données non personnelles

1.1. Le secret des affaires (SDA)

Définition et objectifs

« Dans un monde qui survalorise, parfois dangereusement, la transparence, il importe de préserver le secret des affaires. Il s'agit de protéger la vie privée de l'entreprise, ses savoirs et savoir-faire, ses produits et ses services. Certes, la confidentialité doit avoir des limites et ne jamais masquer de l'illégalité, mais elle a des fondements absolument essentiels. » (45)***.***

Le secret des affaires (SDA) est une loi française relative à la protection des affaires qui a été adoptée le 30 juillet 2018. Cette loi, transposée de la directive européenne du 8 juin 2016 par le Parlement français, avait ravivé les inquiétudes des défenseurs de la liberté d'information tels que les lanceurs d'alerte et les journalistes entre autres.

Pour illustrer cette controverse, en voici 2 exemples :

- En 2018, la journaliste et rédactrice en chef et présentatrice de télévision, Elise Lucet, a demandé aux citoyens de se mobiliser afin que cette loi soit amendée. Selon elle, *« Nous pourrions avoir des procédures judiciaires avant même que ces émissions arrivent à l'antenne, vous pourriez donc en être tout simplement privés. »*
- La même année, Dr. Jean-Marc Bonmatin, chercheur au CNRS en chimie et toxicologie, spécialiste de l'interaction entre pesticides et biodiversité, disait ceci : *« Les recherches que j'ai menées notamment sur l'impact des pesticides sur la biodiversité et maintenant sur la santé humaine n'auraient pas été possibles avec une telle loi, encore moins la publication des résultats. »*

Le SDA protège toute information correspondant aux éléments cumulatifs autour des savoir-faire et informations commerciales de valeur :

- *« Non connus du grand public et/ou du secteur professionnel concerné ».*
- *« Ayant une valeur commerciale, réelle ou potentielle, parce que secrets ».*
- *« Et faisant l'objet de mesures spécifiques destinées à les garder confidentiels ».*

En d'autres termes, un SDA peut être un organigramme, de la R&D, des projets d'acquisition d'entreprise, …

Le SDA n'est pas protégé lorsque :

- *« Le droit en impose la communication, notamment en cas de contrôle ou d'enquête des autorités judiciaires ou administratives ».*
- *« Le secret est divulgué par des journalistes dans le cadre de la liberté d'expression et du droit d'informer ».*
- *« Un lanceur d'alerte révèle de bonne foi, de manière désintéressée et dans le but de protéger l'intérêt général, une activité illégale, une fraude ou un comportement répréhensible »*
- *« Il s'agit d'empêcher ou de faire cesser toute atteinte à l'ordre public, à la sécurité, à la santé publique et à l'environnement ».*
- *« Il a été obtenu dans le cadre de l'exercice du droit à l'information des salariés ou de leurs représentants ».*

Application

Selon l'article L. 152-1 du Code de commerce, ***« toute atteinte illicite au secret des affaires engage la responsabilité civile de son auteur »*** et toute mesure proportionnée de nature à empêcher ou à faire cesser une telle atteinte peut être prescrite par une juridiction. A partir du moment où le détenteur légitime de l'information n'a pas donné son consentement, une atteinte illicite est constituée.
Et à charge aux entreprises de définir les informations qu'elles estiment relevant du SDA.
Dans l'entreprise, un référent doit être nommé pour une prise en charge de tous les sujets afférents au SDA.

Le ***« PETIT GUIDE JURIDIQUE DE PROTECTION DU SECRET DES AFFAIRES*** », ici en *(Annexe 5),* publié par Olivier de Maison Rouge (Avocat - Docteur en droit), explique de manière très didactique ce sujet. On y trouve notamment la démarche permettant de protéger le SDA.
Il souligne dans de ce guide que *« Le secret des affaires ne doit pas être fantasmé, ce d'autant qu'il ne doit pas servir à dissimuler des pratiques condamnables ou répréhensibles, tels que des délits financiers, des schémas d'évasion fiscale, des comptes bancaires dissimulés, des opérations frauduleuses et, plus généralement, des agissements illicites. »*

Sanctions / Points forts ou désavantages (concurrentiels)

Selon une étude de l'OMPI Magazine en 2019, une année auparavant, ***« 20% des entreprises interrogées avaient été victimes d'au moins une tentative de vol d'informations confidentielles, et près de 40% d'entre elles avaient le sentiment que ce type de menace était en hausse. »*** (46)
Cette loi, qui stimule la compétitivité et l'innovation, assure une protection raisonnable aux entreprises en matière de savoir-faire, création de valeur commerciale, … surtout pour les PME. De plus, les procédures lancées dans ce cadre ne sont ni coûteuses, ni longues.
Cependant, il est difficile pour les entreprises d'identifier les informations qu'elles veulent valoriser au sein de leur patrimoine informationnel.
Pour pallier ces lacunes, le mieux à faire serait d'adapter les contrats, d'assurer la formation des collaborateurs et surtout d'assurer la cybersécurité.
Et pour finir, en l'absence de texte précis en matière de sanction pénale, il est plutôt difficile de cerner les contours de ces nouvelles dispositions, même si le détenteur d'un secret d'affaires est en droit de demander des dommages-intérêts en réparation du préjudice subi. Cette évaluation tient compte notamment du manque à gagner et des bénéfices injustement réalisés. En droit français, il est à noter que le gain manqué et la perte subie sont pris en compte.

2. Réglementations françaises pour les données personnelles

2.1 La loi informatique et liberté (loi I&L), le règlement général de protection des données (RGPD)

Définition et objectifs

La loi n°78-17 relative à l'informatique, aux fichiers et aux libertés, appelée **« loi Informatique et Libertés »** (loi I&L) fût adoptée le 6 janvier 1978. Cette loi initialement prévue pour protéger les libertés individuelles des citoyens français contre l'État (Projet SAFARI, programme public de croisement des données des citoyens) sert aujourd'hui à lutter contre toute utilisation des données à caractère personnel.
Afin de protéger les particuliers d'abus éventuels de l'Etat et des entreprises dans la collecte et le traitement des données personnelles, **la Commission Nationale de l'Informatique et des Libertés** (CNIL) a été créée. Cette autorité administrative française est indépendante. Elle remplit 4 missions :

- Informer, protéger les droits des Français en répondant aux demandes des particuliers et des professionnels qui lui adressent une plainte.
- Accompagner la conformité des professionnels et conseiller les particuliers.
- Anticiper et innover dans le cadre de son activité d'innovation et de prospective via respectivement Le Comité de la prospective et le Laboratoire d'innovation numérique de la CNIL (LINC).
- Contrôler et sanctionner les organismes.

Le 6 août 2004, la loi n° 2004-801 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel transcrit en droit français la directive européenne 95/46 de 1995 et vient modifier la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi introduit le **Correspondant Informatique et Libertés (CIL)** qui est chargé d'assurer le respect des obligations de cette loi en toute indépendance. La nomination d'un CIL reste optionnelle pour les entreprises.

Dix années plus tard, le **Règlement Général de Protection des Données (RGPD),** fruit de plus de quatre ans de négociations et adopté en 2016, ré-établit les grands principes de la protection des données personnelles en harmonisant les textes nationaux. Ce règlement laisse une marge de manœuvre aux États membres sur une cinquantaine de points et rend caduque une grande majorité de la loi I&L.

➔ Le RGPD au niveau européen est détaillé dans cette *partie (2.1 Le Règlement général sur la protection des données personnelles (RGPD)).*

Application

Dans le cadre de **la mise en place du RGPD**, la CNIL accompagne les organismes en les aidant à se mettre en conformité en 6 étapes (47) :

- Désigner un pilote qui sera le **Délégué à la Protection des Données (DPO),**
- Cartographier les traitements de données personnelles en élaborant un registre des traitements,
- Prioriser les actions à mener en fonction des impacts des traitements sur les données personnelles,
- Gérer les risques en réalisant une **Analyse d'Impact sur la Protection des Données (AIPD),**
- Organiser les processus internes en fonction du cycle de vie des événements,
- Documenter la conformité en continu, ce qui permet de prouver la conformité au règlement.

De manière générale, avant de recourir à un service Cloud notamment public, **la CNIL recommande aux entreprises, plus précisément aux PME :**

- D'être rigoureux dans le choix de leur prestataire de Cloud « quant aux conditions de réalisation des prestations, notamment sur la sécurité et sur la question de savoir si leurs données sont transférées à l'étranger, et plus précisément à destination de quels pays ».
- De réaliser une analyse de risques en s'assurant *« que ce dernier [leur] fournira toutes les garanties nécessaires au respect de [leurs] obligations au regard de la loi Informatique et Libertés, notamment en termes d'information des personnes concernées, d'encadrement des transferts et de sécurité des données », via une checklist* (48). Le choix du prestataire doit se faire en fonction des considérations tant économiques que juridiques et techniques.

Et pour s'assurer du respect des réglementations et des lois lors de la signature du contrat, **7 recommandations ainsi que des modèles de clauses de contractualisation** sont proposés par la CNIL (49):

1. Identifier clairement les données et les traitements qui passeront dans le Cloud. Ce document datant de 2012, ce point est à mettre à jour suite à l'arrêt de la Cour de Justice de l'Union Européenne (CJUE) dit arrêt Schrems II de juillet 2020. Désormais, pour qu'une TPE/PME soit conforme sur un choix cloud, elle a 2 possibilités :
   - Prendre une solution dont le siège social de l'entreprise est en UE ainsi que ses datacenters
   - Prendre une autre solution et alors signer des clauses contractuelles qui assurent que les mesures de sécurité additionnelles prises assurent que les données personnelles ne peuvent être décrypter dans le cadre de lois extraterritoriales. Ceci dit, aucun Cloudeur étranger n'accepte cela. Et pour être conforme, il faut que les clés de sécurité soient détenues par la société, que les données soient chiffrées au repos et protégées contre le service (en lecture en mémoire vive chez le Cloudeur). Ce dernier point est possible pour les documents avec certaines solutions logicielles et impossible pour les solutions avec des bases de données. **En clair, aucune TPE/PME n'a les moyens de faire cela car c'est trop coûteux et trop complexe.**

2. Définir ses propres exigences de sécurité technique et juridique.
3. Conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise.
4. Identifier le type de Cloud pertinent pour le traitement envisagé.
5. Choisir un prestataire présentant des garanties suffisantes.
6. Revoir la politique de sécurité interne.
7. Surveiller les évolutions dans le temps.

A ces 7 recommandations peuvent être ajoutées les 2 suivantes :

- Assurer la sécurité des développements (sécurité by design) et en production
- Reporter en moins de 72h une faille de données personnelles (ce qui veut dire concrètement mettre en place ou sous-traiter un SOC)

Parmi les modèles de **clauses contractuelles** se trouvent principalement : **le respect des principes de protection, les durées de conservation, le lieu d'hébergement, les obligations de sécurité et de confidentialité, la réversibilité, la traçabilité, la continuité et intégrité, le niveau de service, …**

Sanctions / Points forts ou désavantages (concurrentiels)

En cas de manquement au RGPD, une entreprise peut être mise en demeure ou sanctionnée sous différentes formes :

- Publique, qui se traduit par une publication d'un communiqué sur les sites cnil.fr et legifrance.fr
- Non-publique.
- Pécuniaire, qui peut représenter au maximum 4% du chiffre d'affaires de l'entreprise ou 20 millions d'euros.
- Non-pécuniaire, c'est-à-dire un rappel à l'ordre, une injonction sous astreinte, …

La CNIL a prononcé en ce début d'année des sanctions répressives et dissuasives sous forme d'amende à l'encontre, par exemple, de :

- **TotalEnergies** pour un montant de **1 million d'euros** pour non-respect de ses obligations en matière de prospection commerciale et de droits des personnes *(Annexe 6).*

Le 11 mai 2022, la CNIL a publié **son rapport d'activité sur 2021** (50) dont en voici quelques chiffres :

- 14 143 plaintes **reçues soit une progression de 4% par rapport à 2020**. Les plaintes concernaient les droits d'accès, la prospection commerciale, associative et même politique, …
- Sur 22 organismes contrôlés dans le domaine de la **cybersécurité, 15 ont été mis en demeure pour site web non sécurisé** (5037 notifications reçues concernent les **violations de données personnelles, soit une évolution de 79 % par rapport à 2020**
- …

La CNIL émet sur son site de bonnes idées au travers de recommandations sous forme de points de vigilance à l'égard du Cloud. 3 derniers bels exemples en date en matière de Cybersécurité :

- « Le RGDP : la meilleure prévention contre les risques cyber » (51).
- Le « Baromètre data breach » (52) sur une analyse des tendances 2021.
- Le 7 février 2022, a été mise en ligne une publication nommée *« Violation du trimestre : les défauts de configuration des espaces de stockage dans le Cloud public »* (53). La CNIL s'est inspirée d'incidents réels pour promulguer des recommandations qui permettent de *« comprendre, prévenir et se protéger face à des attaques sur des infrastructures Cloud »*.

Cette année, elle va consacrer 1/3 de ses contrôles sur 3 thématiques : la prospection commerciale, **le Cloud** et la surveillance du télétravail.
Pour 2022-2024, elle a publié son « Plan stratégique » (54) axé sur 3 thématiques :

- Le respect du droit des personnes avec un accent sur une politique répressive dissuasive.
- La promotion du RGPD.
- Ses priorités face à l'usage des données personnelles notamment pour :
  - ✓ Les caméras augmentées.
  - ✓ Le déploiement dans le Cloud.
  - ✓ Les applications des smartphones.

3. Réglementations françaises pour les données mixtes

3.1 La directive Network and Information Security (NIS)

Définition et objectifs

En Europe, la directive Network and Information Security (NIS), expliquée dans cette partie *(3.1 La directive européenne Network and Information Security (NIS)) s'applique* aux opérateurs de services essentiels (OSE) et fournisseurs de services numériques (FSN).
Depuis son entrée en vigueur en août 2016, chaque pays européen doit se mettre en conformité avec cette directive en la transposant dans son droit national avec une date butoir fixée au 09 mai 2018.

Dans le cadre de cette transposition, **l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)**, qui a été Chef de file en France pendant les négociations portant sur cette Directive, a élaboré un référentiel strict de sécurité numérique visant les OSE et les FSN.

Application

Depuis sa mise en application, ***« les opérateurs de services essentiels (OSE)***, *définis comme des opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité*

pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services », sont désignés par l'ANSSI.
Ci-dessous, **la liste des secteurs d'activités pour les opérateurs considérés comme des OSE**, avec en exergue ceux ajoutés par la législation française.

Figure 14 - Opérateurs de Services Essentiels en France[IL6]
Source : https://www.riskinsight-wavestone.com/2018/09/bilan-directive-nis/

Contrairement aux FSN qui prennent des mesures techniques et organisationnelles basées sur une approche par les risques, l'État impose aux OSE des règles de sécurité basées sur la liste précise de mesures ci-dessous (55) :

- **La gouvernance de la sécurité des réseaux et systèmes d'information** *« via l'élaboration de politique de sécurité et d'homologation du SIE [Système d'Information Essentiel] ».*
- **La protection des réseaux et systèmes d'information** *« avec la sécurité de l'architecture, de l'administration et des accès au SI ».*
- **La défense des réseaux et systèmes d'information** *« avec la détection et le traitement des incidents de sécurité ».*
- **La résilience des activités** *« notamment au travers de la gestion de crise ».*

Selon Chakib Kissane, Contributeur d'articles, ***« Dans un monde où l'insécurité cyber grandit, les OSE pourraient ainsi devenir des oasis de confiance où les clients s'arrêteraient pour se désaltérer ».*** (56)

En complément de la Directive européenne sur les FSN décrite dans cette partie *(3.1 La directive européenne Network and Information Security (NIS)),* en France, **les entreprises de moins de 50 salariés avec un chiffre d'affaires de moins de 10 millions € ne sont pas concernées.**
De plus, les FSN implantés hors de l'Union Européenne sont contraints à désigner un représentant en France auprès de l'ANSSI.

Afin de garantir le niveau de sécurité attendu, les FSN ont l'obligation *« d'identifier et d'actualiser lesdits risques existants et/ou d'affecter leurs réseaux et systèmes et d'adopter des contre-mesures dans les domaines prévus par la loi (article 12) » :*

- « La sécurité des systèmes et des installations ».

- « La gestion des incidents ».
- « La gestion de la continuité des activités ».
- « Le suivi, l'audit et le contrôle ».
- « Le respect des normes internationales ».

Selon Olivier de Maison Rouge, Avocat - Docteur en droit, *« ces critères techniques n'englobent pas précisément les aspects de réglementation, notamment* ***les ingérences sous forme d'extraterritorialité des lois étrangères dans le cyberespace européen****. »*

Concernant leur mise œuvre, **les OSE et FSN** doivent respecter certaines **obligations** :
Les OSE doivent :

- Désigner une personne en charge des échanges avec l'ANSSI dans les deux mois.
- Déclarer leurs SIE dans les trois mois.
- Déclarer auprès de l'ANSSI tout incident de sécurité affectant leurs infrastructures et cela sans délai.
- Coopérer pleinement lors des contrôles de conformité réalisés par l'Agence ou par l'un de ses prestataires qualifiés.
- Dès qu'ils sont désignés OSE, ils doivent :
  - ✓ S'homologuer en termes de sécurité dans les trois ans.
  - ✓ Établir leur politique de sécurité dans l'année, tout comme la cartographie et la conformité avec les règles relatives à l'identification, à l'authentification et aux droits d'accès (ce qui suppose la mise en place des procédures rigoureuses de contrôle des accès, notamment via l'authentification forte).
  - ✓ Répondre aux volets liés à l'architecture ou à l'administration jusqu'à deux ans ou au-delà.
  - ✓ Et pour extrapoler, veiller à ce que les règles de sécurité qui leur sont imposées soient étendues à leurs sous-traitants.

En ce qui concerne **les FSN**, ils doivent *« intégrer une politique pertinente de sécurité des réseaux et systèmes d'information (PSSI) et définir des plans de continuité d'activité (PCA) et de reprise d'activité (PRA). Par voie de conséquence, cette cyber-résilience ainsi instituée doit être guidée par des impératifs techniques, mais encore par des considérations relevant de la gestion de crise, d'origine humaine, logique, … »*

Que ce soient les OSE ou les FSN, ils sont tous les deux soumis à des contrôles de l'ANSSI ou des Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI) qualifiés et ont l'obligation de signaler tout incident. Dès que l'agence est informée, elle peut à son tour aviser le public *(Annexe 7).*

Pour répondre aux obligations mises à leur charge, les OSE et FSN doivent engager les moyens nécessaires aux différentes actions de mise en conformité, y compris les contrôles demandés par l'ANSSI.
En cas de manquement, les dirigeants peuvent être sujets à des amendes :

Tout le dispositif de cybersécurité des OSE et des FSN est décrit sur le site de l'ANSSI sous les liens suivants : OSE (57) et FSN (58).

Le cas des **Opérateurs d'Importance Vitale (OIV) qui sont les entreprises** « gérant ou utilisant un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement, d'obérer gravement **le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population** » est à exclure. En effet, ils sont déjà très responsabilisés et aidés par rapport à leurs **systèmes d'information d'importance vitale (SIIV)**. La liste exacte est de ces opérateurs est Confidentiel Défense.

	Montants des amendes	
	OSE	FSN
Non conformité aux règles de sécurité	100 k€	75 k€
Non déclaration des incidents de sécurité	75 k€	50 k€
Obstacle aux opérations de contrôle	125 k€	100 k€

Figure 15 - Sanctions pour les OSE / FSN
Source : https://www.riskinsight-wavestone.com/2018/09/bilan-directive-nis/

Au niveau pénal, les sanctions applicables aux OIV s'élèvent à **150 000 € pour le dirigeant et à 750 000 € pour la personne morale.**
Il est à noter que la loi européenne ne prévoit aucune sanction, contrairement à la France, lorsque le manquement n'est pas intentionnel. La simple négligence est donc condamnable.

4. Certifications, Qualification et Normes françaises

4.1 La certification (ou règlementation) Hébergeur de Données de Santé

Définition et objectifs

Chiffres clés (59) :

- Valeur d'un dossier médical sur le Darkweb : 15€ (qui équivaut à 30 000 comptes d'adresses e-mail).
- Données d'une carte bancaire VISA : 50€
- 2017 : 2,6 milliards de dossiers de données numériques ont été exposés à des fuites, volés ou corrompus. 27% d'entre eux étaient des données de santé comparativement aux données de services financiers de 12%, d'éducation de 11% ou de gouvernements de 11%.

En France, nous avons 3036 établissements de santé et ils sont loin de présenter le même niveau de sécurité.
Depuis la pandémie de la Covid-19, les établissements de santé (centre hospitalier, EHPAD, laboratoires, ...) subissent de plus en plus d'attaques par rançongiciel. Ces attaques ciblent directement les données de santé des patients et peuvent entraîner de lourdes conséquences telles que la paralysie des systèmes biomédicaux, le report des interventions médicales, l'usurpation des données de santé, …
Dans le secteur de la santé, on parle plus précisément de **Données de Santé à Caractère Personnel (DSCP)**. Il s'agit des données relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne (60).
Avoir accès à ces données permet d'analyser voire de détruire l'état de santé d'une personne.

Une des questions qui se posait déjà depuis plus de 10 ans tourne autour de la fiabilité des plateformes destinées à traiter les données de santé des Français en matière de confidentialité, sécurité, intégrité et stockage. **La loi du 4 mars 2002 et le décret du 4 janvier 2006 encadrent l'hébergement des données de santé.**
C'est dans ce contexte que **la réglementation HDS (Hébergeur de Données de Santé)** a été émise par l'ASIP SANTÉ fondée en avril 2015 (61) et qui est responsable de la promotion des solutions de santé électroniques en France et qui dépend du ministère français de la Santé. L'ASIP Santé est devenue depuis le 20 décembre 2019 l'agence du numérique en santé.

Application

Cette réglementation précise et renforce les mesures de sécurité à mettre en œuvre, et surtout, impose leur contrôle via un audit documentaire et sur site par un organisme tiers accrédité avant toute opération d'hébergement.
Depuis avril 2018, elle oblige, *« toute personne hébergeant des données de santé à caractère personnel recueillies dans le cadre d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil des données, ou pour le patient »*, à être certifiée HDS.
Selon le Ministère de Solidarité et de la Santé, l'HDS concerne les patients qui confient l'hébergement de leurs données de santé à un tiers, et d'autre part les responsables de traitements de données de santé à caractère personnel ayant pour finalité la prévention, la prise en charge sanitaire (soins et diagnostic) ou la prise en charge sociale et médico-sociale de personnes (62).

Les hébergeurs d'infrastructure physique et les hébergeurs « infogéreurs » sont soumis à la certification HDS sur le périmètre des activités qu'ils proposent (62). La liste des hébergeurs certifiés est consultable via ce site (63).

La procédure de certification est confiée à des organismes certificateurs accrédités (64) qui accompagnent dans la mise en œuvre des référentiels HDS (65).

Le 18 février 2021, le Président de la République a annoncé l'accélération de la stratégie nationale (66) portée sur la cybersécurité et cela en visioconférence avec les centres hospitaliers de Dax et de Villefranche-sur-Saône, dont l'activité a été fortement impactée par des cyberattaques.
Cette stratégie invite les établissements de santé à consacrer systématiquement 5 à 10 % de leur budget à la cybersécurité.
Afin de pousser les acteurs du secteur à entrer en conformité avec la réglementation française et européenne en vigueur (RGPD et HDS) et à élever le niveau de sécurité des données de santé des personnes, **la CNIL a décidé de conserver les données de santé dans sa liste des thématiques de contrôle jugées prioritaires pour l'année 2021** (67)**.** Cela avait déjà été le cas en 2020.

Sanctions / Points forts ou désavantages (concurrentiels)

Grâce à la certification, **l'hébergeur de données joue la transparence au même titre que l'entreprise cliente.** De plus, l'établissement de santé de même que son sous-traitant, ici l'hébergeur, sont soumis au RDPD. Cela apporte une garantie supplémentaire aux personnes.
Et pour finir, la certification étant confiée à un tiers externe permet de respecter une impartialité/neutralité non négligeable en faisant des contrôles, périodiquement, pour s'assurer que le référentiel de certification est bien respecté.
Cependant, si le sous-traitant est une grosse structure, son audition peut s'avérer fastidieuse.
Pour être certifié, l'hébergeur doit rémunérer l'organisme de certification. **Un petit établissement pourrait manquer de moyens financiers et humains pour auditer ce type de structure.**

4 affaires ont pu illustrer l'application de la réglementation HDS : **Doctolib** et la Plateforme des données de santé (PDS) également appelée **Health Data Hub**.

- Pendant la pandémie du Covid-19, Doctolib a été choisi par l'Etat pour gérer les prises de RDV dans le cadre de la vaccination. Les données sauvegardées sont stockées sur un **serveur AWS hébergé aux Etats-Unis.** Plusieurs associations et syndicats de médecins ont jugé insuffisante la protection des données de santé des Français en déposant un référé devant le juge pour annuler le contrat liant Doctolib à l'Etat. Ces associations se sont basées sur l'invalidation du **« *Privacy shield* »** par l'arrêt Schrems II de la CJUE de juillet 2020 (68) (69).
- En 2019 a été créée la Plateforme des données de santé (PDS), prévue pour faciliter le partage des données de santé issues de sources très variées afin de favoriser la recherche. Ces données étant hébergées chez

Microsoft, la **CNIL** a fait part de son souhait que son hébergement et les services liés à sa gestion doivent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne. Le gouvernement a fini par annoncer la fin de cet hébergement chez Microsoft d'ici 2 ans (70).

- En 2020, la CNIL a sanctionné 2 médecins à hauteur de 3000 et 6000€ d'amendes pour avoir insuffisamment protégé les données de santé de leurs patients (défaut de chiffrement) et ne pas avoir notifié une violation de données à la CNIL (71).
- Le 15 avril 2022, la formation restreinte de la CNIL a sanctionné la société DEDALUS BIOLOGIE d'une amende de 1,5 million d'euros, notamment pour des défauts de sécurité ayant conduit à la fuite de données médicales de près de 500 000 personnes (72).

4.2 Les normes ISO/IEC 27017 : 2015 et ISO/IEC 27018 : 2019

Les normes ISO fournissent « des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information ». Il s'agit d'un référentiel qui permet la reconnaissance de l'atteinte d'un certain niveau de qualité, de performance, de sécurité, … tout en facilitant la comparaison et/ou l'interopérabilité entre des produits, des services, des systèmes ou des organisations.

Les normes 27017 et 27018 sont les principales normes spécifiques au Cloud et se nomment respectivement :

- ISO 27017:2015 Technologies de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO 27002 pour les services du nuage
- ISO 27018:2014 Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

L'ISO 27017 présente les lignes directrices relatives aux mesures de sécurité de l'information applicable au Cloud. **Elle apporte des compléments spécifiques sur le partage des responsabilités entre le prestataire et le client.** Un des compléments concernent, par exemple, les relations avec les autorités en précisant la localisation géographique des données afin de permettre de déterminer les autorités et juridictions compétentes.

Quant à l'ISO 27018, elle définit un code des bonnes pratiques pour la protection des PII dans le Cloud public. **Elle sert de guide pour les prestataires de Cloud agissant en tant que sous-traitant à l'égard des données personnelles.** Les objectifs sont : aider le prestataire à se conformer aux exigences réglementaires, lui permettre d'afficher de la confiance, l'assister dans sa contractualisation avec son client et pour finir, fournir au client une grille d'audit et d'analyse.

Il est intéressant de rappeler ici que la conformité n'est pas synonyme de sécurité. Les certifications ont pour objectif principal de rassurer en démontrant que la mise en œuvre et le paramétrage sont conformes à la norme/qualification.

4.3 La qualification SecNumCloud

Définition et objectifs

Le 17 mai 2021, le gouvernement a dévoilé **sa stratégie nationale pour le Cloud** (73). Celle-ci s'articule autour de 3 piliers :

1. La définition et la caractérisation du **« Cloud de confiance »** qui est une doctrine Cloud Centric garantissant un niveau de protection juridique et cyber pour les données sensibles.

2. La doctrine **« Cloud au Centre »**, initiée par la circulaire du Premier Ministre du 5 juillet 2021, qui fait du cloud un levier prioritaire de la transformation numérique des administrations et participe d'une politique de la demande (74).
3. Une politique industrielle dont il est question ici et qui a pour objectif de bâtir les fondations d'une économie de la donnée européenne de confiance, à travers le soutien à **l'offre et à l'innovation**.

Ce référentiel est destiné aux entreprises privées, mais surtout aux OSE et OIV dont les services accompagnent les entités sensibles à la sécurité. Ils peuvent ainsi démontrer d'un haut niveau de sécurité de leur cloud.

Pour protéger nos données de l'accès non maîtrisé par des tiers extérieurs, le Gouvernement a élaboré une stratégie reposant sur la qualification des offres dites de confiance afin d'encourager les entreprises et administrations françaises à protéger leurs données sensibles par l'utilisation de services Cloud performants (suites bureautiques collaboratives, outils de visioconférence, etc.) tout en assurant la meilleure protection pour leurs données.
La labellisation d'une offre « Cloud de confiance » repose sur le respect de bonnes pratiques de sécurité informatique mais aussi sur l'application exclusive du droit européen aux données hébergées et traitées lors de son utilisation. Ces critères sont repris par **SecNumCloud** (75) dont le référentiel répond aux exigences techniques et juridiques d'immunité aux réglementations non-européennes à portée extraterritoriale.

La première version de SecNumCloud a été présentée en 2016, et a connu une révision en 2018. Depuis mars 2022, nous en sommes à la 3ème version qui est celle utilisée actuellement sous le nom de « SecNumCloud 3.2 » et qui a été renforcée à bien des égards : *« la réglementation avec l'application exclusive du droit européen aux données hébergées et traitées dans le Cloud », « pour un éditeur, de ne certifier que son logiciel dans la mesure où il repose sur une infrastructure déjà qualifiée »,* …**ainsi que la mise en place d'un dispositif d'accompagnement des PME et start-up pour l'obtention du label "SecNumCloud"** pour les services en PaaS/SaaS avec un budget alloué de 2,5 millions d'euros.

Il s'agit d'un visa de sécurité délivré par **l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** pour les opérateurs Cloud qui proposent des services SaaS, PaaS, IaaS et depuis 2022, CaaS (Containers as a Service).

Application

Ce référentiel concerne les données sensibles des acteurs de l'Etat (donc ministères et agences publics qui dépendent de la DINUM, la Direction Interministérielle du Numérique). La définition des données sensibles fournie par l'ANSSI est relative aux données des agents de l'Etat, des données économiques utilisables pour de l'intelligence économique et les données personnelles des citoyens.

Aujourd'hui, 5 fournisseurs ont développé 7 offres avec le label SecNumCloud : Cloud Temple, OVHCloud, Oodrive, Outscale, Worldline.
Oodrive a mis en ligne une infographie à jour qui explique cette labellisation (76).
On y apprend notamment que le prestataire doit répondre à environ 400 points d'exigences concernant :

- La sécurité de l'information et la gestion du risque.
- La cryptologie.
- La continuité d'activité.
- La gestion des actifs et des identités physiques et numériques.
- La relation avec les tiers et leur conformité.
- La sécurité du SI.

Avantages : Les 5 fournisseurs qualifiés SecNumCloud ont permis aux administrations de doubler leur volume de marchés passés.
« De plus, dans le cadre de la stratégie d'accélération Cloud prévue dans France relance 2030, **une vingtaine de projets innovants et à forte valeur ajoutée sont déjà financés pour 380 millions d'euros. »**
De plus, grâce à une collaboration entre l'ANSSI et la CNIL, SecNumCloud répond aux exigences relatives à la protection des données via le RGPD.

En revanche, la mise en place de ce référentiel constitue un processus « long, complexe et coûteux » à travers un travail titanesque de documentation de process et de segmentation du réseau. Avant d'envisager une qualification SecNumCloud, une certification de conformité 27001 pourrait être la première étape.
Chose importante, le référentiel SecNumCloud 3.2 précise que pour être éligibles, les sociétés ne peuvent être à plus de 39% par une entité autre qu'une française… Implicitement, les américains en sont exclus.

Chapitre 3 - Quelques lois étrangères (russes, chinoises et américaines) encadrant la donnée

La Russie

Dès 2015, la Russie a durci sa réglementation concernant les données personnelles avec la loi « Russian Data Localization Law » 242-FZ (77). Cette réglementation impose pour toute entreprise traitant des données personnelles des citoyens russes, opérant ou non dans le pays, le stockage de ces informations sur des serveurs localisés physiquement sur le territoire russe. Les entreprises non conformes à ce règlement doivent s'acquitter de pénalités financières ou se voir couper l'accès à leur site depuis la Russie.

Depuis l'entrée en vigueur de cette loi, certaines grandes entreprises (américaines) ont été sanctionnées :

- Google qui a écopé d'une amende pour défaut de stockage des données personnelles en Russie en Juillet 2021 (78).
- Blocage du réseau social LinkedIn en Russie – Novembre 2016 pour conservation des données personnelles russes en dehors du pays (79).

La Chine

En Chine, deux principales lois (DSL et PIPL) forment le système législatif en termes de protection et de traitement des données, ainsi que de la cybersécurité :

- **DSL** (80) : Cette loi se concentre sur la gouvernance de la sécurité des données et s'applique à toute activité de traitement de la donnée (en ligne ou hors ligne).
- **PIPL** (81) (82) : Dédiée à la protection des données personnelles, cette loi est entrée en vigueur en Novembre 2021. Son objectif est de protéger les informations personnelles des citoyens chinois et de leur droit dans ce cadre. Elle s'applique à tout traitement de données personnelles (Information se rapportant à une personne physique), peu importe si le traitement a eu lieu en dehors ou en Chine, du moment que cela concerne les citoyens chinois se trouvant sur le territoire du pays.

Parmi les lois américaines qui définissent le cadre juridique américain, on retrouve le « **Patriot Act** » et le « **Cloud Act** ». **Ces deux « Act » représentent, de par leur portée extraterritoriale, les législations auxquelles les entreprises européennes pourraient être le plus soumises par rapport à la protection des données.**

D'autres textes viennent compléter ces réglementations comme la loi « Foreign Intelligence Surveillance Act » et le décret présidentiel « Executive order » qui sont plus de l'ordre du renseignement et de la surveillance. Ils permettent aux services de renseignements américains la collecte et le traitement des données des citoyens américains et étrangers.
Sans mandat judiciaire, les communications électroniques et les données de citoyens européens peuvent être interceptées. Ces deux lois servaient de base pour les opérations de surveillance et les programmes réalisés par la NSA (Révélés dans l'affaire Snowden) et font d'ailleurs partie des principales causes de l'annulation de l'accord sur la libre circulation des données entre les Etats-Unis et l'UE (Safe Harbor et Privacy Shield).

Voici les points importants à retenir pour ces deux (Un tableau comparatif des deux lois en *(Annexe 8)* :

A – Le « Patriot Act » :
Le « Patriot Act - Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act » est une loi mise en application le 26 Octobre 2001 (83) suite aux attentats terroristes du 11 Septembre 2001. Elle devait initialement durer 4 ans, sauf qu'une partie du texte est devenue permanente depuis 2005.
Son objectif est de permettre aux agences gouvernementales américaines (FBI, NSA, CIA, l'armée) d'obtenir des informations sans difficultés (possibilités d'intercepter les messages internet, mettre sur écoute des lignes téléphoniques, avoir accès à des documents, articles ...en toute légalité) lors des enquêtes liées à des actes possibles de terrorisme ou au financement de groupes terroristes.
Les enquêtes sont secrètes et la personne concernée n'est notifiée qu'à la fin de l'enquête pour ne pas impacter la récupération des informations. A noter que même un juge américain ne peut s'opposer à la transmission de ces informations.

B – Le « Cloud Act » :
Le « Cloud Act - Clarifyng Lawful Overseas Use of Data Act » est une loi mise en place le 23 Mars 2018 (84), elle faisait partie de la loi concernant le budget fédéral américain et modifiait la loi « Stored Communication Act de 1986 ».
Son objectif principal est de permettre, en cas d'enquête pénale, d'accéder aux données électroniques des entreprises localisées aux États-Unis ou dans d'autres pays. Concrètement, elle permet aux autorités américaines, bénéficiant d'un mandat dans le cadre d'une enquête judiciaire, d'avoir un accès plus rapide aux données électroniques stockées, qu'elles soient localisées sur le sol américain ou ailleurs.
En effet, sur demande des autorités américaines et sous mandat d'un juge américain, aux fournisseurs de services Cloud (L'entreprise américaine qui a le contrôle des données ou l'une de ses filiales hors sol américain), ces derniers sont dans l'obligation de fournir les données sous leur contrôle, sans prise en compte du lieu de stockage.

Le schéma résumant le processus de demande d'accès aux données auprès d'un client et de son fournisseur Cloud est présenté en *(Annexe 9).*

A noter que le « Cloud Act » ne s'applique pas seulement aux fournisseurs de services Cloud. Son champ d'application est plus large et concerne des logiciels et des outils numériques utilisés au quotidien et présents dans la plupart des entreprises européennes. Parmi les applications et logiciels qui entrent dans ce cadre, on retrouve des solutions de protection et sécurité des réseaux fournis par des entreprises américaines : Anti-malware, pare-feu…etc ainsi que, tous les outils américains fournissant des services de communication électronique comme Outlook, skype (toute la suite Microsoft Office).

Les fournisseurs de services Cloud américains essayent de rassurer leurs clients en indiquant qu'ils sont transparents quant aux nombres de demandes reçues de la part des forces de l'ordre américaines (AWS d'Amazon (85) et AZURE de Microsoft (86). **Les Avis des fournisseurs américains de services Cloud sur le « Cloud Act » en** *(Annexe 10).*

> Le Cloud Act au contact du RGPD :
Aujourd'hui, il n'y a aucun accord entre les États-Unis et l'UE qui facilite et cadre l'accès aux données personnelles. Rappelons que le RGPD indique clairement la nécessité d'un accord international pour le transfert ou la communication des données personnelles. Et que le Cloud Act quant à lui précise que les données peuvent être communiquées soit avec le consentement du client soit via un mandat délivré par un tribunal américain (sous réserve de justifications des motifs).

Prenons un exemple d'application :
Une entreprise française utilise les services Cloud d'un acteur américain, elle est donc exposée au règlement du Cloud Act. Suite à la demande des autorités américaines de transmettre les informations de son client, même en l'absence du consentement de ce dernier, ses données vont être divulguées.
En effet, même en essayant de respecter les directives RGPD afin de ne pas compromettre la confidentialité des données de son client, l'entreprise doit répondre favorablement à cette demande. Car au final, comme son fournisseur de Cloud, elle est soumise au droit américain Cloud Act.

Le RGPD, en revanche n'empêche pas les transferts justifiés dans le cadre d'une enquête *(Article 49 du RGPD) « dans un mémoire déposé devant la Cour Suprême en décembre 2017, la Commission Européenne a expliqué que cet article n'entendait pas empêcher tout transfert dans le cadre d'enquêtes, notamment des transferts qui trouvent justification au titre de l'article 49 du RGPD »* (87).

Le chiffrement qui pourrait être envisagé comme mesure de protection dans de telle situation ne permettra pas d'assurer la confidentialité des données. En effet, aux yeux de la loi américaine et française, le fournisseur de services Cloud (ou l'entreprise française) sont obligés de fournir les clés de chiffrement lors de la saisie, sinon ils feront l'objet d'une obstruction à l'enquête (88).

> Le cadre légal pour les échanges des données personnelles et les accords entre les Etats-Unis et l'Europe :
Dans le but de simplifier le transfert des données personnelles entre les Etats-Unis et l'Europe, deux accords ont été passés : Le « Safe Harbor » et le « Privacy Shield » :

- Safe Harbor : Accord mis en place entre 1998 et 2020, son objectif était d'établir un premier cadre juridique au transfert de données personnelles en provenance de l'Union européenne vers les entreprises américaines adhérentes (89).
- Privacy Shield : Texte mis en place en 2016 suite à l'invalidation du Safe Harbor, son objectif est de permettre les transferts de données personnelles tout en respectant à la fois les lois américaines et les lois européennes (90).

<u>Arrêt « Schrems 1 » – Invalidation du « Safe Harbor » – 2015 :</u>
À la suite de publications en 2013 du lanceur d'alerte américano-russe Edward Joseph Snowden (91), montrant que Facebook fournit des informations de ses utilisateurs au renseignement américain, un étudiant autrichien Max Schrems a attaqué en justice Facebook. Le dossier a été transféré de la justice irlandaise à la cour de justice européenne (CJUE) qui a tranché en faveur de Max Schrems et a invalidé ainsi le « Safe Harbor » en 2015.
Suite à l'annulation de cet accord, de nouveaux engagements sur la protection des données personnelles « Privacy Shield » ont été redéfinis entre la Commission européenne et le gouvernement américain.

<u>Arrêt « Schrems 2 » – Invalidation du « Privacy Shield » – 2020 :</u>
Max Schrems attaque de nouveau le texte « Privacy Shield » pour les mêmes manquements soulevés pour le Safe Harbor. En effet, malgré les corrections apportées à ce dernier, de nombreux points restaient à éclaircir, plus précisément au niveau des données européennes traitées par certaines entreprises américaines qui demeuraient

toujours accessibles au gouvernement américain et notamment le non-respect des règles du RGPD qui a été mis en place entre temps.
En 2020, la (CJUE) statue défavorablement une deuxième fois pour le « Privacy Shield » et l'invalide via la décision « Schrems 2 ».

A ce jour, il n'existe pas de loi officielle pour encadrer les échanges entre l'Europe et les Etats-Unis. En attendant, les deux parties ont mis en place (un accord de principe) un contrat de clauses contractuelles types (CCT) en application du RGPD le 25 mars 2022 (92).
Les Etats-Unis ont présenté le 07 octobre 2022 une nouvelle proposition. L'accord vise un nouveau cadre pour le transfert des données personnelles de l'UE vers les Etats-Unis. Avant son entrée en vigueur, il doit être étudié et validé par la Commission européenne (93).

Certains accords avec les États-Unis dans le cadre du « Cloud Act » ont déjà été signés et mis en pratique. Le premier accord est avec le Royaume-Uni : Le « Data Access Agreement » signé en 2019 et entré en vigueur le 03 Octobre 2022 pour une durée de 5 ans. *« À compter de cette date, les deux pays auront la possibilité de s'échanger des informations concernant leurs citoyens respectifs … et peut-être pas que »* (94).
L'Australie a signé le même accord en 2021 et le troisième accord est en cours de discussion avec le Canada depuis le deuxième trimestre 2022.

Au niveau de l'UE, la commission européenne a proposé une directive en Avril 2018 « E-Evidence » (95). Son objectif est de faciliter l'obtention des preuves électroniques dans le cadre d'une enquête judiciaire. Les États membres pourront s'échanger les preuves électroniques au niveau de l'UE, voire au niveau international. En effet, des négociations ont été entamées en septembre 2019 avec les Etats-Unis (96), et sont toujours en cours. L'accord vise à *« faciliter l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale »* (95).

Chapitre 4 – Quelques cas d'usage et conclusion

Cas d'usage :

Cas d'entreprise française	Types de données	Localisation des données	Localisation du fournisseur	Réglementation(s) applicable(s)	Point(s) de vigilance
Une entreprise de comptabilité dont les données sont hébergées chez un fournisseur Cloud américain	Données personnelles/Données stratégiques	Etats-Unis	Europe	RGPD Loi Informatique et Libertés	Penser à mettre en place la réglementation sur le secret des affaires (SDA) Cette entreprise pourrait être soumise au Cloud Act et Patriot Act si une enquête américaine était demandée
Une entreprise fournisseur d'électricité et prestataire d'un OSE dont le principal actionnaire détient la nationalité américaine et est soumis aux droits américains	Données non personnelles	France	France	NIS	Les sous-traitants sont soumis à la même réglementation que l'OSE dont ils sont les fournisseurs
La société, dont l'actionnaire est français, appartient à un groupe coté à la Bourse de New-York	Données mixtes (indissociables), y compris le savoir-faire de l'entreprise	France	France	RGPD Loi Informatique et Libertés	Règlement UE 2018 1807 sur les données non personnelles et le SDA
Les données de l'entreprise sont hébergées On-Premise mais chez IBM	Données de santé à caractère personnel	France	France	RGPD	Les hébergeurs de données de santé (HDS) sont soumis à la certification HDS Cloud Act et Patriot Act

Tableau 4 - Cas d'usage

Conclusion sur la réglementation

Les réglementations, normes et certifications européennes applicables aujourd'hui, et liées aux données ainsi que leur utilisation dans le Cloud, sont axées sur la protection de données des utilisateurs européens, sur la sécurité des systèmes d'information et sur la protection de la propriété des données au sein de l'UE (notamment dans les domaines stratégiques comme la santé ou le transports…).
Les projets en cours de validation ont pour objectifs de promouvoir l'interopérabilité des fournisseurs Cloud et la réversibilité des données, ainsi que l'orientation des Etats membres vers un Cloud dit « souverain ».
En effet, l'utilisation du Cloud représente des risques au niveau de la perte de contrôle des données et de leur confidentialité surtout pour les données stratégiques, ainsi qu'une forte exposition aux lois extraterritoriales (notamment américaines avec le Cloud Act et le Patriot Act).

Au niveau européen, plusieurs projets de « Cloud souverain » ont été initiés. Parmi les plus importants le « European Cloud Industrial Alliance » qui est en cours et le « Gaia-X » qui semble être bloqué. Ce dernier est fortement freiné depuis 2020 à cause du retrait de certains participants européens (Scaleway, Hoster) qui n'approuvent pas l'intégration des acteurs étrangers au projet (Sponsors *du Gaia-X Summit 2021 sont Microsoft, AWS, Alibaba et Huawei, des géants extra-européens* (97)*)*.
En effet, les GAFAM font partie des plus importants lobbyistes (Ici quelques chiffres (98)). Ils œuvrent à garder le monopole du marché Cloud (AWS, Azure, GCP représentent désormais 72 % du marché européen (99)) et semblent influer certains acteurs décisionnaires de l'UE sur les réglementations en leur faveur (Comme peut le démontrer une interview de Reuters avec Mme Vestager « vice-présidente exécutive de la Commission européenne en charge de la Concurrence et du Numérique », qui ne semblait pas inquiète de voir des entreprises abuser potentiellement de leur position dominante : *'Non, jusqu'à présent, nous n'avons eu aucune inquiétude' »* (100)).

Au niveau français, plusieurs offres hybrides « franco-américaines » sont en cours de construction, proposant un Cloud labellisé « Cloud de confiance » : Bleu de Capgemini et Orange & Microsoft ; S3NS de Thales & Google ; Numspot de Dassault Systèmes et pour finir, Docaposte et Bouygues Telecom avec AWS et Atos. Elles ont comme objectifs d'avoir un Cloud sécurisé avec un haut niveau technique et une « meilleure » protection face aux lois extraterritoriales.

En effet, pour atteindre un niveau équivalent des services proposés par les Cloudeurs (leaders américains), il est fort de constater aujourd'hui la dépendance des solutions Cloud européennes aux technologies étrangères. Comme l'estime le directeur général de l'ANSSI M. Guillaume POUPARD, les acteurs français du numérique ne seraient *« pas capables de faire du cloud de haut niveau en France aujourd'hui avec des technologies exclusivement françaises »* (101).

La stratégie « normative » européenne basée sur des lois (par exemple le RGPD, NIS), dont le but est de protéger les données sensibles et de contrer les lois extraterritoriales, semble insuffisante afin de garantir l'immunité contre ces dernières et une souveraineté des données. Le RGPD, texte plutôt défensif, ne fait que limiter la portée des lois extraterritoriales, qui elles à contrario, sont offensives.

Il est donc plus que nécessaire pour une organisation d'assurer la protection de ses données sensibles avant de les « exposer » dans le Cloud. Il serait judicieux pour une TPE/PME, qui n'a pas toujours les compétences en interne, de se faire conseiller par un juriste dans le territoire dans lesquels elle a prévu d'opérer et dans lesquels ses clients résident. En outre, les règlements évoluent fréquemment. Une veille juridique est indispensable afin de rester informé, mais également d'éviter de tomber sous la coupe des sanctions.

Partie 4 - Guide pratique d'une démarche pour aider les TPE/PME dans leur projet de migration Cloud

1. Contexte et hypothèse de l'étude :

Constat et hypothèses de l'étude :

Les TPE/PME ont tendance à utiliser le Cloud en mode SaaS. L'usage des services serait principalement dédié à la sauvegarde de données, associé à une déportation des principaux services utilisés au quotidien. Ces derniers seraient des logiciels bureautiques, de la messagerie électronique et des outils de gestion des clients ou de stock.

Les intérêts du Cloud pour les TPE/PME sont multiples. Les principales raisons sont rappelées dans le Chapitre 1 *(7. Atouts et Inconvénients des modèles de cloud).*

Néanmoins, en utilisant les services Cloud, la plupart des TPE/PME n'ont pas toujours conscience des risques encourus lors de l'hébergement de leurs données, ainsi que la réglementation à laquelle ces dernières sont soumises durant leur traitement. Cela est principalement dû à plusieurs raisons : méconnaissance de la valeur de leurs données et de la réglementation, manque de temps, faibles ressources financières et peu de compétences en interne pour mener à bien un projet de migration Cloud. Le choix du fournisseur reste également un élément important d'autant plus qu'elles n'ont généralement pas de levier de négociation au niveau du contrat et des CGU **(notamment concernant les engagements contractuels sur la protection des données, le partage des responsabilités, …)**

Les nombreuses raisons d'adopter le Cloud représentent, généralement, une plus grande aisance d'emploi pour les utilisateurs et des économies considérables pour les entreprises. Cependant, une concentration massive de ressources et de données constituent une cible plus attrayante pour les attaquants et cela malgré les défenses, ainsi que les mesures de sécurité que peuvent proposer les fournisseurs Cloud. Cette étude permet d'évaluer ces risques liés à la donnée et de fournir des recommandations permettant de réduire ces derniers.

Suite à notre constat, voici les hypothèses prises dans le cadre de notre cas d'usage :

- L'organisation a décidé de migrer ses données dans le Cloud et souhaite procéder à une analyse de risques sur ses données
- Elle envisage d'adopter une solution SAAS
- Nous nous concentrons sur la sécurisation des données et la réglementation applicable à ces dernières
- Ne sont pas traités dans cette étude : les applications, les éditeurs ou les fournisseurs d'application et de services
- Nous traiterons que les étapes d'avant-projet (phase d'étude) et non sa mise en œuvre

Objectif et étapes de l'étude :

L'objectif de notre étude est de proposer une démarche aux TPE/PME qui leur permettrait de prendre en compte la sécurité de leurs données avant de se décider à migrer dans le Cloud, de sorte à garantir la protection des données sensibles/critiques, ainsi que la conformité réglementaire.

A l'issue de cette étude, les risques les plus pertinents pour ce type d'entreprise seront identifiés, ainsi que des propositions de mesures de sécurité pour le traitement de chaque risque.

À la suite de cela, les risques identifiés et leurs impacts permettront à l'organisation de :

- Se décider, en fonction des contraintes et des bénéfices perçus, à migrer dans le Cloud ou pas.
- Choisir le type de Cloud Public, Privé, … et le fournisseur Cloud.
- Anticiper les potentiels risques et mettre en place des mesures de sécurité adéquates.

Les risques auxquels nos entreprises cibles pourraient être exposés dépendent de plusieurs paramètres : les services utilisés, le type de données traitées, l'écosystème de l'entreprise ou encore les actifs, pour n'en citer que quelques-uns. De ce fait, afin de prendre en compte la majorité des risques potentiels, nous avons imaginé des scénarios qui pourraient présenter des risques ayant de forts impacts sur les actifs des TPE/PME. Aussi, nous avons pris en compte les principaux risques liés à la donnée selon une étude de l'ENISA sur la migration dans le Cloud de trois entreprises (102).

Il n'existe pas de processus officiel ou normalisé pour un projet de migration dans le Cloud. Néanmoins, il peut se résumer en cinq parties pour la phase avant-projet :

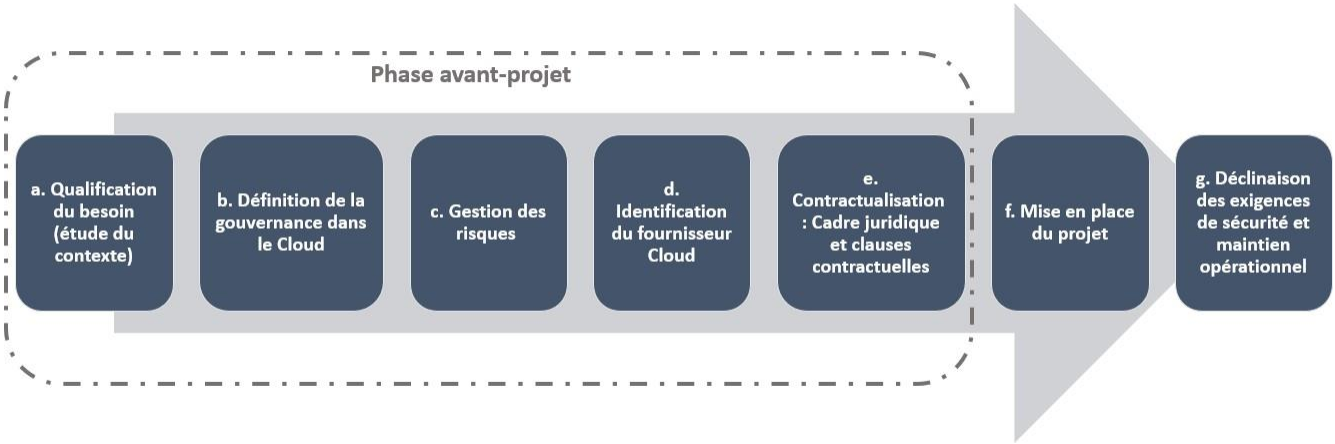


Figure 16 - Processus de migration dans le Cloud

La démarche que nous avons adoptée est une approche par les risques liés à la sécurité des données. En effet, la gestion des risques doit faire partie de la gouvernance de l'entreprise afin d'anticiper les décisions à prendre lorsqu'un événement redouté survient. En fonction des mesures à mettre en place, l'organisme saurait éviter ces risques, les réduire ou assurer un plan de continuité/ de reprise des activités en cas d'une attaque par exemple.

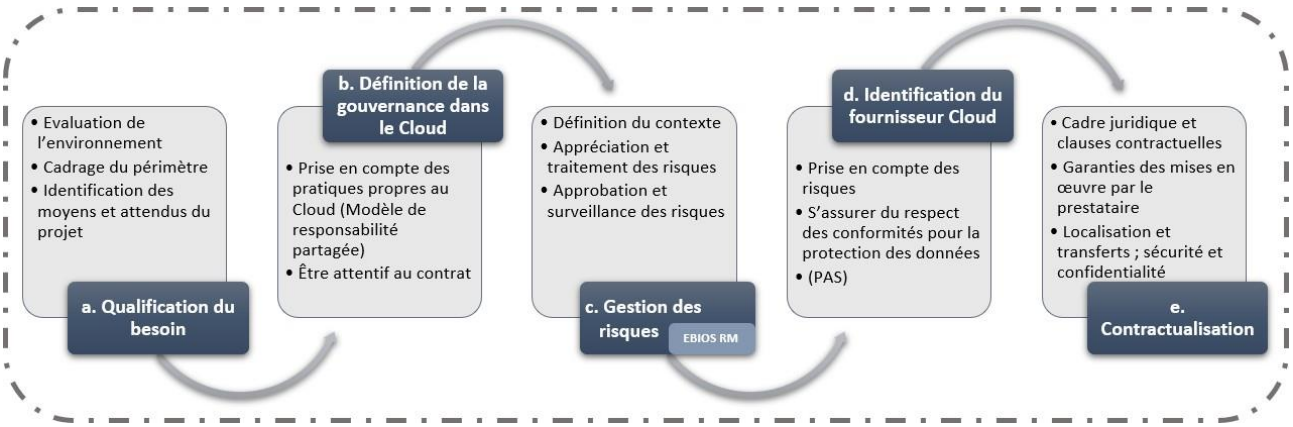


Figure 17 - Processus de la démarche proposée pour la migration dans le Cloud

De ce fait, notre démarche intègre cinq points (parties « a » à « e ») sur les sept listés au-dessus, correspondant à la phase avant-projet :

- **a. Qualification du besoin :** L'objectif est d'évaluer l'environnement, le cadrage du périmètre et d'identifier les moyens, ainsi que les attendus du projet.
- **b. Définition de la gouvernance dans le Cloud :** Evaluation des actions de gouvernance existantes, ainsi que la mise en place de nouvelles mesures. Prévoir l'adaptation de la stratégie de l'entreprise aux nouvelles contraintes du Cloud.
- **c. Gestion des risques :** Différentes méthodologies existent pour l'appréciation et le traitement des risques comme la norme ISO 27005:2022, les méthodes MEHARI ou EBIOS RM. Notre choix s'est porté sur cette dernière. Elles ont toutes des objectifs communs, à savoir : Définition du contexte ; Appréciation et traitement des risques ; Approbation et surveillance des risques
- **d. Identification du fournisseur Cloud :** Choix du fournisseur, ainsi que l'offre doivent se faire en prenant en compte les risques identifiés. En plus de notre évaluation de ces derniers, une liste de questions avec des recommandations sera présentée. Le but est de s'assurer du respect des conformités juridiques en termes de protections des données et de mettre en avant d'autres critères nécessaires pour la sélection du fournisseur Cloud.
- **e. Contractualisation :** S'assurer du respect des réglementations et des garanties mises en œuvre par le fournisseur. S'assurer de la sécurité et la confidentialité des données.

Un questionnaire sur les problématiques liées à la migration des données dans le Cloud, ici en *(Annexe 11)* servira de référentiel pour notre étude. A la fin de cette partie, les questions seront listées et identifiées pour chaque phase d'étude.

Les questions sont à adapter à la taille de la structure afin de répondre à ses propres besoins et en fonction de ses capacités en matière de SI.

Enfin, une étude de cas *(Annexe 12)* d'une entreprise fictive (Conseil&ST) illustrera notre démarche. En marge, en *(Annexe 13)* une analyse de risques des SI d'une entreprise réelle (BSI-Consulting) a été réalisée pour expliciter la méthode EBIOS RM en déroulant les cinq ateliers.

2. Qualification du besoin projet Cloud

La première étape consiste à évaluer les besoins du projet de déploiement Cloud. Dans un premier temps, l'entreprise peut s'appuyer sur la méthode QQOQCP (Qui ? Quoi ? Où ? Quand ? Comment ? Combien ? Pourquoi ?) pour mener une analyse contextuelle de leur besoin.

Cette phase de cadrage permet ainsi à l'organisation de se poser les bonnes questions dont l'objectif sera de répondre à une problématique définie. Cela permettra également aux équipes de travailler ensemble tout en partageant une même vision d'une situation donnée.

Il est primordial de s'interroger sur :

- Le système SI actuel (Ex : Cartographier, classifier et sécuriser les données sensibles/critiques de son organisation)
- Les utilisateurs du Cloud, c'est-à-dire de les identifier
- Les besoins métiers
- Les enjeux de sécurité des données (types de données traitées) et des accès
- Le type et le modèle de Cloud envisagé

- Toutes les mesures de sécurité supplémentaires que pourrait apporter la migration dans le Cloud

Afin de prendre en compte toutes les informations nécessaires pour évaluer ces besoins, il est important d'impliquer tous les métiers concernés et impactés par cette migration dès cette phase.

Nous supposons qu'à cette étape, l'intention de migration dans le Cloud est déjà approuvée par l'entreprise et ses dirigeants, mais qu'une étude de faisabilité doit être proposée avant toute décision de migration effective.

Ci-dessous, les réponses aux principales questions, extraites de la liste complète en *(Annexe 11)* que nous jugeons pertinentes pour cette partie :

QR1	**Quel est mon système d'information actuel ? Quel est le mode d'intégration ?** Cartographier son infrastructure et son parc applicatif et ses interfaces actuelles permettent d'en évaluer les performances et les limites en anticipant / priorisant les évolutions. Cela facilite également l'alignement stratégique. Connaitre son existant aide à mieux définir sa cible et à identifier les prérequis nécessaires afin de s'assurer des adaptations nécessaires pour migrer dans le cloud en termes de compatibilité avec les applications. La possibilité de faire des tests en amont pour déterminer les applications à transférer dans le cloud et d'en analyser les performances (test de latence, impact sur la bande passante de l'équipe…) peut faire partie des facteurs clés de succès du projet de migration. Il est important de comprendre en détail l'architecture de vos applications (tous les composants, leur dépendance et leur intégration) avant d'envisager leur migration vers le cloud.
QR2	**Qui seront les usagers du cloud ? (Interne DSI, métiers, partenaires externes, clients). Combien sont-ils ?** En répondant à cette question en amont, les parties prenantes seront impliquées à temps. Etablir une matrice de responsabilité de type RACI (Réalisateur, Approbateur, Consulté, et Informé) permettra de clarifier les rôles et responsabilités de chaque entité/personne. En définissant le nombre d'usagers, cela permet d'affiner le périmètre du projet et d'anticiper sur un des éléments du budget notamment pour les solutions SaaS où le paiement se fait à l'usage.
QR3	**Un audit de sécurité de mes systèmes d'information a-t-elle déjà été réalisé ? (Analyse de risques, tests d'intrusion…)** En procédant régulièrement à un audit de sécurité de son SI, l'entreprise est en capacité de révéler d'éventuelles failles ou dysfonctionnements qui pourraient compromettre ses activités. Elle vérifie ainsi qu'elle est alignée avec sa politique de sécurité et qu'elle est en conformité avec les référentiels en vigueur. Cela permet de s'assurer que la source de cette migration est saine et sécurisée. Si des audits ont déjà été réalisés, il faut les lister en précisant les dates de réalisation. Si le SI actuel n'est pas assez sécurisé, il faudrait prendre les bonnes dispositions.
QR4	**Quel est le modèle de cloud envisagé ? (Cloud public, cloud privé ou cloud hybride déployé en interne ou en externe) Quel est le type d'offre cloud envisagée ? (IaaS, PaaS, SaaS, etc.)** La rédaction d'une expression de besoin est une étape nécessaire qui décrit la situation actuelle (insatisfaisante) versus la situation future (satisfaisante) le tout combiné à une analyse fonctionnelle (fonction d'un domaine, d'un système…). Pendant cette étape, l'équipe à l'origine de ce besoin peut déjà envisagée le modèle de cloud qui pourrait répondant à sa problématique.
QR5	**Mes données hébergées seront-elles soumises au RGPD ? Ai-je des données sensibles/critiques à protéger ?** Se poser cette question en amont permet de restreindre la liste des fournisseurs et de s'assurer surtout que l'hébergeur est en conformité avec la réglementation en vigueur selon le lieu de stockage et traitement de vos données.

	Ma maîtrise d'œuvre est-elle externalisée ?
QR6	Il est primordial d'impliquer cette équipe dans ce projet en s'assurant qu'elle a toutes les compétences et la disponibilité pour vous accompagner lors de la migration. Il est également intéressant de se demander si elle doit évoluer après la migration et si elle est toujours nécessaire sous sa forme actuelle selon le cloud choisi.
	Mon pilotage économique (FinOps/TCO) est-il intégré dans ma transition ?
QR7	Avant de migrer vers le cloud, il est nécessaire de mener une analyse financière. Le modèle de déploiement SaaS est basé sur une solution de facturation à l'usage des services utilisés et en fonction du volume de ressources utilisées. Cela permet à l'entreprise d'avoir une flexibilité et d'anticiper ses coûts. En mettant en place des calculs du TCO (Coût total de possession, charges directes et indirectes) et du FinOps (monitorer et optimiser les coûts), l'entreprise réalise des économies d'échelle notamment à travers le nombre de jours nécessaires, ainsi que les coûts de licence et la formation par exemple réellement utilisés.

3. La gouvernance dans le Cloud

Le Cloud impacte quatre domaines de la gouvernance et de la gestion des risques. Ces domaines sont liés mais nécessitent des outils et processus différents :

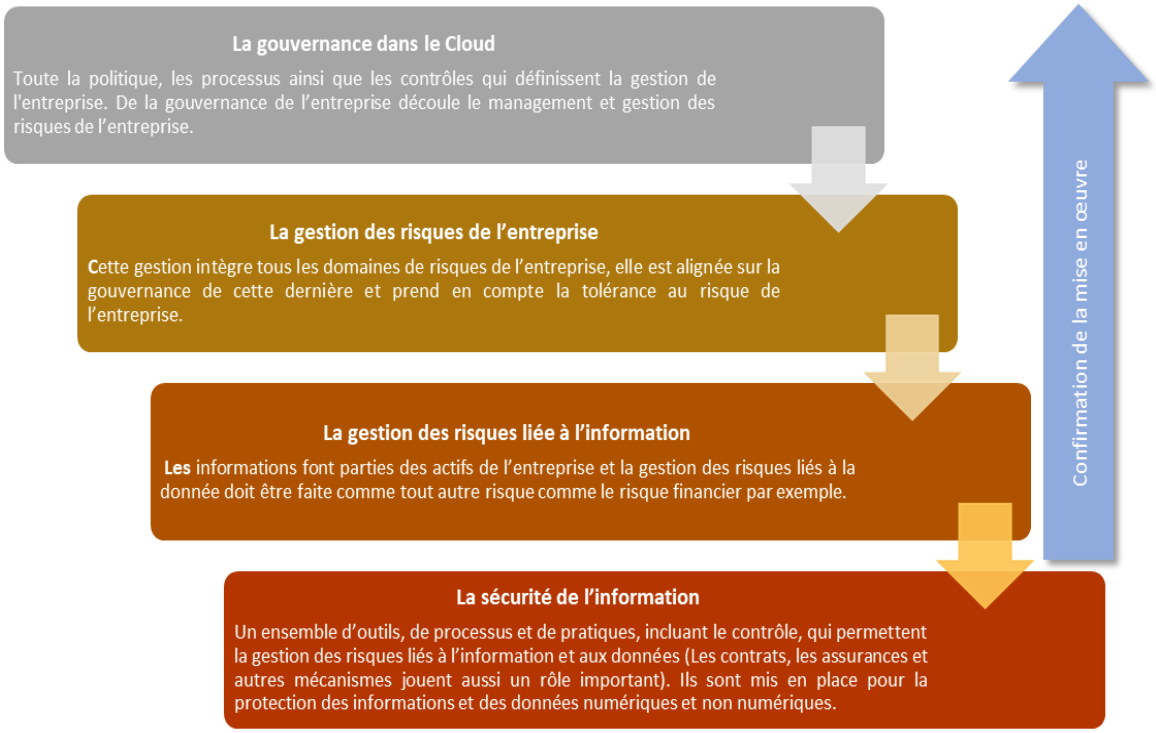


Figure 18 - Hiérarchie simplifiée des risques et de la gouvernance (103)

Les outils utilisés pour la gouvernance établissent un cadre pour les fournisseurs Cloud externes, mais peuvent aussi être utilisés dans le cadre d'un Cloud privé. Parmi ces outils, figure le contrat. En plus de garantir les niveaux de service et engagement, son rôle est d'étendre la gouvernance aux fournisseurs de services Cloud. D'autres outils sont utilisés, pour la Due diligence, pour l'évaluation des fournisseurs et pour les audits et contrôles.

Selon le type de Cloud (Public, privé ou autre), les responsabilités et les mécanismes mis en œuvre dans le cadre de la gouvernance d'une entreprise changent. En effet, ces derniers sont définis dans **le contrat, entre le client et le**

fournisseur Cloud, qui n'est pas forcément adapté aux critères de l'entreprise au **niveau juridique notamment**. Une attention particulière doit être portée à ces contraintes qui ne figurent pas nécessairement dans le contrat. Cela n'exclut pas le fournisseur en soit, néanmoins l'entreprise doit adapter son processus pour compenser ces lacunes, voire accepter les risques induits si possible.
En effet, le Cloud est basé sur le modèle **des responsabilités partagées**. Le fournisseur prend en charge qu'une partie des responsabilités et le client reste responsable de tout le reste. En fonction du modèle et du type de l'offre Cloud, ainsi que de la taille des fournisseurs, la capacité à gouverner dans le Cloud et les négociations des contrats varient :

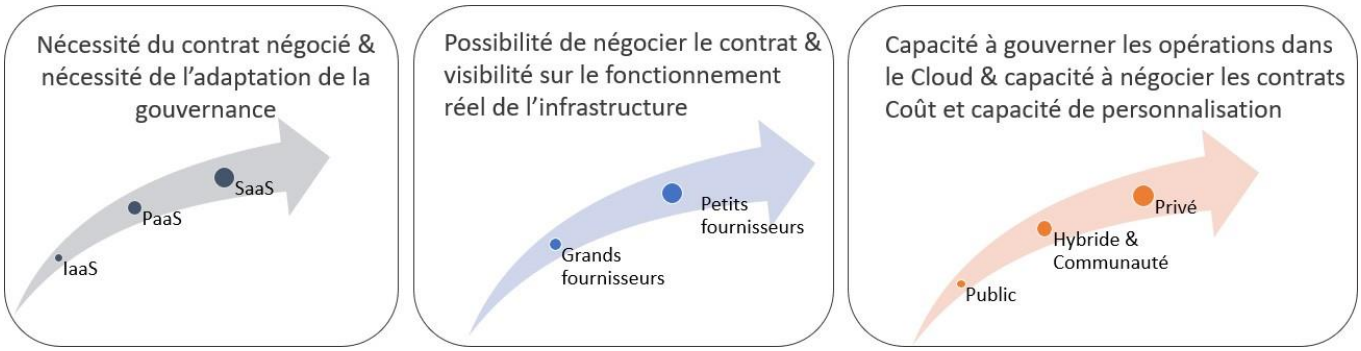


Figure 19 - Capacité à gouverner selon le modèle et le fournisseur Cloud

La définition de la gouvernance, dans le cadre du déploiement Cloud, consiste en l'évaluation des actions de gouvernance existantes, ainsi que la mise en place de nouvelles mesures. Le but est d'élaborer un plan de gouvernance *(Figure 20)* afin d'adapter la stratégie de l'entreprise à ces nouvelles contraintes et de décliner les nouvelles exigences au niveau de chaque projet, métier, mais aussi aux fournisseurs et toutes les parties prenantes. Dans le cadre d'un projet Cloud, cette gouvernance permettrait principalement à l'entreprise d'éviter les risques de sécurité et de tirer un maximum d'avantages du Cloud en termes d'agilité, d'efficacité et d'optimisation de coûts.
A noter que la responsabilité de la gouvernance ne peut jamais être externalisée même en faisant appel à des fournisseurs externes.

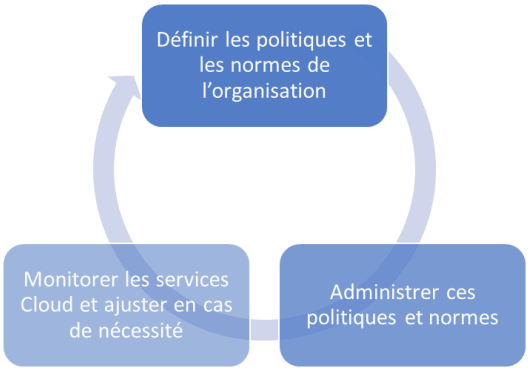


Figure 20 - Plan de gouvernance dans le Cloud

Voici sept bonnes pratiques à retenir lors de la définition de la gouvernance dans le cadre d'un projet Cloud (104) :

- Aligner la politique de gouvernance du Cloud sur les objectifs commerciaux et essayer d'être moins rigide (en cas de besoin d'innover) pour l'adapter à la culture de l'organisation
- Prendre en compte les pratiques de sécurité propre au Cloud qui est régie par le modèle de responsabilité partagée :
  - Personnaliser la stratégie de gouvernance avec des règles plus strictes pour les données sensibles

    - Gérer rigoureusement les rôles et les accès aux données sensibles
- Prendre en compte la gestion financière pour le suivi des dépenses dans le Cloud afin d'éviter les mauvaises surprises
- Faire cohabiter l'écosystème existant et le Cloud, puis se familiariser sur le plan technique et organisationnel à ce nouveau modèle
- Automatiser dans la mesure du possible les processus afin de garantir une détection plus facile des violations de politiques de sécurité (Ex. système automatisé d'alerte pour les accès non autorisés)
- Monitorer l'exploitation de son environnement Cloud, afin de connaître le fonctionnement des actifs à déployer, ainsi que les éventuels risques associés à ces derniers
- Être très attentif au contrat et au CGU (gestion des données, niveau de SLA, réversibilité…)

4. Gestion des risques identifiés pour la sécurisation des données

4.1 Méthodologie et processus de gestion des risques

Le processus de gestion des risques (Ex. Processus ISO 27005:2018 en *Figure 21*) permettra d'identifier, d'analyser et de traiter les risques. L'objectif est de mettre en place les mesures adéquates afin de minimiser et de maîtriser les risques connus et leurs potentielles conséquences sur la sécurité des données de l'entreprise.

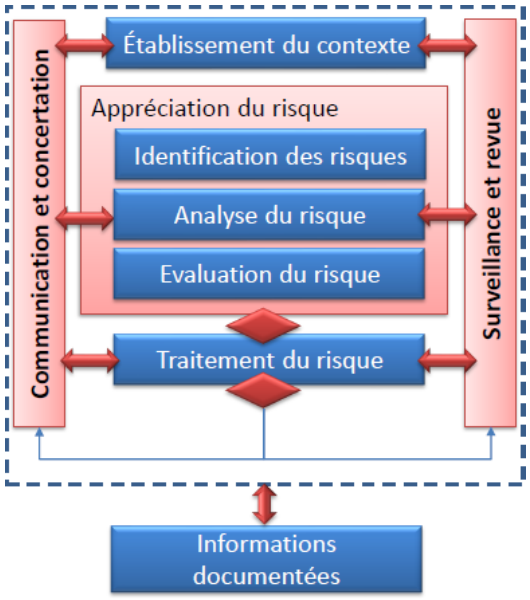


Figure 21 - Processus de gestion des risques ISO 27005 :2018

La méthode utilisée et qui nous paraît la plus adaptée pour la gestion des risques, dans notre cas d'étude, est la méthode française de l'ANSSI « EBIOS Risk Manager » (105). Il s'agit d'une méthode de gestion des risques liés à la sécurité des systèmes d'information.
Selon la définition de l'ANSSI : Elle *« adopte une approche de management du risque numérique partant du plus haut niveau (grandes missions de l'objet étudié) pour atteindre progressivement les fonctions métier et techniques, par l'étude des scénarios de risque possibles. »* et *« permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maîtriser. Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue. »*

Composée de 5 étapes / ateliers, elle est compatible avec les normes de références en matière de gestion des risques (ISO 31000:2018) et de sécurité numérique (la série des normes ISO/IEC 27000:2018).

Elle propose une boîte à outils adaptable constituant 5 ateliers :

- Atelier 1 : Cadrage et socle de sécurité
- Atelier 2 : Sources de risque
- Atelier 3 : Scénarios stratégiques
- Atelier 4 : Scénarios opérationnels
- Atelier 5 : Traitement du risque

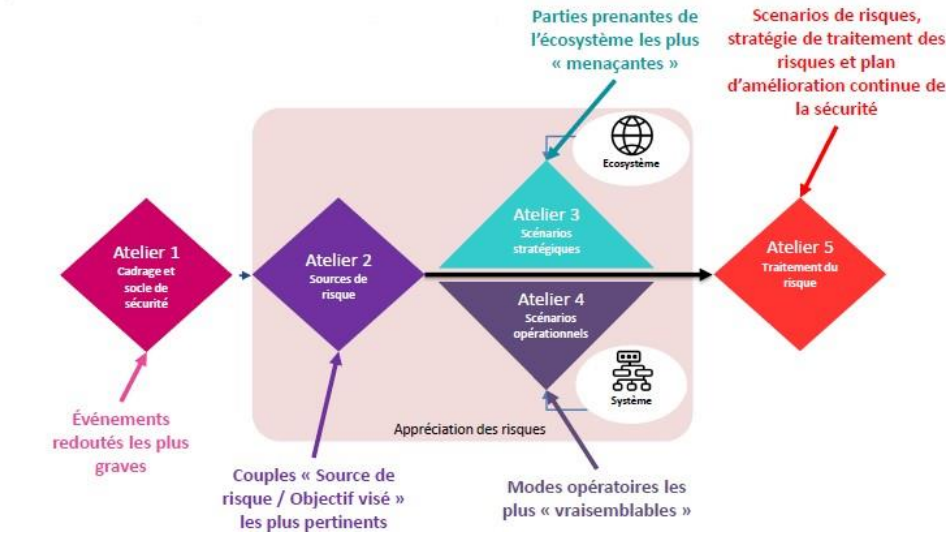


Figure 22 - Ateliers EBIOS RM

La méthode s'applique à toutes les entreprises quelle que soit leur taille. Selon les objectifs et la dimension de l'organisation, les ateliers seront à dérouler partiellement ou en totalité.

Dans notre cas d'étude, **seuls les scénarios 1, 4 et 5 seront déroulés car ils sont mieux adaptés aux TPE/PME, de par leur taille et leurs moyens financiers comme humains.**

4.2 Identification des actifs et des besoins de sécurité

Cette étape fait partie de l'Atelier 1 – Cadrage et socle de sécurité. L'objectif est d'identifier les missions de l'entreprise et d'évaluer les actifs et les biens supports.

<u>Le cadre de l'étude :</u>

Il convient d'identifier dans un premier temps les participants aux différents ateliers, leurs rôles, ainsi que leurs responsabilités. Une matrice de type RACI peut être définie avec les rôles suivants :

- L'analyse de risques est réalisée :
  - En ateliers avec la DSI et les métiers
  - Via une approche métier permettant d'identifier les événements redoutés
  - La qualification de la vraisemblance est portée par la DSI
- La DSI identifie :

- Les actifs
- Les mesures de sécurité déjà en place
- Les risques liés au SI
- Les causes qui sont l'origine de l'événement redouté (ex : exploitation d'une vulnérabilité, absence de mécanisme de chiffrement…)
- La vraisemblance c'est-à-dire l'évaluation de la probabilité d'occurrence du risque
- Le plan d'action

- Le Chef de Projet métier identifie :

  - Le besoin de sécurité des actifs (DCIT)
  - Les événements redoutés qui doivent être décrits de manière détaillée (ex : divulgation des données, indisponibilité du service, …)
  - Les conséquences par l'évaluation de leur matérialisation en rapport avec l'événement redouté (ex : altération de l'image de l'entreprise, amende, ...)
  - Les impacts en terme financier, de notoriété, juridique et règlementaire

Cette analyse est ensuite soumise à validation lors d'un comité de pilotage « COPIL » regroupant tous les acteurs du projet. Le COPIL s'engage ainsi à implémenter les mesures de sécurité identifiées et à allouer le budget adéquat.

Le périmètre technique :

Voici quelques questions qui pourront être posées afin de définir le périmètre :

- A quoi sert le service Cloud identifié ? Quelles sont ses missions principales, ses finalités ?
- Quels sont les processus et les informations majeures permettant au service Cloud de réaliser ses missions ?

L'ensemble des missions et des valeurs métiers peuvent être listées en utilisant ce tableau :

Missions	**La (ou les) mission(s) principale(s) de la TPE/PME**
Dénomination de la valeur métier	Exemple : R&D, Production, contrôle…etc
Nature de la valeur métier (processus ou information)	Processus ou information (Dans le cas de notre étude : information)
Description	Description de la valeur métier
Entité ou personne responsable (INTERNE/EXTERNE)	Responsable du processus ou de l'information
Dénomination du/des biens supports associés	Composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle
Description	Description du bien support
Entité ou personne responsable (INTERNE/EXTERNE)	Responsable du bien support

Tableau 5 - Tableau de recensement des missions, valeurs métiers et biens supports – Atelier 1

Ci-dessous, les actifs que nous avons identifiés et qui nous semblent pertinents, **cette liste est non-exhaustive et doit être adaptée selon le type d'activités de l'entreprise** (La liste selon EBIOS RM est présentée en *(Annexe 14)* :

Actifs d'information	Patrimoine intellectuel (Fichiers de données, bases de données, procédures, archives…) : - Données personnelles - Données sensibles - Données techniques - Savoir-faire
Actifs applicatifs	- Logiciels, outils de développement - Contrôle d'accès et interface de gestion des applications - Journaux d'événements opérationnels/de sécurité
Actifs humains	- Personnels/Décideurs - Utilisateurs (ingénieurs, techniciens…) - Image de la société et confiance des clients - Lien social interne (loyauté des employés et engagement) - Sauvegarde
	- Bâtiment - Serveurs informatiques - PC portables, matériels de communication, tablette…
Actifs financiers	- Chiffre d'affaires - Valeur en bourse - Revenus

Tableau 6 - Liste des actifs

Dans le cadre d'un projet de migration Cloud de type « SaaS », les actifs essentiels qui seront au cœur de la préoccupation de l'entreprise seraient les données à traiter. Elles sont sous la responsabilité du client, contrairement aux autres actifs tels que les supports qui seraient sûrement (selon le type d'offre Cloud sélectionné Public/Privé) sous la responsabilité du fournisseur Cloud.

Il faudra définir les besoins en termes de sécurité des données, car dans le cadre d'un projet Cloud, ces dernières sont encore plus exposées aux risques. Cette étape très importante permettra l'évaluation des impacts sur ces actifs et la détermination des risques critiques par la suite.

Différentes approches peuvent être utilisées pour l'évaluation des actifs *(Evaluation des actifs selon l'Enisa – Cloud Computing Security Risk Assessment « Chapitre 5 Assets »* Ou *Annexe B - (Identification et évaluation des actifs et appréciation des impacts) de la norme ISO 27005:2022).*

Pour ce faire, il faudrait au préalable définir une échelle d'évaluation multiniveaux en indiquant les raisons composées de critères et de métriques. **Il est recommandé d'évaluer ces actifs selon quatre critères de sécurité (DICT) : *Disponibilité, intégrité, confidentialité et traçabilité.***

- Disponibilité : L'utilisation et l'accessibilité attendue (résilience) des systèmes ou des données par les personnes autorisées [ISO 27000:2018]
- Intégrité : La protection de l'exactitude et de la complétude d'un actif [ISO 27000 :2018]
- Confidentialité : La propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés [ISO 27000]
- Traçabilité : Aptitude à conserver et retrouver les traces de l'état et des mouvements de l'information

Voici un exemple de matrice qui peut être utilisée pour l'estimation des besoins en sécurité des données :

Niveau	Disponibilité	Intégrité	Confidentialité	Traçabilité
1	Pas de disponibilité requise	Pas d'intégrité nécessaire	Les données sont accessibles publiquement	Pas de traçabilité nécessaire
2	La donnée ou le système ne peut être indisponible plus d'une semaine	L'intégrité doit être connue	L'accès doit être limité aux employés uniquement	Traçabilité nécessaire pour des besoins de qualité ou techniques
3	La donnée ou le système ne peut être indisponible plus d'une journée	L'intégrité doit être connue et récupérable	L'accès doit être limité à un groupe restreint d'employés uniquement	Traçabilité nécessaire pour des besoins métiers ou contractuels
4	La donnée ou le système ne peut être indisponible plus d'une heure	L'intégrité doit être garantie	L'accès doit être interdit pour tous	Traçabilité nécessaire pour des besoins légaux ou réglementaires

Tableau 7 - Besoins de sécurité des données – Atelier 1

Les métriques à mettre en place pour la disponibilité sont propres à chaque entreprise. Ils doivent être définis en accord avec le seuil d'acceptation (Le temps d'indisponibilité) et le niveau des impacts sur l'actif.

4.3 Identification des évènements redoutés (ER) et scénarios opérationnels

Identification des évènements redoutés :

Cette étape fait également partie de l'Atelier 1. Elle consiste à identifier les évènements redoutés (ER). Sous forme de scénarios, l'objectif est de permettre à l'entreprise de comprendre facilement le préjudice lié à l'atteinte de la sécurité de l'information. Le degré de l'impact est évalué selon une échelle de gravité :

G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégrade).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégrade).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Tableau 8 - Echelle de gravité (ER) EBIOS RM – Atelier 1

L'évaluation des besoins de sécurité peut aider à estimer le niveau de gravité. Ce dernier sera à définir en fonction du niveau de l'impact sur la sécurité des données afin d'assurer les missions de l'entreprise et de respecter la réglementation.
A noter qu'il convient de considérer tous les types d'impacts possibles, internes ou externes, directs ou indirects, pouvant porter atteinte à l'un des quatre critères de sécurité (DICT) des données traitées.

Dans le cadre de notre étude, nous avons imaginé des (ER) que toute TPE/PME pourrait rencontrer suite à sa migration dans le Cloud. Nous avons identifié 23 (ER) qui pourraient portés atteinte à l'un des critères de sécurité des données, à savoir :

- La disponibilité **(D)** : Données (ou systèmes donnant accès) inaccessibles ou perdues
- L'intégrité **(I)** : Modification des données ou détournement d'usage d'un service
- La confidentialité **(C)** : Divulgation d'informations, accès non autorisé, compromission de secret
- La traçabilité **(T)** : Impossibilité de tracer la modification d'une information

Pour chaque (ER), une cotation a été effectuée suivant l'échelle de gravité et les potentiels impacts sur l'entreprise ont été listés.

Les impacts identifiés sont (la liste des impacts selon EBIOS RM est présentée en *(Annexe 15))* :

Références des impacts	Impacts
IMPACT_1	Impact sur l'image de l'entreprise et la confiance des clients
IMPACT_2	Impact sur les missions et services de l'organisme
IMPACT_3	Impact financier
IMPACT_4	Impact sur le patrimoine intellectuel
IMPACT_5	Impact matériel (Destruction de biens supports)
IMPACT_6	Impact juridique
IMPACT_7	Impact sur le lien social interne (Perte de confiance des employés dans la pérennité de l'organisme et baisse de l'engagement)
IMPACT_8	Impact culturel (perte de ressources humaines clés)
IMPACT_9	Impact sur la capacité de développement ou de décision

Tableau 9 - Liste des impacts

A noter, que les impacts ne sont pas triés selon leur gravité. Notre évaluation des impacts est basée sur la donnée comme actif précieux de l'entreprise. Elle ne tient pas compte de l'aspect financier ou de certaines valeurs métier qui pourraient, dans certains cas, présenter aux yeux du dirigent de l'entreprise plus de valeur.

Suite à notre analyse des risques, le tableau suivant représente les impacts critiques des (ER) correspondant aux risques les plus élevés. Ces derniers représentent les cinq risques élevés que nous décidons de garder en « risques résiduels » **(En *Annexe 16* la liste complète des (ER) étudiés)** :

Réf (ER)	Evènement redouté	Impacts	Gravité	DICT (potentiellement atteint)
ER7	Perte de contrôle et de conformité aux exigences de sécurité (Manque de transparence de la part du fournisseur Cloud. Négligence et/ou mauvaise interprétation des responsabilités définies dans le contrat.)	IMPACT_1 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6 ; IMPACT_7 ; IMPACT_8 ; IMPACT_9	G4	(D) (I) (C) (T)
ER10	Changements de juridiction	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G4	(D) (C)
ER11	Non-respect de la réglementation sur la protection des données	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G4	(C)
ER12	Verrouillage du fournisseur Cloud	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4	G4	(D)
ER20	Mauvaise gestion des comptes/autorisations d'accès : Mauvais paramétrage / mauvaise configuration (Vulnérabilité au niveau du système d'exploitation, Erreur humaine, administrateur non formé ou mauvaise application des procédures de sécurité de base et de renforcement)	IMPACT_1 ; IMPACT_3 ; IMPACT_4 (Données de gestion des services Cloud, Données sensibles : stratégiques / personnelles) ; IMPACT_5 ; IMPACT_6 ; IMPACT_7 ; IMPACT_8	G4	(D) (I) (C) (T)

Tableau 10 - Les (ER) correspondant aux risques résiduels élevés

Scénarios opérationnels :

Cette étape fait partie de l'atelier 4. A partir des évènements redoutés, l'objectif est d'élaborer des scénarios opérationnels (SO) que pourraient exploiter les sources de risques pour atteindre leurs objectifs. Ensuite, l'évaluation de la vraisemblance sera faite, en prenant en compte la gravité des impacts. Ces deux paramètres permettront de définir la criticité des risques par la suite.

A noter que les sources de risques (SR) peuvent être multiples. En effet, cela dépendra de l'écosystème et des activités de l'entreprise. Elles peuvent être intentionnelles avec des objectifs visés pour :

- Un gain ou un positionnement sur un marché dans le cadre d'une concurrence déloyale (Etats, crime organisé, une société concurrente)
- Une motivation idéologique (terroristes, activistes)
- Une vengeance, un but lucratif (fraude, rançongiciel...) ou un défi, une reconnaissance ou un amusement (salarié ou prestataire mécontent, amateur, individus isolés ou officine spécialisée)

Les (SR) peuvent aussi provenir d'un manquement au niveau réglementaire, d'une non-conformité ou d'un non-respect des mesures de sécurité liés aux données.

Voici l'échelle utilisée pour l'évaluation de la vraisemblance des scénarios, ainsi que le tableau des (SO) correspondant aux risques résiduels retenus les plus élevés **(La liste complète des (SO) est en *Annexe 17*)** :

V1 **Peu vraisemblable**	La source de risque a très peu de chance d'atteindre son objectif visé en empruntant un des modes opératoires.
V2 **Vraisemblable**	La source de risque est susceptible d'atteindre son objectif visé en empruntant un des modes opératoires.
V3 **Très vraisemblable**	La source de risque va probablement atteindre son objectif visé en empruntant un des modes opératoires.
V4 **quasi certain**	La source de risque va certainement atteindre son objectif visé en empruntant un des modes opératoires.

Tableau 11 - Echelle d'évaluation de la vraisemblance

Réf. SO	Chemin d'attaque stratégique associé au scénario opérationnel	Vraisemblance globale
SO7	Négligence et/ou mauvaise interprétation des responsabilités définies dans le contrat OU Manque de transparence de la part du fournisseur Cloud (sur les fonctionnalités, localisation pour le stockage des données...). Exemples de cas : Chiffrement non compris dans le contrat --> mauvaise interprétation du client. Le client qui croit que le fournisseur Cloud est responsable de toute la sécurité des données alors que ce n'est pas compris dans le contrat --> mauvaise interprétation du client. Le fournisseur Cloud sous-traite le chiffrement des données à un prestataire qui ne fournit pas les mêmes garanties initialement annoncées --> manque de transparence.	**V4 - quasi certain**
SO10	Des données sensibles qui se retrouvent stockées dans un pays avec une juridiction différente et qui ne respecte pas les accords internationaux, ou la protection des données personnelles par exemple. Ou qui pourraient avoir accès ou saisir le matériel physique sans même avoir besoin d'une enquête.	**V4 - quasi certain**
SO11	Le fournisseur Cloud ne respecte pas la législation sur la protection des données personnelles, volontairement ou en perdant tout simplement le contrôle sur le traitement des données.	**V3 - Très vraisemblable**
SO12	Impossibilité d'exporter les applications existantes vers un autre fournisseur Cloud, ainsi que toutes les données au format standard (ou alors cela demanderait beaucoup de temps et un budget conséquent).	**V3 - Très vraisemblable**

SO20	Vol ou divulgation des données stratégiques de l'entreprise par un salarié mécontent. Suite à une mauvaise gestion des accès, ce dernier avait accès par erreur à des répertoires contenant des données sensibles.	**V3 - Très vraisemblable**

Tableau 12 - Les (SO) correspondant aux risques résiduels retenus les plus élevés

4.4 Traitement des risques identifiés

Cette partie présente le dernier Atelier 5 de l'EBIOS RM. Elle consiste à réaliser une synthèse des scénarios des risques identifiés, de définir la stratégie de traitement des risques, ainsi que les mesures de sécurité à mettre en place dans le cadre d'un plan d'amélioration continue de la sécurité. Il convient aussi, pour l'entreprise, d'évaluer les risques résiduels et de mettre en place un document pour leur suivi.

Dans le cadre de notre étude, nous allons définir les mesures de sécurité pour le traitement des risques les plus élevés et réaliser ensuite une synthèse des risques résiduels. Les questions/réponses en *(Annexe 11)* compléteront nos recommandations pour les autres risques identifiés.
Rappelons que les risques identifiés sont principalement liés à la sécurité des données et à la réglementation autour de ces dernières. Leur évaluation est basée sur nos évaluations avec comme principale valeur / actif : La donnée et les services dont elle pourrait dépendre.
L'appréciation des risques dépend fortement de ces actifs. Il convient pour chaque entreprise de prendre en compte cet aspect, car finalement c'est au dirigent de juger et de valider (ou pas) le traitement d'un risque.

Synthèse des scénarios de risques :

Le tableau suivant présente l'échelle choisie pour le seuil d'acceptabilité à trois niveaux :

Niveau du risque	Acceptabilité du risque	Intitulé des décisions et des actions
Faible	Acceptable en l'état	Aucune action n'est à entreprendre
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme
Elevé	Inacceptable	Des mesures de réduction du risque doivent impérativement être prises à court terme

Tableau 13 - Echelle d'acceptabilité des risques à trois niveaux

Ci-dessous, le tableau synthétisant les risques identifiés (R), selon 4 catégories, avant traitement (risques initiaux), ainsi que leur matrice.

Synthèse des risques avant traitement :

Réf. Risque	Catégories des risques	Risques	Niveau du risque	Sources de risque	(ER)	Gravité	(SO)	Vraisemblance

R5	Risques liés aux vulnérabilités techniques	Interception des données sensibles (personnelles, stratégiques) en transit	Elevé	Concurrent déloyal	ER5	G4	SO5	V3
R6	Autres risques	Accès aux données sensibles (personnelles, stratégiques) suite à une erreur ou absence de classification des données	Elevé	Salarié	ER6	G4	SO6	V3
R7	Risques liés à la réglementation et la non-conformité	Perte de contrôle et de conformité aux exigences de sécurité	Elevé	Contrat / Fournisseur	ER7	G4	SO7	V4
R9	Risques liés à la réglementation et la non-conformité	Divulgation forcée des données	Elevé	Concurrent déloyal/Etat	ER9	G4	SO9	V3
R10	Risques liés à la réglementation et la non-conformité	Changements de juridiction	Elevé	Fournisseur	ER10	G4	SO10	V4
R11	Risques liés à la réglementation et la non-conformité	Non-respect de la réglementation sur la protection des données	Elevé	Fournisseur	ER11	G4	SO11	V3
R12	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Verrouillage du fournisseur Cloud	Elevé	Fournisseur	ER12	G4	SO12	V3
R14	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Exploitation illégitime des données par le fournisseur Cloud (Personnel malveillant du fournisseur Cloud)	Elevé	Concurrent déloyal	ER14	G4	SO14	V3
R17	Risques liés aux vulnérabilités techniques	Défauts d'isolement des ressources	Elevé	Hacktiviste	ER17	G4	SO17	V3
R18	Risques liés aux vulnérabilités techniques	Compromission de l'interface de gestion des clients du fournisseur Cloud (Disponibilité de l'infrastructure, manipulation)	Elevé	Hacktiviste	ER18	G4	SO18	V3
R20	Risques liés aux vulnérabilités techniques	Mauvaise gestion des comptes/autorisations d'accès	Elevé	Salarié	ER20	G4	SO20	V3
R21	Autres risques	Utilisation d'application sans l'approbation de la Direction et du service IT (Shadow IT)	Elevé	Salarié	ER21	G4	SO21	V3

Tableau 14 - Synthèse des risques élevés avant traitement

Réf. Risque	Catégories des risques	Risques	Niveau du risque	Sources de risque	(ER)	Gravité	(SO)	Vraisemblance
R1	Risques liés aux vulnérabilités techniques	Perte des clés de chiffrement nécessaires pour l'accès aux données	Moyen	Concurrent déloyal	ER1	G3	SO1	V2
R2	Risques liés aux vulnérabilités techniques	Attaque via une élévation de privilèges	Moyen	Salarié	ER2	G3	SO2	V2
R3	Autres risques	Attaque avec usurpation d'identité (ingénierie sociale)	Moyen	Amateur / Individu isolé	ER3	G3	SO3	V2
R4	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Perte ou vol de(s) seule(s) sauvegarde(s) existante(s)	Moyen	Hacktiviste	ER4	G4	SO4	V2
R8	Risques liés à la réglementation et la non-conformité	Suppression inefficace des données (Durée de conservation des données non respectée)	Moyen	Fournisseur	ER8	G3	SO8	V2
R13	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Défaillance de la chaîne d'approvisionnement	Moyen	Concurrent déloyal	ER13	G3	SO13	V2
R15	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Faille au niveau de la sécurité physique de l'infrastructure du fournisseur	Moyen	Concurrent déloyal	ER15	G4	SO15	V2
R16	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Acquisition du fournisseur Cloud (Possibilité de changement des conditions du contrat …)	Moyen	Fournisseur	ER16	G3	SO16	V2
R19	Risques liés aux vulnérabilités techniques	Perte ou compromission des journaux d'événements / sécurité (Besoin en cas d'enquête médico-légale)	Moyen	Fournisseur	ER19	G4	SO19	V2
R22	Autres risques	Catastrophe naturelle	Moyen	Catastrophe naturelle	ER22	G4	SO22	V2
R23	Autres risques	Vol de matériel informatique	Moyen	Personne Malveillante (Escroc)	ER23	G4	SO23	V2

Tableau 15 - Synthèse des risques avec un niveau moyen

Gravité \ Vraisemblance	V1 Peu vraisemblable	V2 Vraisemblable	V3 Très vraisemblable	V4 quasi certain
G1 MINEURE				
G2 SIGNIFICATIVE				
G3 GRAVE		R1 ; R2 ; R3 ; R8 ; R13 ; R16		
G4 CRITIQUE		R4 ; R15 ; R19 ; R22 ; R23	R5 ; R6 ; R9 ; R11 ; R12 ; R14 ; R17 ; R18 ; R20 ; R21	R7 ; R10

Tableau 16 - Matrice des risques avant traitement

Stratégie de traitement des risques et mesures de sécurité :

La stratégie de traitement des risques consiste à choisir une option appropriée afin d'éviter, réduire, transférer ou accepter le risque :

- L'éviter permet d'en supprimer la cause en éliminant totalement l'incertitude
- Le réduire l'amène à un niveau inférieur en minimisant la probabilité d'occurrence
- Le transférer à une tierce partie qui est principalement une assurance qui en supporterait les conséquences
- L'accepter ne demande aucune action mais nécessite une supervision

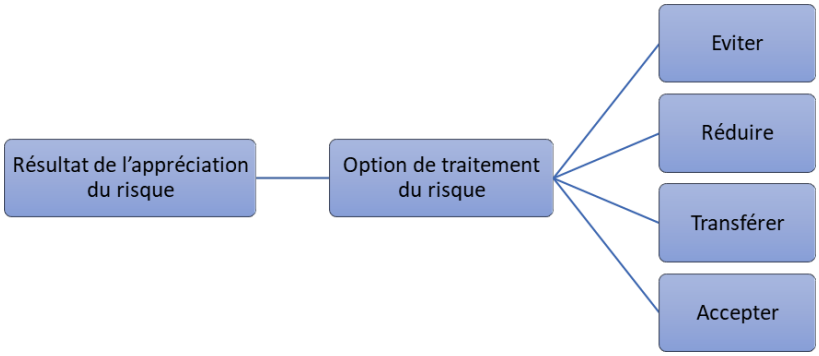


Figure 23 - Stratégie de traitement des risques

Parmi les douze risques élevés, nous avons identifiés sept risques que nous avons traités. En appliquant les recommandations proposées **(Détaillées en *Annexe 11*),** la vraisemblance des risques pourrait être diminuée. **Il est important de noter que les mesures de sécurité mises en place diminueraient les vraisemblances des risques en question, mais ne feront jamais baisser la gravité des impacts.**

Réf. Risque	Catégories des risques	Risques	Niveau du risque	Traitement	Gravité	Vraisemblance	Traitement du risque / Mesures de sécurité
R5	Risques liés aux vulnérabilités techniques	Interception des données sensibles (personnelles, stratégiques) en transit	Moyen	Transférer	G4	V2	QR29
R6	Autres risques	Accès aux données sensibles (personnelles, stratégiques) suite à une erreur ou absence de classification des données	Moyen	Réduire	G4	V2	QR30
R9	Risques liés à la réglementation et la non-conformité	Divulgation forcée des données	Moyen	Réduire	G4	V2	QR32
R14	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Exploitation illégitime des données par le fournisseur Cloud (Personnel malveillant du fournisseur Cloud)	Moyen	Transférer	G4	V2	QR13 ; QR15 ; QR17 ; QR18 ; QR24
R17	Risques liés aux vulnérabilités techniques	Défauts d'isolement des ressources	Moyen	Transférer	G4	V2	QR11 ; QR13 ; QR15 ; QR17 ; QR18 ; QR20 ; QR24 ; QR25
R18	Risques liés aux vulnérabilités techniques	Compromission de l'interface de gestion des clients du fournisseur Cloud (Disponibilité de l'infrastructure, manipulation)	Moyen	Transférer	G4	V2	QR11 ; QR13 ; QR15 ; QR17 ; QR18 ; QR20 ; QR24 ; QR25
R21	Autres risques	Utilisation d'application sans l'approbation de la Direction et du service IT (Shadow IT)	Moyen	Réduire	G4	V2	QR37 ; QR39

Tableau 17 - Traitement des risques élevés

A noter que le transfert des risques au fournisseur ne délègue, en aucun cas, toute la responsabilité à ce dernier. En effet, tous les risques ne seraient pas transférés au fournisseur, notamment certains risques qui ne peuvent pas être partagés, comme les risques entrainant une grave atteinte à l'image de l'entreprise, une faillite ou des implications juridiques.

Suite à l'analyse de risque, une étape finale d'acceptation des risques atteste que le porteur du projet a pris connaissance des risques et qu'il en assume la pleine responsabilité.

Ci-dessous, la matrice des risques retenus après traitement, ainsi que leur cartographie :

Gravité \ Vraisemblance	V1 Peu vraisemblable	V2 Vraisemblable	V3 Très vraisemblable	V4 quasi certain
G1 MINEURE				
G2 SIGNIFICATIVE				
G3 GRAVE		R1 ; R2 ; R3 ; R8 ; R13 ; R16		
G4 CRITIQUE		R4 ; R15 ; R19 ; R22 ; R23 ; R5 ; R6 ; R9 ; R14 ; R17 ; R18 ; R21	R11 ; R12 ; R20	R7 ; R10

Tableau 18 - Matrice des risques après traitement (Risques résiduels)

Réf. Risque	Catégories des risques	Risques	Niveau du risque	Traitement	Gravité	Vraisemblance	Traitement du risque / Mesures de sécurité
R7	Risques liés à la réglementation et la non-conformité	Perte de contrôle et de conformité aux exigences de sécurité	Elevé		G4	V4	QR17
R10	Risques liés à la réglementation et la non-conformité	Changements de juridiction	Elevé		G4	V4	QR27
R11	Risques liés à la réglementation et la non-conformité	Non-respect de la réglementation sur la protection des données	Elevé		G4	V3	QR27 ; QR5
R12	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Verrouillage du fournisseur Cloud	Elevé		G4	V3	QR28 ; QR34
R20	Risques liés aux vulnérabilités techniques	Mauvaise gestion des comptes/autorisations d'accès	Elevé		G4	V3	QR33 ; QR36 ; QR37

Tableau 19 - Risques résiduels élevés retenus

Figure 24 - Cartographie des risques après traitement

Au terme de l'analyse, la Direction doit formellement émettre sa décision quant aux risques résiduels.
Ce sont les risques qui subsistent après la mise en œuvre du traitement du risque. Ils doivent faire l'objet d'un suivi dans le temps (ex : chaque semestre) car leur vraisemblance peut évoluer.

Surveillance des risques

Surveillance des risques et revue

Une fois la stratégie de traitement des risques définie, les risques résiduels synthétisés et formellement acceptés par la Direction, il est conseillé de définir :

- Les mesures de sécurité reprises dans un Plan d'Amélioration Continue de la Sécurité (PACS) sous forme de tableau comme dans l'exemple ci-dessous :

Mesures de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	Coût / Complexité	Echéance	Statut

- Le cadre du suivi des risques à travers :
  - Le PACS
  - Les indicateurs de maintien en condition de sécurité pour vérifier l'efficacité des mesures prises et leur adaptation à l'état de la menace
  - Les mises à jour de l'étude des risques dans le respect des cycles stratégique et opérationnel prévus. En cas d'événements importants susceptibles de remettre en cause la pertinence des scénarios (émergence d'une nouvelle menace, évolutions applicables à la législation et à la réglementation, …), ceux-ci feront l'objet d'une mise à jour au juste niveau

En d'autres termes, il est recommandé de constituer un comité de pilotage se réunissant tous les six mois pour aborder cette montée en puissance ou tous les douze mois en rythme de croisière afin d'assurer un suivi des indicateurs, de l'avancement du PACS et de l'évolution des risques.

Gouvernance des risques et communication relative aux risques identifiés

La gouvernance (organisation, rôles et responsabilités, comités associés) devrait prévoir à ce stade :

- L'organisation de management de risque et l'amélioration continue
- La gestion du facteur humain via un programme de sensibilisation, de formation et d'entrainement à la sécurité de l'information
- La connaissance des vulnérabilités et de la menace grâce à la mise en place d'une veille

Il est également important d'élaborer un plan de communication relative aux risques indiquant :

- Leurs causes, leurs conséquences, leur vraisemblance et les moyens de maîtrise mis en œuvre pour les traiter aux parties intéressées externes et internes, ou fournies par celles-ci
- D'améliorer la compréhension mutuelle entre les propriétaires du risque (les responsabiliser) et les parties intéressées (la sensibilisation à la sécurité de l'information).

5. Identification du fournisseur Cloud

Avant de confier ses données à une tierce partie, il faut s'assurer que cette dernière est en capacité de les protéger. Le Plan d'Assurance Sécurité (PAS) adapté aux besoins de l'organisation représente une étape fondamentale dans cette analyse de risque et le choix du fournisseur Cloud.

Ce « PAS » a pour but de préciser comment les prestataires se conforment aux exigences de sécurité définies par l'organisation.
Il permet ainsi à un donneur d'ordre de solliciter, auprès de ses fournisseurs, des règles de sécurité qu'il impose, et par conséquent les garanties souhaitées. Dans notre cas d'étude, des garanties sur l'intégrité, la disponibilité et la confidentialité des données.
Le « PAS » est à la fois un document juridique et technique. En d'autres termes, le prestataire sera sanctionné si jamais il ne respecte pas les engagements.
Ce document constitue une action stratégique au stade de l'avant-vente pour évaluer le niveau de sécurité du fournisseur et contribue ainsi aux critères de choix de celui-ci.
Dans le but de vérifier que le niveau de sécurité du fournisseur Cloud est en adéquation avec les exigences de la TPE/PME, il convient d'adresser un questionnaire à celui-ci. Ce questionnaire fera figure d'analyse sécurité du fournisseur.
Ci-dessous, l'exemple de quelques questions qui pourraient être adressées au fournisseur. Il est à adapter à l'organisation et à ses besoins en termes d'exigences.

QUESTIONS	RÉPONSES
Où sont localisées les personnes qui ont accès aux données ? (Le support, les développeurs, …)	
Qui peut accéder à nos données tout au long du cycle de vie des données ? Quelle est la procédure en matière d'accès ?	
Est-ce que la solution fournit des moyens tels que l'anonymisation, la purge, ... pour limiter l'accès aux données ?	
Quels sont les moyens de réversibilité mis en place en cas de changement de fournisseur ?	
Proposez-vous des accords de SLA ?	
Existe-t-il une matrice d'escalade pour toute violation de sécurité ?	
Avez-vous déjà été victime d'une violation de sécurité ? Si oui, quelles actions avez-vous mises en œuvre pour éviter qu'elle ne se reproduise à l'avenir ?	
Quelles sont les dispositions réglementaires mises en place avec vos sous-traitants ?	
Les employés de vos sous-traitants signent-ils un accord de confidentialité avec vous qui inclut également la clause de confidentialité du contrat entre nous ?	
Décrivez le RACI autour de votre solution ainsi que les responsabilités partagées entre vous et nous	

Tableau 20 - Exemple de quelques questions à destination du fournisseur pour la préparation du « PAS »

Si le fournisseur ne dispose pas de « PAS » ou que ses réponses sont satisfaisantes, les 2 parties peuvent se baser sur ce questionnaire pour en rédiger un qui sera co-signé : Questionnaire sécurité proposé par La Cloud Security Alliance (CSA), adapté à tous les fournisseurs Cloud pour l'IAAS, le PAAS et le SAAS via son site STAR Level 1 : Security Questionnaire (CAIQ v4) | CSA *(cloudsecurityalliance.org).*

6. Contractualisation : Cadre juridique et clauses contractuelles

Concernant la contractualisation, la CNIL a publié des « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing » (106). Cette aide à la prise de décision se décline ainsi :

- Informations relatives aux traitements. (Ex : Respect des principes européens en matière de protection des données personnelles et de la loi Informatique et Libertés ; Moyens de traitement)
- Garanties mises en œuvre par le prestataire. (Ex : Durée de conservation des données limitée et raisonnable au regard des finalités pour lesquelles les données ont été collectées ; Destruction et/ou restitution des données en fin de prestation ou en cas de rupture anticipée du contrat dans un format structuré et couramment utilisé)
- Localisation et transferts. (Ex : Indication claire et exhaustive des pays hébergeant les centres de données du prestataire où les données seront traitées ; Information immédiate du client en cas de requête provenant d'une autorité administrative ou judiciaire étrangère)
- Formalités auprès de la CNIL
- Sécurité et confidentialité. (Ex : Indication des obligations incombant au prestataire en matière de sécurité des données et, lorsque celui-ci est sous-traitant, précision qu'il ne peut agir que sur instruction du client ; Réversibilité/portabilité : garantir la réversibilité ou la portabilité aisée des données dans un format structuré et couramment utilisé, sur demande du client et à tout moment)

Enfin, il est primordial de vérifier le cadre juridique et règlementaire des données hébergées et traitées par le fournisseur Cloud. Cela passe par la juridiction applicable « en fonction du type de données concernées (personnelles ou non), de la localisation de ces dernières, de la nationalité du prestataire ou de sa maison-mère ».

7. Les points à retenir et quelques recommandations

Les interrogations classées en différentes catégories peuvent être utilisées tout le long du processus. Elles permettront à l'entreprise de mieux qualifier les besoins du projet Cloud, de pouvoir anticiper les réponses à apporter aux enjeux de sécurité des données et de s'interroger sur les garanties que pourraient offrir les fournisseurs Cloud dans ce cadre. Les réponses apportées en *(Annexe 11)* aideront à définir les mesures de sécurité à mettre en œuvre.

A noter :

- **Cette liste n'est pas exhaustive et doit être complétée en fonction des activités de l'entreprise, de son écosystème et de ses attentes en termes de sécurité.**
- **Toutes les questions peuvent être utilisées durant les phases b et c.**

Réf. QR *(suivre le lien)*	QUESTIONS EN FONCTION DES PHASES DU PROCESSUS (LISTE NON EXHAUSTIVE)	Phase (En plus des phases b ; c)
	Qualification du besoin	
QR1	Quel est mon système d'information actuel ? Quel est le mode d'intégration ?	a
QR2	Qui seront les usagers du cloud ? (Interne DSI, métiers, partenaires externes, clients). Combien sont-ils ?	a
QR3	Un audit de sécurité de mes systèmes d'information a-t-elle déjà été réalisé ? (Analyse de risques, tests d'intrusion…)	a
QR4	Quel est le modèle de cloud envisagé ? (Cloud public, cloud privé ou cloud hybride déployé en interne ou en externe) Quel est le type d'offre cloud envisagée ? (IaaS, PaaS, SaaS, etc.)	a
QR5	Mes données hébergées seront-elles soumises au RGPD ? Ai-je des données sensibles/critiques à protéger ?	a

QR6	Ma maîtrise d'œuvre est-elle externalisée ?	a
QR7	Mon pilotage économique (FinOps/TCO) est-il intégré dans ma transition ?	a
	Contrat & Choix de l'offre	
QR8	Est-ce que toutes les conditions d'évolution (tarifaires, techniques...) de la solution Cloud sont clairement détaillées dans le contrat ?	e
QR9	Quelle est la durée du contrat et quelles sont les possibilités de rupture (même en cours de contrat) ?	e
QR10	Est-ce que le contrat est soumis au droit européen ou à d'autres réglementations ? Quelle est la politique et les engagements du fournisseur pour la protection des données personnelles ?	e
QR11	Quelles sont les mesures prisent par le fournisseur pour garantir que les tiers/sous-traitant respectent et maintiennent les niveaux de sécurité et de services ?	e
QR12	Est-ce que l'offre inclut un service d'infogérance ou de télémaintenance ?	e
QR13	Les services proposés et identifiés sont-ils couverts par l'assurance professionnelle du fournisseur en cas d'incident ?	e
QR14	Le fournisseur s'engage-t-il à fournir les journaux d'événements ? quelles informations, leur format et fuseau horaire ?	e
QR15	Quels sont les engagements du fournisseur en termes de communication sur les incidents de sécurité (fuite de données …) ?	e
QR16	Le fournisseur/hébergeur accepte-t-il d'être audité ?	e
QR17	Quelles sont les garanties de niveau de service ? (SLA, OLA) Est-ce que les rôles et responsabilités sont indiqués clairement dans le contrat ?	e
	Fournisseur / Prestataire (obligations)	
QR18	Quelle est la réputation du fournisseur ? Sa santé financière ? Fait-il partie d'un registre de référence de type CSA Star : https://cloudsecurityalliance.org/star/registry ?	d
QR19	Le prestataire fait-il appel à un SOC (Security Operations Center) ?	d
QR20	Est-ce que le fournisseur externalise / sous-traite des services qui sont essentiels à la sécurité de mes opérations / données ?	d
QR21	Quels sont les accès qu'auraient mes sous-traitants / fournisseurs ?	d
QR22	Les datacenters du fournisseur offrent-ils des garanties de sécurité suffisantes ? Quelles sont les assurances que le fournisseur peut communiquer pour la sécurité physique de son infrastructure ? Evaluation et gestion des risques, audits et contrôles ?	d
QR23	Est-ce qu'un fournisseur / sous-traitant de remplacement en cas d'incident a été identifié ?	d
QR24	Le fournisseur propose-t-il un Plan d'Assurance Sécurité (PAS) ?	d
	Réglementation & Sécurité des données/accès	
QR25	Comment garantir l'isolation des données entre les clients dans le cas d'un cloud public ?	d
QR26	Existe-t-il un processus d'archivage et de temps de rétention des données ?	d
QR27	Est-ce que le service Cloud utilisé implique le transfert de données vers un pays hors UE ? (Pour des raisons de support notamment)	d ; e
QR28	Que se passe-t-il au niveau des données à la fin du contrat avec le fournisseur Cloud ? (Procédure de réversibilité et d'effacement des données)	e
QR29	Comment les données seront-elles collectées, traitées et transférées ? Et comment seront-elles protégées et sécurisées ?	d ; e
QR30	Qui aura accès à mes données ?	d
QR31	La gouvernance du prestataire est-elle en conformité avec le RGPD ?	d

QR32	Quelles sont les restrictions en termes d'accès et les informations fournies au client en cas de requête provenant d'une autorité administrative ou judiciaire étrangère ?	d ; e
	Les aspects techniques	
QR33	Quelle est la solution de chiffrement prévue par le prestataire pour les données, notamment les données sensibles/critiques ? (En transit, au repos ou en cours de manipulation). Même question pour les échanges sensibles (mails confidentiels)	d
QR34	La migration est-elle réversible ?	d
QR35	Quelles sont les procédures de sauvegarde et de restauration des données ? Y a-t-il une redondance/copie prévue ? Si oui, sont-elles sauvegardées dans la même infrastructure de sauvegarde initiale ?	d
QR36	Comment se passe la gestion des comptes à haut niveau de privilège ?	c
QR37	Comment sera gérée l'identification des utilisateurs et des comptes dans le Cloud ?	d
QR38	Quelles sont nos limites de stockage dans le Cloud ?	d
QR39	Comment maintenir un environnement cloud sécurisé ?	d

Tableau 21 - Questionnaire en fonction des phases du processus de migration Cloud

Recommandations pour les risques résiduels :

R7 : Perte de contrôle et de conformité aux exigences de sécurité
Se référer à la QR17. Les TPE/PME n'ont généralement pas de possibilité de négociation, elles doivent donc vérifier en détail les items dont ils sont responsables. Pour les offres SaaS les responsabilités sont déléguées en grande partie au fournisseur Cloud. Il est donc nécessaire :

- Dans le cadre de la continuité et la reprise des activités suite à un incident, d'avoir au minimum des accords sur les niveaux de services (SLA/OLA) et des informations sur la durée minimale de disponibilité des systèmes, ainsi que la gestion et la réponse aux incidents
- De s'assurer de la répartition des responsabilités et des rôles définis dans le contrat

R10 : Changements de juridiction ; R11 : Non-respect de la réglementation sur la protection des données
Voir *Chapitre 3 : Cadre réglementaire et normatif autour du Cloud* pour plus de détails.
Il est très important de savoir les pays par lesquels les données vont transiter et où est-ce qu'elles seraient stockées physiquement. Il faut garder à l'esprit que différentes réglementations seront appliquées aux données : selon les lois locales du pays de stockage ou encore selon les lois du pays auxquelles les responsables de traitement dépendent. Aussi, Il faut s'assurer que le fournisseur est en conformité avec la réglementation en vigueur selon le lieu de stockage et traitement des données.

R12 : Verrouillage du fournisseur Cloud
Il faut pouvoir garder le contrôle sur ses données et d'éviter de se retrouver dépendant du fournisseur Cloud. Il est primordial de s'assurer de la réversibilité et de l'interopérabilité, respectivement des données et des applications. En d'autres termes, il faut être capable de pouvoir exporter les données et les transférer chez un autre fournisseur Cloud sans rupture de service. Et de s'assurer que les systèmes du fournisseur sont compatibles avec d'autres systèmes comme les logiciels libres par exemple ou avec les solutions utilisées dans un Multicloud.
Le cas du SaaS est le plus simple et le plus compliqué à la fois. Aujourd'hui aucune norme n'existe pour l'exportation des données.
Cependant, de nombreux fournisseurs de SaaS ont pensé une clause de réversibilité incluant la possibilité de réaliser à minima une extraction des données. Encore mieux, dans certains cas, l'API du fournisseur permet à des outils tiers de réaliser une migration automatisée vers un autre fournisseur. C'est le cas d'outils permettant de migrer par exemple de Salesforce.com vers Microsoft Dynamics et vice-versa.

R20 : Mauvaise gestion des comptes/autorisations d'accès

Généralement, les procédures de gestion des identifications des utilisateurs et des comptes dans le Cloud sont mises en place par le fournisseur, ces derniers ont développé leur propre procédure.
On peut y ajouter l'authentification multi facteurs (souvent proposée par le fournisseur) et on peut choisir aussi de mettre en place la fédération d'identité (pour les grosses PME uniquement). C'est-à-dire la possibilité d'utiliser une seule authentification sécurisée pour avoir accès à plusieurs ressources ou applications dans le Cloud.

Concernant les enjeux de sécurité liés aux utilisateurs à privilèges, voici les 5 recommandations fondamentales de l'ANSSI aux RSS/DSI :

- Limiter le nombre de comptes à privilèges
- Mot de passe individuel
- Séparation des postes de travail (cette mesure est peu accessible aux TPE/PME)
- Analyser les journaux d'évènements
- Supprimer les anciens comptes

Points d'attention pendant la phase de l'étude :

- La stratégie Cloud de l'organisation doit être bien définie pour faciliter la décision de déploiement des applications et de leurs données dans le Cloud
- La classification des données de l'entreprise est indispensable pour identifier leur niveau de sensibilité
- Les ressources internes et externes nécessaires pour mener à bien les analyses de risques doivent être identifiées pour s'assurer de leur disponibilité tout au long du projet
- La prise en compte des délais de réponse des fournisseurs lors de l'analyse de sécurité ne doit pas être négligés
- La conduite du changement doit être intégrée bien en amont pour que la sécurité ne soit pas identifiée comme un point de ralentissement du projet

Conclusion

La majorité des entreprises utilisent déjà quelques services Cloud comme les courriers électroniques par exemple. Un jour ou l'autre, même si l'entreprise n'a pas vocation à adopter le Cloud, elle sera devant le fait accompli car bon nombre de ses employés utilisera le Cloud.

Le Cloud se développe très vite et l'évolution technologique (Quantique, IA, Big data, Blockchain…) évolue parallèlement à l'apparition de nouvelles menaces. La réglementation accompagne ce changement et évolue en fonction des contextes géopolitiques. Il serait donc judicieux pour toute entreprise souhaitant assurer sa survie, tout en restant compétitive, d'anticiper les potentiels risques. De ce fait, il est nécessaire d'adapter sa gouvernance, de mettre en place une veille technologique et réglementaire. Puis, dans le cadre d'une amélioration continue, de suivre et d'intégrer ces contraintes aux risques existants de l'entreprise.

Au-delà des éventuels atouts en termes d'agilité, de résilience et d'économie, c'est aussi en termes de sécurité que les entreprises vont tirer avantages du Cloud. Les fournisseurs en sont conscients et par conséquent, mettent en place les mesures nécessaires pour protéger les données de leurs clients. Néanmoins, une mauvaise compréhension des risques encourus ou des responsabilités de part et d'autre peut conduire à des impacts graves en termes de coûts, sécurité et conformité pouvant menacer la survie de l'entreprise.

Selon notre entretien avec Emmanuel MEYRIEUX - Responsable sécurité clients chez OVHcloud,

" Trop d'entreprises n'ont pas encore pris la mesure des risques associés à leur utilisation des systèmes d'information, que ce soit On-Premise ou en Cloud. Du coup elles ont tendance à vouloir externaliser l'ensemble de leurs responsabilités ce qui n'est pas possible. Très peu de PME sont en maîtrise de leurs risques et elles ont tendance à se reposer sur leurs sous-traitants. Une tendance consiste aussi à externaliser notamment l'assistance à maîtrise d'ouvrage pour les systèmes d'information envoyés dans le Cloud. Cela entraîne des problèmes de compréhension par les entreprises de leur contexte opérationnel et de leurs risques "

Dans ce mémoire, nous avons proposé une approche à travers laquelle nous souhaitions éclairer les TPE/PME sur les risques liés au Cloud et les guider dans leur démarche de migration pour assurer la sécurité de leurs données.

L'objectif de ce guide n'est pas d'en faire un modèle de référence. La complexité du processus et les nombreux aspects à prendre en compte n'aident pas les TPE/PME à trouver facilement les réponses adéquates. Elles ne sont pas toujours conscientes des risques liés à leurs données. Nous avons donc essayé de présenter une approche pratique en différentes étapes, avec un questionnaire en référence et une étude de cas afin d'illustrer notre processus.

En guise de poursuite de ces travaux, voici quelques propositions :

- ✓ Elaborer une matrice d'aide à la décision déclinant la stratégie Cloud de l'entreprise
- ✓ Mettre en place une matrice avec les différentes réglementations en vigueur afin de pouvoir identifier plus facilement les contraintes juridiques
- ✓ Mise en œuvre de cette approche en collaboration avec un cabinet

Références

1. **32 chiffres et statistiques sur les TPE et PME en France en 2022.** 32 chiffres et statistiques sur les TPE et PME en France en 2022. *independant.io.* [En ligne] [Citation : 04 12 2022.] https://independant.io/chiffres-statistiques-tpe-pme/.

2. **ANSSI : PANORAMA DE LA MENACE INFORMATIQUE 2021.** PANORAMA DE LA MENACE INFORMATIQUE 2021. *www.cert.ssi.gouv.fr.* Citation : 04 12 2022

3. **2020, une année record pour les fuites de données.** 2020, une année record pour les fuites de données. *incyber.org.* Citation : 04 12 2022

4. **Epitech - Quand et comment est né internet.** La naissance d'Internet et du World Wide Web : vers la connectivité à l'échelle mondiale. *www.epitech.eu.* Citation : 30 11 2022

5. **The NIST Definition of Cloud Computing.** The NIST Definition of Cloud Computing. *csrc.nist.gov.*

6. **Architecture d'un Datacenter.** Architecture d'un datacenter. *www.dataxion.com.* Citation : 30 11 2022

7. **Illustration simplifiée DNS.** Domain Name System (DNS). *web.njit.edu.* Citation : 30 11 2022

8. **Le CIGREF : Fondamentaux du Cloud Computing.** Le CIGREF publie le rapport : Fondamentaux du Cloud Computing . *www.cigref.fr.* Citation : 30 11 2022

9. **Architecture du Cloud Computing .** Architecture du Cloud Computing . *www.researchgate.net.* [En ligne] Citation : 30 11 2022

10. **Attaque par déni de service.** Attaque par déni de service. *fr.wikipedia.org.* [

11. **Facebook : une fuite massive de données se profile, 2,8 milliards d'utilisateurs sont concernés.** Facebook : une fuite massive de données se profile, 2,8 milliards d'utilisateurs sont concernés. *www.phonandroid.com.*

12. **Mort de Code Spaces : les erreurs fatales d'un service Cloud.** Mort de Code Spaces : les erreurs fatales d'un service Cloud. *magazine.qualys.fr.* Citation : 30 11 2022 https://magazine.qualys.fr/menaces- alertes/code-spaces-mort/comment-page-1/

13. **Quelle est la différence entre une donnée et une information ?** Quelle est la différence entre une donnée et une information ? *www.iqualit.com.* Citation : 30 11 2022

14. **Comprendre les données structurées, semi-structuré, et non structurées.** Comprendre les données structurées, semi-structurées et non structurées. *www.astera.com.* Citation : 30 11 2022

15. **Une donnée à caractère personnel, c'est quoi ?** Une donnée à caractère personnel, c'est quoi ? *www.cnil.fr.* Citation : 30 11 2022

16. **Définition juridique et classification de la donnée Par Olivier de MAISON ROUGE.** Définition juridique et classification de la donnée. *www.journaldeleconomie.fr.* [Citation : 30 11 2022

17. . *www.vie- publique.fr.* [En ligne] [Citation : 30 11 2022

18. **RECOMMANDATIONS POUR LES ARCHITECTURES DES SYSTÈMES D'INFORMATION SENSIBLES OU DIFFUSION RESTREINTE.** RECOMMANDATIONS POUR LES ARCHITECTURES DES SYSTÈMES D'INFORMATION SENSIBLES OU DIFFUSION RESTREINTE. *www.ssi.gouv.fr.* Citation : 30 11 2022

19. **EXTERNALISATION ET SÉCURITÉ DES SYSTÈMES D'INFORMATION : UN GUIDE POUR MAÎTRISER LES RISQUES.** EXTERNALISATION ET SÉCURITÉ DES SYSTÈMES D'INFORMATION : UN GUIDE POUR MAÎTRISER LES RISQUES. *www.ssi.gouv.fr.* Citation : 30 11 2022

20. **LA CNIL : Les durées de conservation des données.** Les durées de conservation des données. *www.cnil.fr.* Citation : 30 11 2022

21. **THE EUROPEAN COMMISSION : CLOUD STRATEGY.** *ec.europa.eu.* Citation : 30 11 2022.].

22. **Le règlement UE 2018 1807.** RÈGLEMENT (UE) 2018/1807 DU PARLEMENT EUROPÉEN ET DU CONSEIL. *eur-lex.europa.eu.* Citation : 08 10 2022

23. **RÈGLEMENT (UE) 2016/679 (RGPD).** RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL. *eur-lex.europa.eu.* Citation : 08 10 2022

24. **ZDNET : RGPD : de la difficulté à faire appliquer le droit à l'oubli.** RGPD : de la difficulté à faire appliquer le droit à l'oubli. *www.zdnet.fr.* Citation : 30 11 2022

25. **NIS : RÉSULTATS DES ÉVALUATIONS EX POST DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT.** Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148. *eur-lex.europa.eu.* Citation : 08 10 2022

26. **Directive européenne sur la sécurité des réseaux, et des systèmes d'Information (NIS).** DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL. *eur-lex.europa.eu.* Citation : 08 10 2022

27. **NIS 2 : Révision de la directive (UE) 2016/1148.** DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL concerant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148. *eur-lex.europa.eu.*

28. **NIS 2 - Annexes : listes des entités essentielles, et importantes.** ANNEXES de la directive NIS 2. *eur-lex.europa.eu.* Citation : 08 10 2022

29. **Règlement sur la gouvernance européenne des données, Data Gouvernance Act.** Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la gouvernance européenne des données (acte sur la gouvernance des données). *eur-lex.europa.eu.* [Citation : 08 10 2022

30. **Data Act ; (règlement sur les données).** RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données). *eur-lex.europa.eu.* Citation : 08 10 2022

31. **Data Governance Act, Data Act : de quoi s'agit-il.** Stratégie européenne pour la donnée : la CNIL et ses homologues se prononcent sur le Data Governance Act et le Data Act. *cnil.fr.* Citation : 08 10 2022

32. **Cybersecurity Act, RÈGLEMENT(UE) 2019/881 relatif à l'ENISA ; la certification de cybersécurité des technologies de l'information & communications.** RÈGLEMENT (UE) 2019/881 DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité). *eur-lex.europa.eu.* [Citation : 08 10 2022.

33. **Cloud Computing Compliance Controls Catalogue (C5).** Cloud Computing Compliance Controls Catalogue (C5). *bsi.bund.de.* Citation : 08 10 2022

34. **Certifications espagnoles OC-CCN.** Certifications OC-CCN. *oc.ccn.cni.es.* Citation : 08 10 2022

35. **EUCS – Cloud Services Scheme.** EUCS – Cloud Services Scheme. *enisa.europa.eu.* Citation : 08 10 2022

36. **Position des associations d'utilisateurs allemande, et française sur le projet EUCS.** Position des associations d'utilisateurs, allemandes et françaises, sur le projet de schéma européen de certification pour le cloud. *cigref.fr.* Citation : 08 10 2022

37. **Lettre adressée à l'ENISA OVHcloud et 3DS Outscale appellent l'UE à ne pas céder au lobbying des géants américains.** Cloud : OVHcloud et 3DS Outscale appellent l'UE à ne pas céder au lobbying des géants américains. *lesnumeriques.com.* Citation : 08 10 2022

38. **Désaccord entre les pays européens sur le schéma, EUCS.** Projet de certification du Cloud en Europe : les européens loin de s'accorder. *actualites-cci.com.*

39. **PROPOSAL 15.9.2022, CYBER RESILIENCE ACT.** PROPOSAL 15.9.2022, CYBER RESILIENCE ACT. *european-cyber-resilience-act.com.*

40. **loi sur la cyber-résilience de l'UE - Questions et réponses.** État de l'Union : loi sur la cyber-résilience de l'UE – Questions et réponses. *ec.europa.eu.* Citation : 08 10 2022

41. **Stratégie pour un marché unique numérique en Europe.** Stratégie pour un marché unique numérique en Europe. *wayback.archive-it.org.*

42. **Cloud computing, Stratégies du Marché unique numérique.** Stratégies du Marché unique numérique - Cloud computing. *wayback.archive-it.org.*

43. **DSA (Législation sur les services, numériques).** RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE. *eur-lex.europa.eu.* Citation : 08 10 2022

44. **DMA (règlement sur les marchés numériques).** RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques). *data.consilium.europa.eu.* Citation : 08 10 2022

45. **Le secret des affaires : à la frontière de la vie, privée de l'entreprise Olivier de Maison Rouge.** Le secret des affaires : à la frontière de la vie privée de l'entreprise. *cairn.info.* Citation : 11 10 2022

46. **Etude de l'OMPI Magazine en 2019 sur la protection des secrets d'affaires.** Protection des secrets d'affaires : comment relever le défi des "dispositions raisonnables". *wipo.int.*

47. **RGPD : se préparer en 6 étapes - CNIL.** RGPD : se préparer en 6 étapes. *cnil.fr.* Citation : 11 10 2022.

48. **Checklist de la CNIL.** Évaluer le niveau de sécurité des données personnelles de votre organisme. *cnil.fr.* Citation : 11 10 2022

49. **Recommandations de la CNIL pour les entreprises, qui envisagent de souscrire à des services Cloud Computing.** Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing. *cnil.fr.* [Citation : 11 10 2022

50. **Rapport d'activité 2021 de la CNIL.** La CNIL publie son rapport d'activité 2021. *cnil.fr.* [En ligne] [Citation : 11 10 2022.] https://www.cnil.fr/fr/la-cnil-publie-son-rapport-dactivite-2021.

51. **CNIL : Le RGPD : la meilleure prévention, contre les risques cyber.** Le RGPD : la meilleure prévention contre les risques cyber. *cnil.fr.* [Citation : 11 10 2022

52. **BAROMÈTRE DATA BREACH par la CNIL.** BAROMÈTRE DATA BREACH. *cnil.fr.* Citation : 11 10 2022

53. **Les défauts de configuration des espaces de stockage dans le cloud public - La CNIL.** Violation du trimestre : les

défauts de configuration des espaces de stockage dans le cloud public. *cnil.fr.* Citation : 11 10 2022

54. **Plan stratégique 2022-2024 de la CNIL.** La CNIL publie son plan stratégique 2022-2024. *cnil.fr.* [En ligne] Citation : 11 10 2022

55. **Souveraineté numérique dans le cyberespace par Olivier de Maison Rouge.** Souveraineté numérique dans le cyberespace. *journaldeleconomie.fr.*

56. **Obligations des OIV et OSE - OODRIVE.** OIV et OSE : des obligations strictes pour la cybersécurité des acteurs de l'assurance. *oodrive.com.* Citation : 12 10 2022

57. **ANSSI : Les dispositifs de cybersécurité pour les OSE.** NIS : UN DISPOSITIF DE CYBERSÉCURITÉ POUR LES OPÉRATEURS DE SERVICES ESSENTIELS. *ssi.gouv.fr.* Citation : 12 10 2022

58. **ANSSI : DISPOSITIF DE CYBERSÉCURITÉ POUR, LES FSN.** UN DISPOSITIF DE CYBERSÉCURITÉ POUR LES FOURNISSEURS DE SERVICE NUMÉRIQUE. *ssi.gouv.fr.* Citation : 12 10 2022.

59. **Sécurité des données de santé - Orange Healthcare.** Sécurité des données de santé. *healthcare.orange.com.* Citation : 12 10 2022.

60. **CNIL : Qu'est-ce ce qu'une donnée de santé ?** *cnil.fr.* Citation : 12 10 2022

61. **esante : solutions de santé électroniques , en France.** La transformation numérique de notre système de santé commence ici, pour vous et avec vous ! *esante.gouv.fr.* [En ligne] [Citation : 12 10 2022.] https://esante.gouv.fr/.

62. **HDS : Certification Hébergeur de Données de Santé.** HDS : Certification Hébergeur de Données de Santé. *esante.gouv.fr.* Citation : 12 10 2022

63. **esante : Liste des hébergeurs certifiés.** Liste des hébergeurs certifiés. *esante.gouv.fr.* [En ligne] [Citation : 12 10 2022.] https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies.

64. **esante : Liste des organismes de certification HDS.** Liste des organismes de certification HDS. *esante.gouv.fr.* Citation : 12 10 2022

65. **Les référentiels de la procédure de certification de santé.** Les référentiels de la procédure de certification. *esante.gouv.fr.* [Citation : 12 10 2022

66. **Cybersécurité dans le secteur, esante.** Cybersécurité dans le secteur. *esante.gouv.fr.* Citation : 12 10 2022

67. **Cybersécurité, données de santé, cookies, CNIL.** Cybersécurité, données de santé, cookies : les thématiques prioritaires de contrôle en 2021. *cnil.fr.* Citation : 12 10 2022

68. **Affaire FACEBOOK IRELAND ET SCHREMS.** ARRÊT DU 16. 7. 2020 – AFFAIRE C-311/18 FACEBOOK IRELAND ET SCHREMS. *eur-lex.europa.eu.* Citation : 12 10 2022

69. **La Cnil ne veut pas de Microsoft pour héberger les données de santé des Français.** La Cnil ne veut pas de Microsoft pour héberger les données de santé des Français. *journaldeleconomie.fr.* Citation : 12 10 2022

70. **CNIL : La Plateforme des données de santé (Health Data Hub).** La Plateforme des données de santé (Health Data Hub). *cnil.fr.* Citation : 12 10 2022

71. **La CNIL sanctionne deux médecins pour violation de, données de santé.** La CNIL sanctionne deux médecins pour violation de données de santé. *usine-digitale.fr.*

72. **CNIL : Sanction DEDALUS BIOLOGIE pour, fuite de données.** Fuite de données de santé : sanction de 1,5 million

d'euros à l'encontre de la société DEDALUS BIOLOGIE. *cnil.fr.* Citation : 12 10 2022

73. **Stratégie nationale pour le Cloud, Gouvernement français.** STRATÉGIE NATIONALE POUR LE CLOUD Soutenir l'innovation dans le Cloud. *gouvernement.fr.* Citation : 12 10 2022

74. **Doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre ») legifrance.** Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État. *legifrance.gouv.fr.* Citation : 12 10 2022

75. **Référentiel d'exigences Prestataires de services de services d'informatique en nuage (SecNumCloud).** Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences. *ssi.gouv.fr.* [En ligne] Citation : 12 10 2022

76. **SecNumCloud, « Cloud de confiance ». Infographie, oodrive.** SecNumCloud, ce rempart de la souveraineté des données numériques pour un « Cloud de confiance ». Infographie. *oodrive.com.* Citation : 12 10 2022

77. **Durcissement de la loi Russe pour les données personnelles.** Données personnelles : la Russie durcit sa réglementation, les DSI sur le pont. *silicon.fr.* Citation : 08 10 2022

78. **Russie - Amende contre Google pour défaut, de stockage des données personnelles en Russie.** Google écope d'une amende de 34 500 euros pour défaut de stockage des données personnelles en Russie. *usine-digitale.fr.*] Citation : 08 10 2022

79. **Russie - Blocage de LinkedIn pour défaut de stockage des données personnelles en Russie.** La justice russe ordonne de bloquer le réseau social LinkedIn en Russie. *lemonde.fr.* Citation : 08 10 2022

80. **Data Security Law of the People's Republic of China.** Data Security Law of the People's Republic of China. *en.wikipedia.org.*

81. **Chine - Personal Information Protection Law (PIPL).** Personal Information Protection Law of the People's Republic of China. *en.wikipedia.org.*

82. **GDPR Versus PIPL - Principales différences.** GDPR Versus PIPL - Principales différences et implications pour la conformité en Chine. *china-briefing.com.*

83. **Patriot Act - Définition.** DEFINITION Patriot Act. *lemagit.fr.* Citation : 08 10 2022

84. **CLOUD Act Clarifying Lawful Overseas Use of Data Act.** CLOUD Act. *fr.wikipedia.org.*

85. **Avis AWS - Amazon sur le Cloud Act.** Clarifying Lawful Overseas Use of Data (CLOUD) Act. *aws.amazon.com.* Citation : 08 10 2022

86. **Microsoft - Rapport sur les demandes d'application de la loi.** Rapport sur les demandes d'application de la loi. *microsoft.com.* Citation : 08 10 2022

87. **Cloud Act au contact du RGPD.** LE CLOUD ACT AMÉRICAIN NE PERMET PAS D'ESPIONNER LES ENTREPRISES EUROPÉENNES. *eurocloud.fr.* Citation : 08 10 2022

88. **CLOUD Act : entre le marteau et l'enclume, Chiffrement des données dans le Cloud.** CLOUD Act : entre le marteau et l'enclume. *lemagit.fr.* Citation : 08 10 2022

89. **Définition de Safe Harbor.** Définition de Safe Harbor. *glossaire-international.com.*

90. **Bouclier de protection des données UE-États-Unis.** Bouclier de protection des données UE-États-Unis. *fr.wikipedia.org.*

91. **Edward Snowden.** Edward Snowden. https://fr.wikipedia.org/wiki/Edward_Snowden.

92. **Accord de principe entre l'UE et les Etats-Unis, pour le transfert des données à caractère personnel.** Vers un nouvel accord pour le transfert des données entre l'UE et les États-Unis. *nextinpact.com.* Citation : 08 10 2022

93. **Proposition d'un nouvel accord de la part des Etats-Unis pour remplacer le Privacy Shield.** Transfert des données avec l'Europe : les États-Unis présentent les nouvelles règles de l'accord. *lefigaro.fr.* Citation : 08 10 2022

94. **Accord dans le cadre du Cloud Act entre, les Etats-Unis et d'autres pays.** Les États-Unis et le Royaume-Uni vont-ils s'échanger vos données personnelles ? *portail-rgpd.com.*

95. **Proposition de règles UE pour faciliter l'accès, aux preuves électroniques au niveau international.** Union de la sécurité: la Commission facilite l'accès aux preuves électroniques. *ec.europa.eu.* Citation : 08 10 2022

96. **Négociations entre UE et les Etats-Unis, Projet "E-evidence".** Un meilleur accès aux preuves électroniques pour lutter contre la criminalité. *consilium.europa.eu.* Citation : 08 10 2022

97. **Scaleway quitte le projet Gaia-X.** Scaleway quitte le projet Gaia-X. *www.guideinformatique.com.* [En ligne] Citation : 30 11 2022

98. **Big Tech Lobbying Google, Amazon &, friends and their hidden influence.** Big Tech Lobbying Google, Amazon & friends and their hidden influence. *corporateeurope.org.* [Citation : 30 11 2022

99. **Synergy : European Cloud Providers Continue , to Grow but Still Lose Market Share.** European Cloud Providers Continue to Grow but Still Lose Market Share. *www.srgresearch.com.* Citation : 30 11 2022

100.

101. **Reuters : Selon Mme Vestager, l'informatique dématérialisée ne suscite pas encore d'inquiétude.** Selon Mme Vestager, l'informatique dématérialisée ne suscite pas encore d'inquiétude sur le plan de la concurrence. *www.zonebourse.com.* Citation : 30 11 2022

102. **Cloud de confiance selon Guillaume POUPARD.** ur le cloud de confiance, on ne parle pas de souveraineté absolue » (Guillaume Poupard, Anssi). *www.latribune.fr.* Citation : 30 11 2022

103. **ENISA : Cloud Computing Risk Assessment.** ENISA : Cloud Computing Risk Assessment. *www.enisa.europa.eu.* [En ligne] [Citation : 30 11 2022.] https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

104. **CSA Security Guidance for Critical Areas of Focus in Cloud Computing.** CSA Security Guidance for Critical, Areas of Focus in Cloud Computing. *cloudsecurityalliance.org.* Citation : 30 11 2022

105. **Pratiques redsen-consulting : Gouvernance cloud : les bonnes.** Gouvernance cloud : les bonnes pratiques. *www.redsen-consulting.com.* [En ligne] [Citation : 30 11 2022.] https://www.redsen-consulting.com/transformation-digitale/gouvernance-cloud-bonnes-pratiques/.

106. **LA MÉTHODE EBIOS RISK MANAGER – LE GUIDE.** LA MÉTHODE EBIOS RISK MANAGER – LE GUIDE. *www.ssi.gouv.fr.* Citation : 30 11 2022

107. **CNIL : Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing.** Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing. *www.cnil.fr.* Citation : 30 11 2022

108. **Rapport Amazon sur les demandes du gouvernement, américain.** Amazon Information Request Report. *d1.awsstatic.com.* Citation : 08 10 2022

109. **Demandes internationales d'informations sur, les utilisateurs - Google.** Demandes internationales

d'informations sur les utilisateurs. *transparencyreport.google.com.* Citation : 08 10 2022

110. **Etude sur le Cloud Act et les données fournies, par les fournisseurs de Cloud américains riskinsight-wavestone.** Le C.L.O.U.D Act. : Une manière de rendre les données « non-souveraines » ? *riskinsight-wavestone.com.* Citation : 08 10 2022

111. **IFP : Les 7 questions les plus importantes à poser, à un fournisseur de cloud.** Les 7 questions les plus importantes à poser, à un fournisseur de cloud. *www.insightsforprofessionals.com.*

112.

113. **AddWorking : 4 conditions pour bien piloter les missions de vos sous-traitants.** 4 conditions pour bien piloter les missions de vos sous-traitants. *www.addworking.com.* Citation : 30 11 2022

114. **Conseil général de l'économie : La responsabilité des fournisseurs de systèmes numériques.** La responsabilité des fournisseurs de systèmes. *www.economie.gouv.fr.* Citation : 30 11 2022

115. **IFP : Les 7 questions les plus importantes à poser, à un fournisseur de cloud.** Les 7 questions les plus importantes à poser à un fournisseur de cloud. *www.insightsforprofessionals.com.* Citation : 30 11 2022

116. **uniprint : 3 étapes pour l'audit d'un fournisseur , de services cloud.** 3 étapes pour l'audit d'un fournisseur de services cloud. *www.uniprint.net.* Citation : 30 11 2022

117. **Yousri Kouki : Approche dirigée par les contrats, de niveaux de service pour la gestion de l'élasticité du "nuage".** Approche dirigée par les contrats de niveaux de service pour la gestion de l'élasticité du "nuage" - Yousri Kouki. *theses.hal.science.* Citation : 30 11 2022

118. **CSA : SECURITY GUIDANCE FOR CRITICAL AREAS, OF FOCUS IN CLOUD COMPUTING V3.0.** SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0. *downloads.cloudsecurityalliance.org.* Citation : 30 11 2022

119. **Guide sur le Cloud Computing et les Datacenters, à l'attention des collectivités locales.** Guide sur le Cloud Computing et les Datacenters à l'attention des collectivités locales. *www.entreprises.gouv.fr.* Citation : 30 11 2022

120. **D.N.D Agency : PLAN D'ASSURANCE SÉCURITÉ.** PLAN D'ASSURANCE SÉCURITÉ. *dndagency.fr.* Citation : 30 11 2022

121. **JDN : Sécurité des données dans le Cloud : que font les hébergeurs ?** Sécurité des données dans le Cloud : que font les hébergeurs ? *www.journaldunet.com.* Citation : 30 11 2022

122. **Isolation dans le cloud public Azure.** Isolation dans le cloud public Azure. *learn.microsoft.com.* Citation : 30 11 2022

123. **JDN : 4 risques majeurs liés au passage au cloud, et comment les gérer.** 4 risques majeurs liés au passage au cloud et comment les gérer. *www.journaldunet.com.* Citation : 30 11 2022

124. **EUROPEAN DATA PROTECTION SUPERVISOR, Transferts internationaux.** EUROPEAN DATA PROTECTION SUPERVISOR : Transferts internationaux. *edps.europa.eu.* Citation : 30 11 2022

125. **VERITAS : Sauvegarde et récupération des données, Le guide essentiel pour les entreprises.** Sauvegarde et récupération des données : Le guide essentiel pour les entreprises. *Veritas.* Citation : 30 11 2022

126. **APFI : La sécurité des données dans le cloud.** La sécurité des données dans le cloud. *www.capfi.fr.* Citation : 30 11 2022

Principaux acronymes

ACS	Azure Container Service (Microsoft)
AIPD	Analyse d'Impact sur la Protection des Données
Amazon EC2	Service d'orchestration de conteneurs Docker
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application programming interface
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
AWS	Amazon Web Service
BATX	Baidu, Alibaba, Tencent, Xiaomi
BSI	Bundesamt für Sicherheit in der Informationstechnik (L'Office fédéral de la sécurité des technologies de l'information, Allemagne)
BYOD	Bring your Own Divice (apportez son propre matériel)
CaaS	Containers as a Service
CASB	Cloud Access Security Broker : point d'application de la stratégie de sécurité (sur site ou dans le cloud) qui intervient entre les utilisateurs et les fournisseurs de services cloud. Il combine et associe les stratégies de sécurité d'entreprise lorsque des utilisateurs accèdent à des ressources dans le cloud.
CCT	Clauses Contractuelles Types
CD	Compact Disc
CEPD	Le Contrôleur européen de la protection des données
CEPD	Contrôleur européen de la protection des données
CIA	Central Intelligence Agency
CIA	Central Intelligence Agency
Cigref	Club informatique des grandes entreprises françaises
CIL	Correspondant Informatique & Libertés
CJUE	Cour de justice de l'Union Européenne
Cloud computing	Informatique en nuage
CNIL	Commission nationale de l'informatique et des libertés
CNRS	Centre National de la Recherche Scientifique
COREPER	Comité des représentants permanents, organisme de l'UE
COREPER	Le Comité des représentants permanents, organisme de l'UE. Il prépare les travaux du Conseil de l'UE
CPU	Central Proccessing Unit (processeur ou microprocesseur)
CRA	Cyber resilience Act
CRM	Customer Relationship Management
DaaS	Desktop as a Service
DB	Base des Données
DCP	Données à caractère personnel
DDoS	Distributed Denial of Service attack (Attaque par Déni de Service)
DevOps	"développement" et "opérations"
DGA	Data Governance Act

DGA	Data Governance Act
DMA	Digital Market Act
DMA	Digital Market Act
DNS	Domain Name System
DPO	Délégué à la Protection des Données
DSA	Digital Service Act
DSA	Digital Service Act
DSCP	Données de Santé à Caractère Personnel
DSM	Digital single Market
DSM	La Stratégie Digital single Market
DVD	Digital Versatile Disc
EHPAD	Établissement d'hébergement pour personnes âgées dépendantes
ENISA	Agence de l'Union européenne pour la cybersécurité
ENISA	Agence de l'Union européenne pour la cybersécurité
ERP	progiciel de gestion intégré
ESN	Entreprise de Services du Numérique est une société de services experte dans le domaine des nouvelles technologies et de l'informatique
ETC	Et cetera
EUCS	European Union Cloud Services Scheme
EUCS	European Union Cloud Services Scheme
FaaS	Function-as-a-Service
FBI	Federal Bureau of Investigation
FBI	Federal Bureau of Investigation
FinOps	Contraction des termes de finance et d'opérations (monotoring et optimisation des coûts Cloud)
FSN	Fournisseurs de Services Numériques
FSN	Fournisseurs de service numérique, définition dans la directive NIS (22)
GAFAM	Google, Apple, Facebook (Meta), Amazon, Microsoft
GAFAM	Google, Apple, Facebook, Amazon et Microsoft
GCP	Google Cloud Platform
GKE	Google Kubernetes Engine
HDS	Hébergeur de Données de Santé
HDS	Hébergement de données de santé
HIPAA	Health insurance Portability and Accountability Act
HIPAA (loi)	Health Insurance Portability and Accountability Act
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HVD	Holographic Versatile Disks (même famille que DVD)
IA	Intelligence Artificielle
Iaas	5.2 Infrastructure en tant que service
IBM	International Business Machines
INSEE	Institut national de la statistique et des études économiques
IOS (iPhone OS)	système d'exploitation mobile
IP	Internet Protocol

ISO	International Organization for Standardization : organisation internationale de normalisation édictant des normes dont le respect est une garantie de qualité, de sûreté et de fiabilité.
IT	Informatique
JPG ou JPEG	Joint Photographic Experts Group
Le Cigref	Association/réseau de grandes entreprises et administrations publiques françaises dans le numérique
Logs	Journal
Loi I&L	Loi Informatique et Liberté
LPM	Loi de Programme militaire
MFA	Multi Factor Authentication : méthode d'authentification forte par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté plusieurs preuves d'identité distinctes à un mécanisme d'authentification.
ML	Machine learinin (technologie d'intelligence artificielle)
MySQL	My Structured Query Language (système de gestion de base de données relationnelle open source)
NAS	Network Attached Storage
NIS	Network and Information Security (directive européenne)
NIST	National Institute For Standard and Technology
NSA	National Security Agency
NSA	National Security Agency
OCR	Office for Civil Rights
OIV	Opérateurs d'importance vitale
OS	Operatinf system, système d'Exploitation
OSE	Opérateurs de Services Essentiels
OSE	Opérateurs de services essentiels, définition dans la directive NIS (22)
OVH	On Vous Héberge
Paas	Plateforme as a service
PASSI	Prestataires d'Audit de la Sécurité des Systèmes d'Information
PCA	Plan de Continuité d'Activité
PCD	Protein-coated disks
PCI-DSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PDS	Plateforme des Données de Santé
PII	Les informations personnelles identifiables
PME	Petites Moyennes Entreprises
PSSI	Politique de Sécurité des Réseaux et Systèmes d'Information
R&D	Recherche et Développement
RAID	Redundant Array of Independent Disks
RAID/NAS	Redundant Array of Independent Disks/Network Attached Storage
RAM	Random Access Memory
RGPD	Règlement Général de Protection des Données
RSA	Ron Rivest, Adi Shamir et Leonard Adleman du MIT (un système cryptographique pour le chiffrement à clé publique)

SaaS	Software as a Service
SAIV	Sécurité des Activités d'Importance Vitale
SAP	Systemanalyse Programmentwicklung (développement de programmes d'analyse de système)
SDA	Secret des affaires
SI	Système d'Information
SIIV	Systèmes d'Information d'Importance Vitale
SOX	Sarbannes-Oxley
STaas	Le Stockage en tant que Service
Système DNS	Système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines
TCO	Total Cost of Ownership (vision globale de l'impact financier d'un produit/service)
TPE	Très Petites Entreprises
UE	Union europèenne
UE	Union européenne
UK	Royaume-Uni
USB	Universal Serial Bus
VM	Virtual Machine, Machine Virutelle
VOICE	Association fédérale allemande des utilisateurs de l'informatique.
VoIP	Téléphonie IP
VPN	Virtual Private Network (Réseau privé virtuel)
WWW	World Wide Web
XHTML	Extensible HyperText Markup Language
XML/RDF	Extensible Markup Language (langage de balisage extensible)
ZRR	zones à régimes restrictifs

Principales définitions

Active Directory	L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, macOS ou encore Linux. Il permet également l'attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés (en), les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.
Bien support	Composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle
CGU (Conditions Générales d'Utilisation)	Définissent et encadrent les modalités d'accès et de navigation sur le site Internet, et déterminent les droits et les obligations respectifs de l'utilisateur et de l'éditeur dans le cadre de l'utilisation du site. Les CGU ne sont pas obligatoires.
Chiffrement et tokenisation	Les deux technologies sont différentes. Le résultat du chiffrement est un bloc de texte chiffré. Les données sont protégées à l'aide d'un algorithme mathématique qui brouille les données et qui ne peuvent être récupérées qu'à l'aide d'un processus de déchiffrement avec une clé adéquate. La tokenisation quant à elle remplace les données par des valeurs aléatoires qui sont stockées avec les données originales dans une base de données sécurisée. Cette technologie est souvent utilisée lorsqu'il y a un fort besoin de respecter le format des données (Ex. remplacement des numéros de carte de crédit dans un système exigeant le même format), le chiffrement dispose aussi de cette possibilité mais peut ne pas être aussi sûr en raison des compromis.
Cloud souverain	L'Union européenne définit le cloud souverain comme une infrastructure et des services cloud opérés par les acteurs privés des pays membres de l'Union européenne, dont les infrastructures sont situées dans l'espace européen, et assurant la protection des données.
CSA (Cloud Security Alliance)	Organisation à but non lucratif ayant pour mission de « promouvoir l'utilisation de bonnes pratiques afin d'assurer la sécurité au sein des environnements de cloud computing et de fournir des informations sur les utilisations du cloud computing, dans le but de contribuer à la sécurité de l'informatique sous toutes ses formes

CSL	Cette loi chinoise est entrée en vigueur en Juin 2017, son objectif est d'uniformiser le règlement du point de vue de la protection des données et de la cybersécurité en Chine. Les obligations sont destinées aux opérateurs de réseau et d'infrastructures d'information critiques chinois
Directive	Acte juridique européen pris par le Conseil de l'Union européenne avec le Parlement ou seul dans certains cas. Elle lie les États destinataires de la directive quant à l'objectif à atteindre, mais leur laisse le choix des moyens et de la forme pour atteindre cet objectif dans les délais qu'il a fixé au préalable.
EDGE computing	Une méthode d'optimisation employée dans le cloud computing qui consiste à traiter les données à la périphérie du réseau, près de la source des données.
Événement redouté (ER)	Un événement redouté est associé à une valeur métier. Il porte atteinte à un critère, ou à un besoin de sécurité, de la valeur métier (ex : indisponibilité d'un service, divulgation de données classifiées, modification d'une base de données ou modification illégitime du seuil de température haute d'un processus industriel). Les ER à exploiter sont ceux des scénarios stratégiques et se rapportent à l'impact d'une attaque sur une valeur métier. Chaque ER est évalué selon le niveau de gravité des conséquences.
Impact	Conséquence d'un événement redouté estimé en gravité. Il peut être interne, externe, direct ou indirect (ex : impact sur la mission, impact humain, impact financier, impact juridique, impact sur l'image de marque…).
Interopérabilité	La capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits, applications ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions.
L'altruisme en matière de données (data altruism)	L'altruisme en matière de données, ou data altruism en anglais, est une notion en gouvernance des données. Il consiste à inciter les parties prenantes (entreprises, particuliers, etc.) à partager les données qu'elles estiment utiles pour l'intérêt général.
Le chiffrement basé sur un proxy	Le proxy placé dans une zone de confiance entre l'utilisateur et le Cloud, gère le chiffrement avant le transfert des données.
Missions EBIOS RM	Fonction, finalité, raison d'être de l'objet de l'étude
ML	Le Machine Learning est une technologie d'intelligence artificielle permettant aux machines d'apprendre sans avoir été préalablement programmées spécifiquement à cet effet. Il permet de réaliser des prédictions à partir du Big Data.

module de sécurité matériel (HSM)	Un module de sécurité matériel (HSM) est un processeur de chiffrement dédié, spécialement conçu pour protéger les clés cryptographiques tout au long de leur cycle de vie. Les modules de sécurité matériels sont les bases de confiance qui protègent l'infrastructure cryptographique de certaines des organisations les mieux sécurisées au monde, en gérant, traitant et conservant de manière sécurisée les clés cryptographiques à l'intérieur d'un appareil renforcé inviolable.
PME	Définition INSEE : Les petites et moyennes entreprises (PME) sont celles qui, d'une part, occupent moins de 250 personnes, d'autre part, ont un chiffre d'affaires annuel n'excédant pas 50 millions d'euros ou un total de bilan n'excédant pas 43 millions d'euros. Elles incluent la catégorie des microentreprises. (MIC) qui occupent moins de 10 personnes et ont un chiffre d'affaires annuel ou un total de bilan n'excédant pas 2 millions d'euros.
Protocole TLS	TLS, ou Transport Layer Security, est un protocole en deux couches, une nouvelle version de SSL qui reprend ses caractéristiques principales tout en améliorant certaines fonctions pour mieux sécuriser les échanges de données. Les deux couches désignent deux clés qui agissent l'une en parallèle de l'autre lorsqu'un utilisateur souhaite par exemple rejoindre une navigation sécurisée.
Règlement	Acte juridique européen, de portée générale dont toutes les dispositions sont obligatoires: les États membres sont tenus de les appliquer tel qu'elles sont définies par le règlement. Celui-ci est donc directement applicable dans l'ordre juridique des États membres. Il s'impose à tous les sujets de droit : particuliers, États, institutions.
Risque	Possibilité que des menaces exploitent des vulnérabilités d'un actif ou d'un groupe d'actifs et nuisent / perturbent les missions de l'objet de l'étude
RPO	RPO ou Recovery Point Objective, désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne. Le fait de quantifier le RPO définit en fait les objectifs de sauvegarde, ce qui demande de connaître la volumétrie et les fenêtres de sauvegarde.
RTO	Le RTO ou Recovery Time Objective, peut se traduire par la durée maximale d'interruption admissible d'une ressources informatiques. Il s'agit du temps maximal acceptable pendant lequel une brique IT (serveur, réseau, ordinateur, application) peut ne pas être fonctionnelle suite à une interruption majeure de service. Cette durée est définie à l'avance, et ce en fonction des besoins de production d'une entreprise vis-à-vis de la ressource informatique.

Services d'intermédiation de la donnée	Les services d'intermédiation de la donnée sont un modèle commercial visé par le Data Governance Act qui a pour objectif de permettre aux entreprises et particuliers de partager des données. Ces services peuvent prendre par exemple la forme de plateformes numériques permettant le libre partage ou contrôle de leurs données par les entreprises et particuliers ainsi que d'exercer leurs droits pour ces derniers. https://www.cnil.fr/fr/definition/services-dintermediation-de-la-donnee
SFTP	SFTP signifie SSH File Transfer Protocol ou Secure File Transfer Protocol. Comme l'indique la première définition, SFTP fait partie de SSH ou Secure Shell. Il s'agit d'un remplaçant sûr pour l'établissement d'une session de terminal sur des machines UNIX. SFTP est le composant de ce protocole SSH qui assure le transfert de fichiers.
SLA (Service Level Agreement)	Engagement de service en français, il s'agit d'une clause contractuelle qui définit les objectifs précis et le niveau de service qu'est en droit d'attendre un client de la part du prestataire signataire.
Source de risque (SR)	Entité ou personne susceptible de porter atteinte aux missions de l'organisation ou à des intérêts supérieurs (sectoriel, étatiques, etc…).
TPE	Définition INSEE : Les très petites entreprises emploient moins de 10 salariés, n'appartiennent pas à un groupe (sauf s'il s'agit d'un groupe de type microentreprise au sens de la LME), ont un chiffre d'affaires ou un total de bilan inférieur à 2 millions d'euros
Valeurs métiers	Composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé

Annexes

Annexe 1

Entretien réalisé le 19 octobre auprès de Valery Rieß-Marchive, rédacteur-en-chef de LeMagIT

Est-ce que la réglementation actuelle, associée au cloud de confiance, nous protège suffisamment des lois extraterritoriales ?

Non. Il y a une très bonne analyse, le « Memo Cloud Act », du Centre National de Cybersécurité des Pays-Bas publiée le 16 août de cette année. (Cf. Cloud Act Memo | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)). Ce n'est pas fondamentalement nouveau. Cela vient conforter des analyses antérieures. L'analyse est intéressante à lire et les conclusions sont assez énormes. Grosso modo, le Cloud Act est susceptible de toucher la donnée d'entreprises européennes via des sous-contractants, des fournisseurs de matériels et de logiciels jusqu'à des fournisseurs Cloud de manière directe et indirecte. Il s'agit de la dernière « Closing remarks » de la page 15. Le Cloud Act va tellement loin que c'est extrêmement dur de s'en protéger de façon hermétique à compter du moment où soit, soi-même, soit un petit fournisseur utilise des techno américaines et/ou est susceptible d'engager des ressortissants américains. On est dans des scénarios qui sont quand même relativement extrêmes. Il n'y a pas de doute là-dessous, ça va très loin. Mais l'objectif de cette analyse est vraiment d'aller jusqu'au bout du truc et essayer de voir ce qui peut se passer. C'est quasiment une analyse de risque.

On en revient toujours aux mêmes questions fondamentales, c'est-à-dire la disponibilité, l'intégrité et la sécurité des données. A partir de là, si on regarde la disponibilité, l'intégrité et la sécurité, objectivement, on peut se dire que le Cloud a pas mal d'avantages. Effectivement, les taux de disponibilité sont élevés, l'intégrité des données est quand même plutôt pas mal protégée et leur sécurité, on peut commencer à faire confiance au fournisseur Cloud pour avoir des niveaux de sécurité au moins sur les couches basses de l'infrastructure qui sont généralement plus élevées que ce que la moindre entreprise fera elle-même dans son Data Center. Mais il faut éviter de se faire des illusions. Ce n'est pas parce qu'on est dans le cloud qu'on n'a pas de responsabilités sur ses données. La modélisation du partage de responsabilités sur la sécurité des données, sur le contrôle de l'accès aux données en fonction du type de service a été très bien réalisée par Microsoft il y a de nombreuses années. Mais grosso modo, si je recours au service d'infrastructure en mode service d'IaaS d'Azure ou d'AWS et que je fais tourner mes applications sur des machines virtuelles, je suis forcément responsable mécaniquement d'une grosse partie de l'actif de sécurité autour de ces machines virtuelles, donc autour de mes applications et données. Puis après, j'ai recours à simplement des services SaaS, l'essentiel de la sécurité est de la responsabilité de l'opérateur des services SaaS. Donc ça ne veut pas dire pour autant que moi je n'ai pas de responsabilité du tout. Mes utilisateurs vont rester responsables de l'accès aux données, de leur partage, du respect de leur confidentialité, etc. Ce n'est pas parce que je suis sur le Cloud et même sur le type de cloud le plus managé possible que je n'ai pas de responsabilité dessus. Ça c'est une première chose. La deuxième chose, si on commence à se poser la question de la capacité d'accès légal ou technique par des tiers à mes données qui sont dans le cloud :

1 - J'ai une responsabilité légale vis-à-vis du RGPD

2- Mais aussi une responsabilité vis-à-vis de moi-même, en tant qu'entreprise, de m'assurer que mes données ne vont pas tomber dans de mauvaises mains.

Déjà ça veut dire 2 choses cette responsabilité. Ça veut dire que ce n'est pas parce que tu es dans le Cloud que tu ne vas pas faire de backup. Parce que si jamais il y a une défaillance, si jamais il y a une rupture d'accès ou une rupture de disponibilité, mais que grosso modo, je dois maintenir la disponibilité de mes données et que rien qu'une simple destruction ou une rupture d'accès aux données, j'en reste responsable au regard du RGPD. Les entreprises qui ont été affectées par l'incendie chez OVH devaient faire une déclaration à la CNIL dans le cas où elles auraient hébergé des données personnelles chez OVH dans des serveurs.

Donc un, maintenir l'accès à la donnée, ça veut dire avoir une sauvegarde, ça veut dire avoir des capacités de reprise si jamais je perds l'accès à mes données pour une raison X ou Y. Donc après, ce que montre l'analyse néerlandaise, c'est que je n'ai pas fondamentalement de bouclier ni légal, ni organisationnel contre le Cloud Act si jamais je décide de passer complètement dans le Cloud. Ça veut dire quoi derrière ? Ça veut dire que moi, si j'estime dans mon analyse de risque dans le Cloud Act est une menace ou qu'une éventuelle érosion de la qualité des relations diplomatiques entre l'Europe et les

Etats-Unis, si je crains un espionnage de la part de compétiteurs proches des États-Unis etc., je n'ai pas d'autre choix que de mettre en place des mesures techniques de protection. Cela veut dire mettre en place du chiffrement.
Le chiffrement c'est quand-même quelque chose qui marche suffisamment bien pour que les « méchants », lors des attaques avec ransomware, arrivent à se faire payer quand-même dans certains cas. Donc quelque part le chiffrement ça fonctionne. Si on chiffre suffisamment bien ses données avec des algorithmes suffisamment robustes, avec des clés suffisamment robustes, je pense qu'on atténue déjà significativement le risque d'accès à ses données par des tiers. Mais c'est une question de mise en œuvre, c'est-à-dire que si je vais chiffrer mes données sur Azure ou AWS ou sur n'importe qui d'autre, mais que je laisse n'importe qui d'autre, ce tiers, gérer mes clés de chiffrement, et voire, décider de mes algorithmes de chiffrement, je deviens dépendant de lui quelque part. C'est le même risque qui consiste à dire : j'emploie une société de gardiennage et je fais confiance à cette société pour bien faire son job, faire le bon recrutement pour pouvoir être en confiance avec la société de gardiennage à laquelle je vais finalement confier les clés de mes locaux et une partie des clés de mon activité, de mon entreprise et ma valeur. Donc on élimine un risque mais pas totalement. J'estime que j'ai des données qui sont particulièrement sensibles mais je vais quand- même aller dans le Cloud. Dans ce cas-là, je ne vois pas d'autre solution que d'employer du chiffrement qui sera en local, en propre dans mon infrastructure dont je vais maitriser les clés. En définitive, les données seront stockées, elles vont transiter jusqu'à mon environnement, jusqu'à mon système d'information là où elles vont être traitées, utilisées, exploitées par les employés. Jusque-là, elles vont être chiffres ici. Et puis, soit elles seront déchiffrées sur le poste de travail de mon employé, soit elles seront déchiffrées par une passerelle dédiée qui sera dans mon système d'informations, ce qui permettra l'exploitation de mes données en local, dans mon infrastructure, dans mon environnement. Et dans ce cas-là, le tiers auquel je confie ma donnée, je ne lui confie jamais ma donnée entière. Je lui confie, pour le stockage, que de la donnée chiffrée et je reste maître de mes clés de chiffrement et mes algorithmes. Et là on arrive à une réduction assez significative du niveau de risque.

Par rapport à notre cible, c'est-à-dire les TPE/PME, et de par votre connaissance du marché, est-ce que vous pensez que globalement, elles ont conscience de la valeur de leurs données et des risques auxquels elles sont exposées ?
Absolument pas ! Si elles en avaient conscience, on n'aurait tout simplement pas autant de victimes d'attaques par ransomware qui se retrouvent mises à genoux pendant des semaines. Je ne dis pas qu'avec la meilleure des protections, des préparations au monde, il n'y a pas d'impact à une cyberattaque avec ransomware. Mais l'ampleur des dégâts que l'on observe chez pas mal d'entreprises, l'ampleur du chantier pour remonter les systèmes d'informations, le fait qu'on ait si peu d'attaques qui soit détectées dans les phases préalables au déclenchement du ransomware, dans les phases préliminaires de l'attaque, montre bien qu'on a encore un faible niveau de conscience du risque qui pèse sur les données en général. Le ransomware n'en est qu'un exemple, mais il illustre en fait un manque de conscience sur l'importance de la donnée et de sa valeur. Parce que si tout le monde avait super conscience de la valeur de la donnée, on aurait des capacités de détection beaucoup plus répandues permettant de stopper une attaque en cours avant le déclenchement du ransomware, avant que le pire n'arrive. On a quelques cas dans lesquels ça se produit. On a vu récemment avec la ville de Caen, avec Lactalis, mais ça reste relativement rare. Cela révèle un niveau de conscience et de préparation qui est relativement bas.
Je reviens juste à votre première question. Il y a un acronyme. Quand je parlais de passerelle pour chiffrer des données stockées etc., il y a un type d'outil qui s'est développé au cours de la dernière décennie pour faciliter les choses. C'est ce qu'on appelle les CASB, le Cloud Access Security Broker. On a un témoignage du déploiement d'un CASB chez AXA IM. J'avais d'ailleurs fait un papier en 2018 sur le sujet et sur comment ces trucs peuvent aider (Cloud Act & Patriot Act : comment les CASB peuvent aider (lemagit.fr)). Encore une fois, comme on se disait, en matière de sécurité, il n'y a pas de solution absolue et comme partout, on essaie de l'atténuer, de le réduire mais en revanche ça peut aider.

Justement vous disiez que les TPE/PME ne sont pas conscientes de tous ces risques. Quelles pourraient être les solutions à leur apporter ? Hormis la sensibilisation par exemple, voyez-vous d'autres critères ou d'autres aides qui peuvent leur être apportés justement pour accélérer cette prise de conscience ?
Franchement je ne vois pas. Je sais qu'il y a des Chambres de Commerces et de l'Industries (CCI) qui essayent justement de sensibiliser en région parce que certaines CCI ont identifié le problème du manque de conscience il y a longtemps. Je me souviens avoir discuté avec la CCI de Touraine en 2010 (CCI de Touraine : « les entreprises en région sont très en retard en matière de sécurité » (lemagit.fr)). Le Président de la CCI à l'époque en était déjà parfaitement conscient et cherchait vraiment à les responsabiliser.

Donc le problème a été identifié depuis bien longtemps.

Alors certains, clairement, l'avaient déjà identifié en 2010 et en avait déjà conscience et cherchaient à mener des actions de sensibilisation auprès du tissu économique local. Toutes les opérations de sensibilisation ne sont pas faciles, ça prend du temps. Et puis le patron d'une TPE/PME moyenne n'a pas le temps de venir. Il va lire de la presse spécialisée sur son secteur d'activité. Il n'a pas forcément de culture de l'IT parce que pour lui, l'IT est un outil de travail et puis c'est tout ! Ce n'est pas quelque chose qu'il pense devoir comprendre, ni maîtriser, etc. Et si vous voulez le faire venir sur un colloque sur la cybersécurité ou un truc comme ça, je ne sais pas si c'est toujours le cas aujourd'hui mais il y a encore quelques années, les réponses étaient : « Je n'ai pas le temps, j'ai d'autres choses à faire, j'ai une entreprise à faire tourner ». Même parmi les acteurs économiques les plus proches de moi, j'en vois peu qui viennent vers moi et qui me disent : « Tiens Valery, prends une heure avec moi pour m'expliquer quels sont les dangers et à quoi je dois faire attention ». Même si on en parle à table, en famille ou comme ça, ça reste relativement loin de leurs sujets de préoccupation. Ils ont des préoccupations beaucoup plus immédiates. Réussir à faire rentrer ça dans leur logiciel, c'est difficile.

Ce qui aide, je vois bien par exemple, les transports Fatton (Ransomware : comment les transports Fatton se remettent d'une cyberattaque avec Conti (lemagit.fr)). La Direction des transports Fatton, même s'ils ont été victime d'une cyberattaque, a déjà fait des efforts pour renforcer leur posture de cybersécurité avant car ils avaient été sensibilisés, à l'occasion d'un retour d'expérience, par un témoignage d'un pair qui avait été victime. Le témoignage de pair, c'est quelque chose qui marche très bien, c'est quelque chose qui est entendu. Et c'est là que, par exemple, organiser des sessions de sensibilisation sectorielles, en région, localement par les CCI, ça peut être un levier. Il s'agit de dire : « On a eu une victime dans tel secteur d'activité. On est au courant à la CCI. On va attendre un petit peu et puis on va faire un colloque avec cette victime qui va venir nous parler de ce qui s'est passé. On va inviter seulement des entreprises du même secteur d'activité ». Parce que là, ils vont se sentir à parler entre pairs etc. …, ça va mieux passer. Même si la menace n'est absolument pas sectorielle et que fondamentalement elle concerne absolument toutes les entreprises de n'importe quelle taille, le message a plus de facilité à passer. On a plus de facilité, j'imagine en tout cas, à attirer l'attention quand on joue justement sur cette corde sensible de l'entre pairs. Dans le même sens qu'on ne peut pas forcer une entreprise à améliorer la sécurité physique de ses installations, elle se rend compte à un moment, par exemple, que l'assurance peut aider. Quelque part, si on a amélioré la sécurité physique des bâtiments, c'est bien aussi parce qu'à un moment les assureurs ont mis des exigences sur le type de sécurité physique qu'on mettait en place. On va accepter d'assurer le risque vandalisme, incendie volontaire, etc … Quand les assureurs auront vraiment cherché progressivement à toucher le tissu des TPE/PME en termes de cybersécurité, ils ne vont pas avoir d'autre choix que de développer leur niveau d'exigences minimums. Et quelque part, ça va aider à la prise de conscience des entreprises que l'information, la donnée, c'est un actif. C'est un actif immatériel de l'entreprise. Ceux qui travaillent avec de la propriété intellectuelle ont déjà conscience de ce que c'est qu'un actif immatériel. D'autres n'ont pas forcément conscience du fait que la donnée est déjà un actif immatériel en soi et qu'il y a déjà une valeur. Le fait est que beaucoup d'entreprises ont de la donnée mais ce n'est pas de la donnée à partir de laquelle elles génèrent véritablement de la valeur. C'est de la donnée qui ne prend sa valeur qu'à partir du moment où elle est perdue ou on y a plus accès, ou on ne peut plus l'utiliser. Donc en fait, elle n'a pas de valeur positive en tant que tel. En revanche, elle pénalise fortement l'entreprise et son activité quand elle n'est plus accessible.

Toujours en lien avec votre connaissance du marché français, à part les Cloudeurs français et américains, est-ce que vous voyez l'émergence d'autres fournisseurs de nationalité moins connue ?

Les Chinois pour commencer, avec Alibaba. On a des Suisses avec Proton ou Infomaniak. Infomaniak et Proton misent sur leur identité suisse pour se poser en champions de la confidentialité et de la protection des données. Infomaniak n'a pas aujourd'hui la capacité de fondamentalement aller affronter un AWS ou un Microsoft ne serait-ce qu'en termes d'éventails fonctionnels proposés. Mais pour les besoins essentiels d'une PME ou d'une TPE, que ce soit de la messagerie, de la bureautique en ligne, que ce soit de l'échange de données, Infomaniak commence à avoir des offres franchement raisonnables. Infomaniak est capable de faire de l'hébergement, de l'IaaS, du serveur privé virtuel, de la messagerie. Je ne suis pas certain qu'on soit aujourd'hui au niveau de l'étendue d'offres qu'on va trouver chez un AWS, un Azure mais ça avance déjà pas mal. Et sur l'aspect messagerie, bureautique, etc …, Infomaniak vient de lancer une offre appelée kSuite qui intègre le stockage en ligne, avec un drive, le partage chiffré d'informations, le Mail, le partage de fichier, le chat, … Bref, ça se développe. Et puis Proton, qui est né à partir d'une niche sur du mail confidentiel, cherche à se développer. Aujourd'hui le premier auquel je penserai, ce serait Infomaniak. Il ne faut pas oublier non plus l'allemand, IONOS, qui fait quand-même

pas mal de choses. Ce n’est pas négligeable. Il y a de l’offre Clouds. Il y a plus d’offres qu’on ne l’imagine. Sauf que Google et Microsoft ont une grosse force avec ce qu’ils ont comme bureautique en ligne. Et ça reste quand même des outils qui sont au cœur de l'activité économique de la plupart des entreprises. Donc entre la messagerie, Teams, …, ce sont des rouleaux compresseurs. Mais ça ne veut pas dire qu’il n’y a pas d'alternative. Et en l'occurrence à l'échelle européenne, il y a des offreurs qui n’ont pas baissé les bras. Enfin pour moi, que ce soit un OVH, un IONOS ou un Infomaniak, il y a des gens qui n’ont pas baissé les bras. Il y a des solutions alternatives mais pas pour tout, pas aussi intégré, aussi évolué, avançant aussi vite que l’éventail de produits dans les offres Cloud de Microsoft ou Amazon. C'est juste énorme. Mais ça ne veut pas dire qu'il n’y a pas de moyen de faire assemblage d’offres qui viennent d'ailleurs. Je ne dis pas que c’est trivial mais ce n’est pas impossible.

Un DSI ou un RSSI ne va pas forcément chercher à faire cet assemblage. Il regardera probablement le Magic Quadrant de Gartner pour faire le choix de la solution.

Les TPE/PME n'ont pas forcément de RSSI. Elles ne vont pas gérer nécessairement leur informatique elles-mêmes. Elles vont passer par des ESN, ce qu'on appelle des infogéreurs. C'est d'ailleurs la raison pour laquelle l'ANSSI se préoccupe autant de la sécurité des ESN. C'est pour ça aussi que les ESN sont prises en compte dans la version 2 de la Directive NIS. C'est parce qu'elles sont le sang et le cœur battant de l'informatique de beaucoup de TPE/PME et donc d'une grosse partie du tissu économique. On a eu une illustration qui a donné lieu à un échange téléphonique, que je qualifierai de viril sur une ESN qui a subi une attaque par ransomware.

Donc au niveau contractuel, il faut muscler le contrat.

C'est difficile car il y a des interprétations parce qu'il y a une relation contractuelle. On va y faire attention mais on ne peut pas tout faire peser sur l'infogéreur. Le RGPD le souligne très bien, ce n'est pas parce qu'on confie ses données à un infogéreur qu'on est exempt de responsabilités sur tout ce qui pourrait arriver à ses données.

Annexe 2

Entretien réalisé le 2 novembre 2022 auprès de Arnaud Muller, Co-Founder & GM @Cleyrop, 1er DataHub Souverain Européen sécurisé

Dans ce document, nous nous adressons aux TPE/PME qui décident de migrer leurs données dans le Cloud à se poser les bonnes questions en amont de leur décision. Nous traitons toute la partie d'analyse de risque avant la migration et nous sommes plus concentrés sur la partie donnée et réglementation. Ces 2 thématiques semblent les moins maitrisées par les TPE/PME. Qu'en pensez-vous ?

Pour moi, il y a une nécessité pour les grandes entreprises/organisations comme pour les plus petites d'aborder le choix du Cloud provider sous l'angle des risques et de la compliance. Et donc ce qui est important pour une entreprise, qui aujourd'hui ne serait pas équipée (ce qui est le cas de beaucoup de PME qui font le choix de migrer et de démarrer de nouveaux projets dans le Cloud), c'est de comprendre qu'il y a une réglementation qui est en train de monter notamment autour des nouvelles lois (Digital Governance Act, Data Act…).

Je pense que ce qui est très important, c'est de pouvoir associer la sécurité et la qualité dans le choix du Cloud et notamment pour des entreprises qui manipulent des données sensibles ou qui sont dans un secteur d'activité qui serait particulièrement exposé comme les domaines de l'énergie, de la santé, des services financiers ou qui travaillent avec des collectivités territoriales et avec des acteurs du public (le secteur public étant le plus encouragé et voir le plus contraint à adopter des solutions qui vont justement s'appuyer sur les certifications SecNumCloud). Ces entreprises doivent, à mon sens, intégrer ce risque mais aussi cette opportunité de se différencier par une offre et par une infrastructure qui sera portée par un acteur souverain. Donc il faut l'aborder autant par les risques que par l'opportunité. Aujourd'hui, je pense que le marché sur les TPE principalement doit être vu sous l'angle du secteur d'activité. Il y a peut-être encore des secteurs d'activité comme la grande distribution, par exemple, qui est moins concerné par ces contraintes. En effet, il y aura moins de manipulation de données sensibles. C'est peut-être moins prioritaire pour eux.

Maintenant il faut savoir que le risque réglementaire évolue. Cela amène des éléments de différenciation à des acteurs de PME/TPE et sur lesquels ils peuvent communiquer justement sur le fait qu'il y a une approche peut-être plus responsable et éthique du traitement des données.

Dernier point là-dessus, c'est qu'on a un enjeu aussi quand on a un risque à ne pas pouvoir revenir sur ses choix et sur la liberté de ses choix. Cette liberté est essentielle pour une entreprise qui ne veut pas créer une dépendance énorme avec des frais de migration. C'est une question de sensibilité et de conscience. Ce qui ne nous coûte pas à l'entrée va nous coûter à la sortie. Et que les fournisseurs de Cloud français n'ont pas mis en place le péage à la sortie. C'est un élément aussi lié au fait que certains patrons entendent quelle est la liberté.

Si aujourd'hui vous devez dire un mot sur la maturité des TPE/PME par rapport à cette migration et tous les risques qu'ils encourent en l'effectuant, que diriez-vous ?

Pour des TPE/PME et des start-ups, qu'on peut inclure dans cette liste, les risques sont principalement des risques financiers aujourd'hui. Puisqu'on a quand même une économie qui est plongée dans un climat d'incertitude totale. On imagine bien que le politique et le régulateur ne vont pas venir taper sur les acteurs les plus fragiles de la chaîne de valeur. Donc, de toute façon, les plus concernés sur le risque juridique et réglementaire seront des organisations, on va dire de rang 1, qui seront des grandes organisations avec une dimension très visible. On peut imaginer de toute façon que le risque réglementaire n'interviendra et ne se matérialisera que dans quelques années. Puisque l'Etat et l'Union Européenne laisseront du temps à ces sociétés pour se mettre en conformité. En effet, ce sont les acteurs les plus fragiles, ils auront besoin de plus de temps pour s'adapter à la nouvelle réglementation et ce ne seront pas les premiers cas d'école qui seront révélés.Sur la partie financière, c'est complétement différent. C'est-à-dire, aujourd'hui, une entreprise TPE/PME qui fait le

choix d'un acteur américain va ensuite se retrouver piégée à ne pas savoir finalement comment revoir son choix et être confrontée à une réalité qui est l'augmentation des prix et un manque de transparence.
On voit qu'il y a un coût qui augmente, qui a déjà augmenté et qui augmente de manière très rapide. Et donc le risque, il est surtout la maîtrise des coûts, aujourd'hui c'est quelque chose de fondamentale.

On a, par exemple, un acteur comme OVH qui explique que les coûts vont augmenter avec telle et telle raison et une approche très transparente finalement. On aura une approche beaucoup plus opaque à la fois des contrats et de la facturation de la plupart des autres acteurs. Notamment, sur la partie de tarification. Car ce qui peut représenter un gros risque, c'est qu'on va dépendre d'un acteur tiers qui peut revoir sa politique de prix avec un rapport de force qui est complètement déséquilibré.
En fait, il faudrait certainement y aller graduellement. En d'autres termes, essayer de conserver des infrastructures On-Premise et donc de pratiquer ce qu'on appelle le déploiement hybride du cloud.
Aussi, il faudrait privilégier un acteur local et si ce n'est pas possible de sécuriser finalement les applications qui vont être plus sensibles dans des Clouds très sécurisés type SecNumCloud. Et à minima de cartographier ses applications et de ne pas tout mettre dans un Cloud américain notamment sur tout ce qui est essentiel.

Est-ce que la réglementation actuelle associée au Cloud de confiance protège suffisamment des lois extraterritoriales d'après vous ?
Le Cloud de confiance ne protège pas suffisamment. Je pense qu'il faut aller un cran plus loin et donc ce qu'on est en train de travailler justement. C'est le caractère SecNumCloud d'un côté et le caractère qui est porté aussi par l'ENISA au niveau de l'Europe sur les données les plus sensibles. Là on parle du niveau 3 en matière de degrés de sensibilité de la donnée et de Gaia X qui justement prévoit un renforcement et une réelle protection et immunité aux lois extraterritoriales que ne procurent pas la notion de Cloud de confiance telle qu'elle est formulée aujourd'hui par l'État français.

Au niveau de Gaia X, en quoi vous pensez qu'elle protège mieux ?
En fait Gaia X ce n'est pas en tant que tel une réglementation, c'est un label. Je pense que ce qui est important c'est de comprendre en fait où va la demande. C'est la loi de l'offre et de la demande. Aujourd'hui, en matière de consommation, on parle de consommation responsable et de consommation et d'usage responsable dans tous nos actes du quotidien et notamment dans le choix de nos fournisseurs. Mais le fait d'aller vers un label, c'est faire le choix des acteurs qui respecteront les plus hauts degrés de confiance notamment par rapport aux lois extraterritoriales américaines. Et donc Gaia X vient amener cette information et transparence. Après, chacun a le choix d'acheter et de consommer les solutions de son choix. Donc ce n'est pas imposé, mais en tout cas cela oblige à la fois aux fournisseurs et aux consommateurs d'être informé sur ce qui va être consommé. Et donc de consommer d'une manière transparente. Ce qui est aujourd'hui complètement noyé par une sorte de désinformation autour du Cloud de confiance. L'objectif est de redonner aux acteurs la capacité de décider sur la base d'une information fiable. C'est vraiment une logique de label et donc ça amène la transparence ce qui n'existe tout simplement pas aujourd'hui.

Le fait que justement les Américains fassent partie de Gaia X, est-ce que cela ne constitue pas un frein à cette confiance justement ?
Je trouve ça effectivement contre-intuitif qu'il y ait des Américains qui y participent. Ça a discrétisé Gaia X. Ce qu'il faut savoir, c'est que les Américains ne votent pas. Les Américains sont juste observateurs.

Le fait d'être observateur ne leur permet pas d'avoir une longueur d'avance justement ? Sachant que les Américains sont souvent pro-actifs sur ces sujets. L'Europe ne fait que réagir dans la plupart des cas.
Les Américains n'ont pas le droit de voter, ils ont le droit de participer et donc ils comprennent en fait quelles sont les normes et les standards sur lesquels eux devront finalement s'aligner.
C'est important puisque ça permet de ne pas avoir à fournir un effort de migration énorme avec du développement spécifique. Et d'informer les fournisseurs de Cloud non européen de l'effort de mise à niveau pour rendre leur Cloud interopérable avec tout l'écosystème. Gaia X est donc un gros plus pour nous. En effet, cela veut dire que l'effort d'interopérabilité ne sera pas supporté que par des acteurs européens mais aussi par les acteurs américains. Ils vont devoir

se mettre au niveau des normes et des standards et le fait de les avoir impliqués et informés, c'est aussi leur donner du temps pour se mettre à niveau sans contraintes.

Annexe 3

Echange réalisé le 21 novembre 2022 auprès d'Emmanuel Meyrieux - Responsable sécurité clients chez OVHcloud

Quel est le niveau de maturité des TPE/PME qui s'adressent à OVHcloud en termes de : protection des données (classification des données, droits d'accès…etc.) et de risques auxquels elles seront exposées en migrant dans le Cloud ?

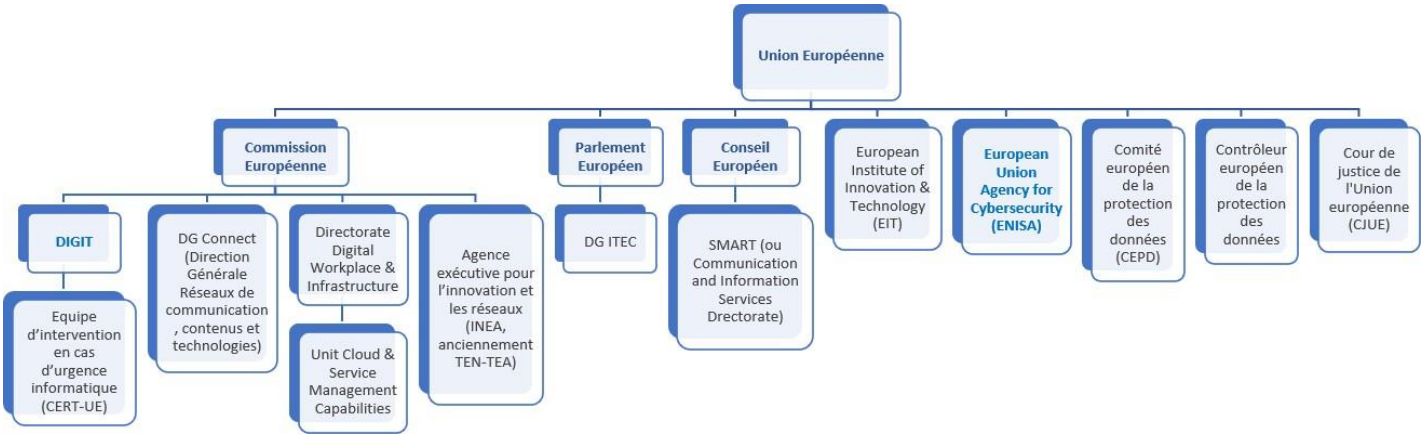
On trouve de tout : de l'ignorance aux experts. Plus les entreprises sont grosses ou soumises à des réglementations contraignantes, plus elles ont d'exigences pour leurs sous-traitants. Hélas ça ne veut pas dire que les exigences sont raisonnables. Trop d'entreprises n'ont pas encore pris la mesure des risques associés à leur utilisation des systèmes d'information, que ce soit On-Premise ou en Cloud. Du coup elles ont tendance à vouloir externaliser l'ensemble de leurs responsabilités ce qui n'est pas possible. Très peu de PME sont en maîtrise de leurs risques et elles ont tendance à se reposer sur leurs sous-traitants. Une tendance consiste aussi à externaliser notamment l'assistance à maîtrise d'ouvrage pour les systèmes d'information envoyés dans le Cloud. Cela entraîne des problèmes de compréhension par les entreprises de leur contexte opérationnel et de leurs risques.

Comment OVHcloud protège les données des TPE/PME face au Cloud Act ?

Le Cloud Act n'est qu'une partie du problème : d'autres lois américaines permettent l'accès aux données hébergées chez des fournisseurs totalement ou partiellement américains (d'autres pays ont ce type de lois). L'affaire Alstom nous a appris comment les lois anti-corruption US peuvent être utilisées pour prendre le contrôle d'une industrie sensible (j'ai été d'ailleurs surpris d'apprendre qu'une partie du conflit ukrainien était liée à la diplomatie nucléaire). Il est extrêmement compliqué d'avoir une assurance complète sur la non-application du Cloud Act car in fine ce sont des juges américains qui l'appliquent, juges pour la plupart élus. Au-delà du Cloud Act, certaines lois sont d'applications plus confidentielles et pourraient être soumises au huis clos. Du coup, plusieurs catégories de mesures combinées entre elles permettent d'avoir une assurance raisonnable de l'impossibilité d'accès par voie juridique aux données :

- ✓ Localiser les supports de données hors du territoire américain
- ✓ Employer des équipes de proximité dans les datacenters ainsi que des équipes de run techniques qui n'ont pas la nationalité américaine et qui n'opèrent pas depuis le sol des états unis d'Amérique
- ✓ Limiter la part d'actionnariat américain du fournisseur à un niveau raisonnable (cf. exigences 19.6 de SecNumCloud pour les seuils)
- ✓ Dans le cas où on opère une filiale aux USA (cas d'OVHcloud) : la filiale doit être autonome, mettre en œuvre son propre système d'information distinct de celui du reste du monde, avec un contrôle strict des partages d'informations entre les US et le reste du monde. A partir du moment où les control plane sont séparés et où les équipes n'ont aucun droit sur les control plane qui ne sont pas ceux de leur employeur, le risque commence à être maîtrisé (il reste entre autres le risque d'attaque sur la base de vulnérabilités de ces logiciels)
- ✓ Nouer des relations avec les fournisseurs de technologies logicielles permettant l'opération de leurs solutions en complète déconnexion avec leurs propres centres de supports de manière à ne pas importer un RUN US à nos opérations. Ici aussi, il s'agit de limiter l'information de notre fournisseur au besoin d'en connaître.

Annexe 4
Les institutions européennes



- La DIGIT (Direction Générale de l'Informatique) est un service de la Commission européenne. L'institution se concentre sur la protection des données mais n'a pas comme thématique directe le cloud, comme la plupart des organisations évoquées ici.
- La DG ITEC (Directorate-General for Innovation and Technological Support) est le service équivalent à la DIGIT, propre au Parlement Européen.
- Le SMART (ou Communication and Information Services Directorate), propre au Conseil Européen.
- DG Connect est la Direction Générale Réseaux de communication, contenus et technologies, direction générale de la Commission européenne
- CEPD (Contrôleur européen de la protection des données)
- Comité européen de la protection des données qui veillent au respect du RGPD.
- CERT-UE : service interinstitutionnel, l'Équipe d'intervention en cas d'urgence informatique.
- INEA anciennement TEN-TEA : Agence de la Commission européenne est Agence exécutive pour l'innovation et les réseaux.
- L'ENISA (European Union Agency for Cybersecurity) : Agence de l'Union européenne pour la cybersécurité, chargée de la sécurité des réseaux et de l'information, est une structure reconnue émettant des recommandations suivies. L'ENISA a, depuis 2013, avec l'élaboration de réglementations dans le domaine de la cybersécurité, de la protection des données et du cloud, pris en notoriété et confère des conseils et élabore des réglementations et délivre des certifications avec l'appui du Parlement européen et du Conseil de l'UE. De plus, le DIGIT est chargé de la mise en œuvre au sein de l'UE, de la sécurité des réseaux et des systèmes informatiques. La DIGIT quant à elle est écouté par la Commission européenne dans ses directives, mais n'a pas de pouvoir de réglementation.
- L'EIT (European Institute of Innovation & Technology), chargée du soutien des projets financés comme Horizon 2020.

Annexe 5
Cyber resilience Act (CRA) : L'application du règlement et les sanctions

Application du règlement :

Dès son entrée en vigueur, tous les États membres devront l'appliquer de la même manière. Ensuite, les opérateurs économiques et les États membres devront se mettre en conformité aux nouvelles exigences dans les deux ans qui suivent au plus tard.

La loi s'appliquerait aux fabricants, aux importateurs et aux distributeurs, lorsque ces derniers commercialisent des produits sous leur marque ou qu'ils effectuent une modification majeure. Afin de démontrer que les exigences ont été satisfaites en fonction de la criticité du produit, les fabricants pourraient procéder à une auto-évaluation ou une évaluation de la conformité par un tiers. Ensuite, une déclaration de conformité sera rédigée par les fabricants et les développeurs afin que leurs produits puissent circuler sur le marché européen.

Sanctions, points forts ou désavantages (concurrentiels) :

Suite à des non-conformités, les autorités nationales de surveillance du marché pourraient demander des corrections, des interdictions ou que le produit soit retiré / rappelé. En cas de récidives, les montants des amendes administratives seront fixés par les états membres en fonction des plafonds suivants :

- Jusqu'à 15 M€ ou 2,5% du dernier chiffre d'affaires (CA) annuel pour une non-conformité avec les exigences de sécurité et jusqu'à 10 M€ ou 2% du CA pour les autres exigences.
- Jusqu'à 5 M€ ou 1% du CA pour un manque de transparence envers les autorités compétentes (Informations incorrectes, incomplètes ou trompeuses).

Annexe 6
Digital Service Act “DSA” & Digital Market Act “DMA” : L’application des règlements et les sanctions prévues

Application des règlements :

- **DSA :** Le règlement s’applique à tous les intermédiaires en ligne, peu importe leur lieu d’établissement, qui offrent des services, des biens ou des contenus sur le marché européen :

- Les services Cloud.
- Les fournisseurs d’accès internet.
- Les plateformes en ligne (Marketplace, réseaux sociaux, plateforme de voyage…).
- Les plateformes en ligne et moteurs de recherche de très grandes tailles (Utilisation par plus de 45 millions d’européens par mois).

Les intermédiaires de petites tailles (< 45 millions d'utilisateurs) seront dispensés de certaines obligations.

Tous les acteurs concernés auront des obligations, ils doivent désigner un point de contact unique ou un représentant légal s’ils sont basés hors de l’UE afin de coopérer avec les autorités nationales. Les autres obligations, classées en trois catégories, vont varier en fonction des acteurs et surtout de leur rôle. Voici quelques exigences du règlement :

- La lutte contre les contenus illicites.
- La transparence en ligne (Explication du fonctionnement des algorithmes pour les plateformes et obligation de proposer un système de recommandation de contenu sans utilisation du profilage).
- Atténuation des risques et réponse aux crises. Cette partie est à destination des très grandes plateformes et des très grands moteurs de recherche de par leur importance à influencer l’opinion publique et les grands risques que leurs contenus « illicites ou préjudiciables » pourraient représenter. En plus des obligations qu’ils ont en termes d’analyse des risques et audits, ces acteurs devront fournir les algorithmes de leurs interfaces à la commission et aux autorités nationales compétentes et permettre l’accès à leurs données clés de leurs interfaces aux chercheurs agréés pour mieux suivre l’évolution des potentiels risques en ligne.

- **DMA :** Le règlement liste dix « services de plateforme essentiels » jugés très répandus et souvent utilisés. Parmi ces services, on retrouve les services Cloud, les moteurs de recherches, les réseaux sociaux, les messageries en ligne … etc.

Il cible des entreprises dites « contrôleurs d’accès » fournissant un ou plusieurs « services de plateforme essentiels ». Serait concernée toute entreprise jugée trop dominante ou remplissant certains critères comme le chiffre d’affaires ou le nombre d'utilisateurs dans l’UE. Elle sera donc désignée comme contrôleur d’accès et devra s’identifier auprès de la commission européenne.

L’obligation commune à tous les « contrôleurs d’accès » est la nomination d’un ou plusieurs responsables de la conformité avec ce règlement.

D’autres obligations (aujourd’hui une vingtaine, que la commission européenne pourrait compléter en fonction de l’évolution des pratiques de ces acteurs) seront toutes applicables ou en partie selon l’importance et la taille des acteurs identifiés.

Ces obligations listent les pratiques que les contrôleurs d'accès pourront faire et ne pas faire. On retrouve généralement des points impactant la liberté des utilisateurs et des vendeurs des plateformes / logiciels, ainsi que des pratiques principalement anticoncurrentielles.
Cette liste d'obligations servira surtout d'élément utilisable devant un juge national en cas de désaccord entre les utilisateurs et les contrôleurs d'accès ou en cas d'abus de pratique de la part de ces derniers.

Sanctions, points forts ou désavantages (concurrentiels) :

- **Le DSA** prévoit des amendes pouvant aller jusqu'à 6% du chiffre d'affaires mondial pour les très grandes plateformes et les très grands moteurs de recherche. Les activités de ces derniers peuvent être interdites sur le marché européen en cas de violations graves et répétées du règlement.
- **Le DMA** prévoit des amendes pouvant aller jusqu'à 10% du chiffres d'affaires mondial ou jusqu'à 20% de ce dernier en cas de récidive. A partir de trois violations sur huit ans, le contrôleur d'accès pourrait être obligé de céder une de ces activités ou de lui interdire d'acquérir des entreprises fournissant des services dans le numérique ou des services de collectes de données.

Annexe 7
Petit guide juridique de protection du secret des affaires

Village de la Justice*www.village-justice.com*

Le secret des affaires : une protection juridique des données stratégiques. Par Olivier de Maison Rouge, Avocat.
Parution : jeudi 2 août 2018
Adresse de l'article original :
https://www.village-justice.com/articles/secret-des-affaires-une-protection-juridique-des-donnees-strategiques,29154.html

A l'ère de la transparence, donner corps au secret des affaires ne semblait pas être une chose facile. En effet, il existe une véritable opposition à reconnaître la vie privée de l'entreprise et lui permettre de protéger son avantage concurrentiel. C'est pourtant chose faite avec la loi n°2018-670 du 30 juillet 2018

Avec le secret des affaires, il s'agit d'offrir à l'entreprise la protection de sa sphère privée, à savoir ses connaissances stratégiques et ses informations sensibles, dans un environnement où les atteintes aux données et les actes prédateurs sont devenus monnaie courante.

I - Une définition par défaut juridiquement consacrée

Cela pouvait être une gageure de définir, de la manière la plus large possible, ce qui par principe n'est connu que d'un petit nombre d'initiés.
Et pourtant, relevant ce défi, le droit a consacré une norme juridique unifiée afin « d'étalonner », par défaut, cette notion constituée de R&D, « de savoir-faire et d'informations commerciales non divulguées » pour reprendre le titre de la directive.

Les secrets d'affaires sont ainsi identifiés sous trois conditions cumulatives :

1) non connus du grand public et/ou du secteur professionnel concerné ;
2) ayant une valeur commerciale, réelle ou potentielle, parce que secrets ;
3) et faisant l'objet de mesures spécifiques destinées à les garder confidentiels.

Cela peut être un algorithme, une méthode, une stratégie commerciale comme le lancement d'un nouveau produit, un schéma organisationnel, la composition d'une recette, d'un parfum, …
Sous cette définition commune, le secret des affaires est présenté comme un outil juridique alternatif permettant de consolider la sécurité des actifs informationnels de l'entreprise.

II - Les exceptions au secret :

- le droit en impose la communication, notamment en cas de contrôle ou d'enquête des autorités judiciaires ou administratives ;
- le secret est divulgué par des journalistes dans le cadre de la liberté d'expression et du droit d'informer ;
- un lanceur d'alerte révèle de bonne foi, de manière désintéressée et dans le but de protéger l'intérêt général, une activité illégale, une fraude ou un comportement répréhensible ;
- il s'agit d'empêcher ou de faire cesser toute atteinte à l'ordre public, à la sécurité, à la santé publique et à l'environnement ;
- il a été obtenu dans le cadre de l'exercice du droit à l'information des salariés ou de leurs représentants.

III - Comment protéger le secret des affaires de l'entreprise ?

Seules les entreprises ayant mis en place en amont des « protections raisonnables » pour garder leurs informations secrètes pourront faire valoir leurs droits devant les tribunaux et les faire reconnaître en tant que telles.
Si elle ne le fait pas, elle risque de ne pas pouvoir opposer sa protection des secrets d'affaires devant le juge qui écartera la qualification de secret des affaires et la protection qui va de pair.
En d'autres termes, le texte suppose que les entreprises prennent en charge leur protection selon une politique de sécurité qu'il lui appartient de définir en fonction de la nature des informations qu'elle entend protéger.

Par conséquent, une protection efficace du secret des affaires suppose la mise en œuvre d'un processus composé de trois étapes-clés :

1. l'identification des informations confidentielles ;
2. leur classification ;
3. l'organisation de leur protection par des moyens adaptés.

Conseils pratiques :
Il faut se concentrer sur ce qui doit être tenu secret ; toute information n'a pas vocation à être protégée. En effet, tout classifier serait contreproductif - car une entreprise par nature évolue dans un monde économique qui appelle souplesse, agilité, réactivité et disponibilité - il convient au préalable de recenser les données constitutives des avantages concurrentiels de l'entreprise. Puis, l'entreprise doit faire l'effort de prioriser et hiérarchiser les informations. Il est fortement conseillé de leur attribuer un code reflétant le niveau de classification selon différents critères : public, sensible, critique, stratégique (par exemple C0, C1, C2, C3). Il faut également délimiter le périmètre des personnes ayant accès à ces informations.

IV – Secret des affaires et protection des données personnelles de l'entreprise

D'une certaine manière, l'approche relative à la protection de ces données confidentielles n'est pas une démarche éloignée de celle instituée par le RGPD. Elle diffère néanmoins par ce besoin d'identification préalable des secrets de l'entreprise qu'il lui appartient de désigner conformément à la définition ci-dessus tandis que le RGPD protège les données des tiers strictement désignées par la loi.
En outre, le mode de protection des données personnelles est beaucoup plus contraint selon des obligations règlementaires, quand le choix des moyens de protection raisonnable est à la discrétion de l'entreprise ; mais par souci d'efficacité opérationnelle la politique de protection des données personnelles peut inspirer celle organisant la sécurité des secrets d'affaires de l'entreprise, ne serait-ce qu'en désignant un seul et même délégué à la protection des données (DPO).

V - Le rôle cardinal du juge dans la qualification du secret des affaires

La protection des secrets d'affaires peut être invoquée devant les tribunaux contre les actes :

- d'obtention,
- de divulgation,
- et d'utilisation illicites.

Le procès sera déterminant à double titre :

- Le juge va estimer si l'entreprise a mis en œuvre les moyens de protection raisonnables pour sécuriser ses informations stratégiques, rendant ainsi celles-ci éligibles à la protection du secret des affaires telle que prévue par loi ;
- dans l'affirmative, le juge devra veiller à instituer les mesures nécessaires afin que le secret ne soit pas dévoilé :
  - a) Création d'un périmètre de confidentialité pour les parties (avocats, experts, témoins).
  - b) Restriction dans l'accès aux pièces produites au cours de la procédure.
  - c) Restriction dans l'accès aux audiences.
  - d) Jugement élagué de l'énonciation des secrets d'affaires.

Cette saisine du juge permet à son titulaire :

- de solliciter auprès du juge des mesures d'interdiction, y compris provisoires ;
- de solliciter des mesures « correctives » se traduisant notamment par l'interdiction d'importation de produits fabriqués en violation de secrets d'affaires.

En matière de réparation civile, outre le préjudice constaté, le juge pourra également tenir compte des conséquences économiques négatives telles que le manque à gagner ou les bénéfices réalisés par le contrevenant.

Olivier de Maison Rouge, avocat - docteur en droit - Lex-Squared Rapporteur du groupe d'experts constitué auprès du Ministère de l'Economie sur la transposition de la directive sur le secret des affaires du 8 juin 2016 Auteur du \"droit de l\'intelligence économique\" Lamy, 2012 \"le droit du renseignement - renseignement d\'Etat, renseignement économique\", LexisNexis, 2016

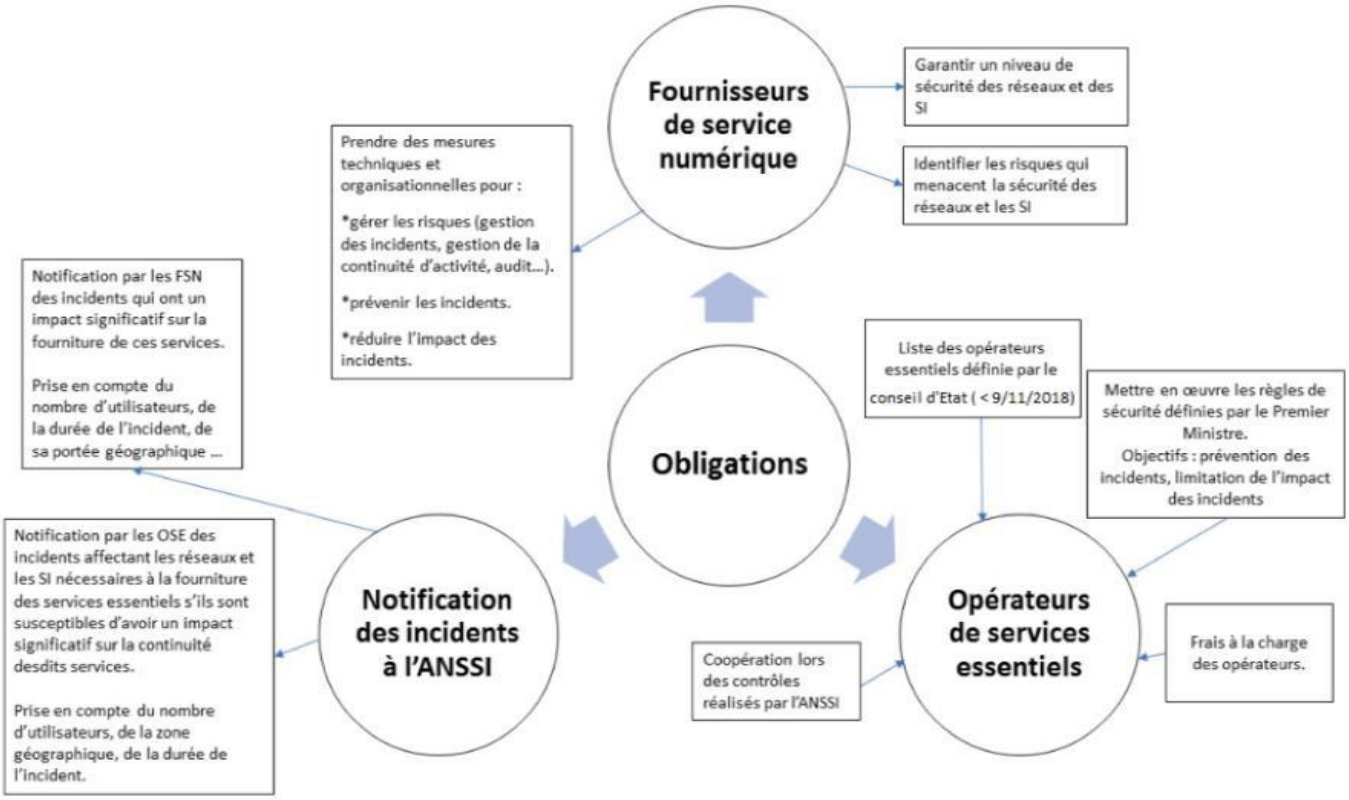
Annexe 8
Sanction CNIL à l'encontre de TOTALENERGIES

[IL7]

Source : LinkedIn (https://www.cnil.fr/fr/prospection-commerciale-et-droits-des-personnes-sanction-de-1-million-deuros-lencontre-de)

Annexe 9

Transposition de la directive NIS en France



Source : https://evabssi.com/transposition-de-la-directive-nis-en-france/

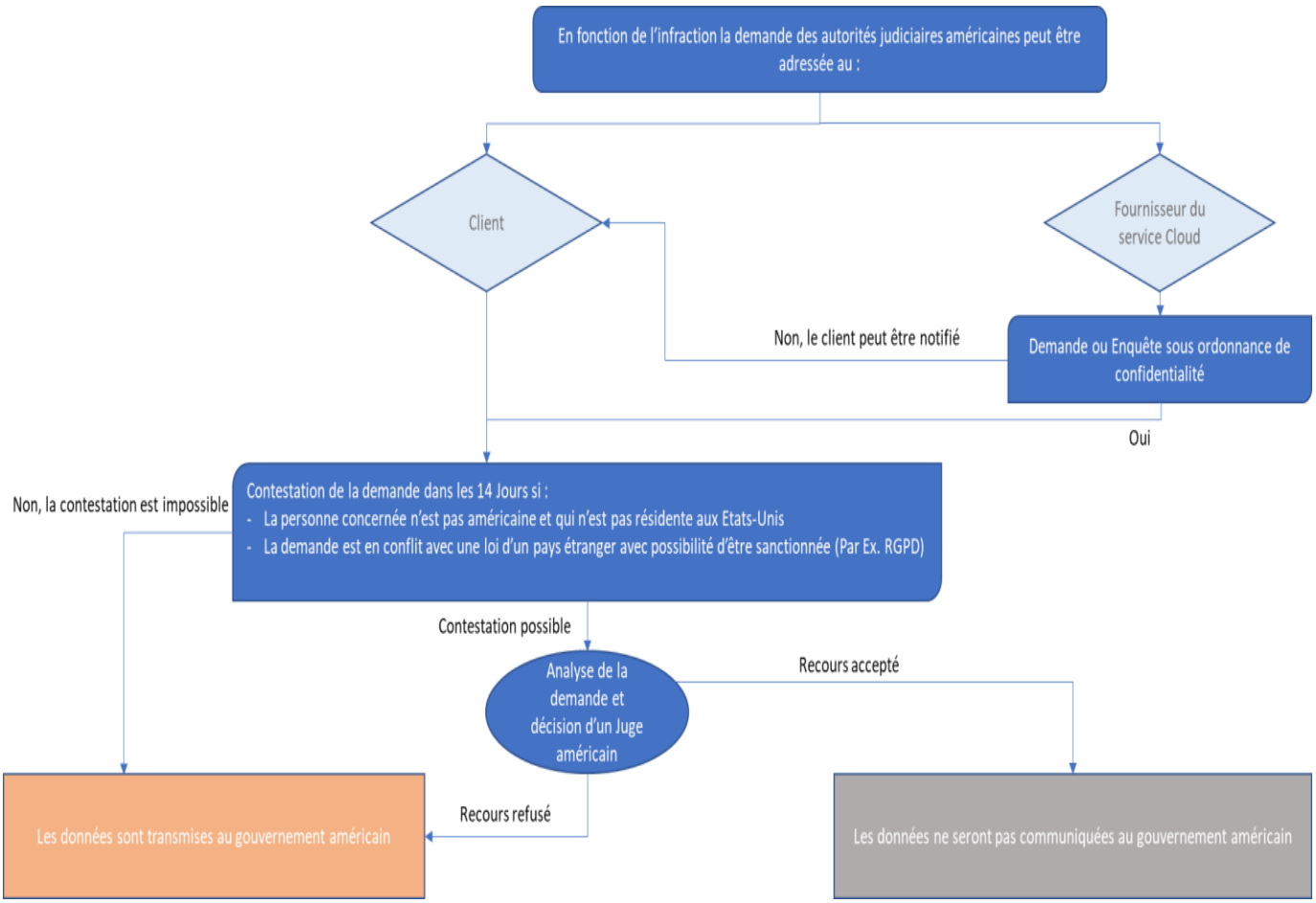
Annexe 10
Comparaison du « Patriot Act » et du « Cloud Act »

Comparaison PATRIOT Act & CLOUD Act

	PATRIOT Act	CLOUD Act (hors executive agreements)
Date	26 octobre 2001 Loi d'exception devant durer 4 ans mais dont certaines dispositions ont été rendues permanentes en 2005.	23 mars 2018 Loi jointe au budget fédéral américain.
Bénéficiaires	Agences gouvernementales américaines (FBI, CIA, NSA, armée)	Autorités américaines bénéficiant d'un mandat
Matière	Terrorisme	Pénal
Contexte	Enquête relative à des actes de terrorisme	Enquête judiciaire
Cibles	Entreprises américaines et leurs filiales à l'étranger	Entreprises américaines et leurs filiales à l'étranger
Nationalité de la personne concernée	Américain ou étranger	Américain ou étranger
Lieu où est située l'information	Aux États-Unis ou à l'étranger	Aux États-Unis ou à l'étranger
Type de données	Données de connexion (sans recours au juge) et données de contenu (avec nécessaire recours à un juge)	Données placées sous le contrôle du fournisseur de service

Source : https://www.lemagit.fr/conseil/Quelles-differences-entre-CLOUD-Act-et-PARTIOT-Act-et-quels-impacts- sur-les-entreprises-francaises

Annexe 11
Cloud Act, Le processus de demande d'accès aux données auprès d'un client et de son fournisseur



Source : https://www.riskinsight-wavestone.com/2021/11/le-cloud-act-une-maniere-de-rendre-les-donnees-non-souveraines/

Annexe 12
Cloud Act, Les Avis des fournisseurs américains de services Cloud

Amazon indique qu'ils contestent les demandes inappropriées et qu'ils continueront d'avertir leurs clients, si la loi l'autorise, en cas de nécessité de fournir les informations *« Nous avons toujours contesté les demandes d'informations des clients émanant du gouvernement et que nous estimons excessives ou inappropriées. Si nous sommes tenus de divulguer le contenu du client, nous continuerons d'avertir les clients avant la divulgation afin de leur donner la possibilité de demander la protection de la divulgation, sauf si la loi l'interdit ».*

Aussi, des rapports avec des chiffres détaillant les demandes reçues de tous les pays sont publiés deux fois par an par les fournisseurs Microsoft (86), Amazon (107) et Google (108). Les informations publiées diffèrent d'un fournisseur à un autre. Il faut noter que les fournisseurs Cloud ne sont pas obligés de communiquer ces informations (quand ils le peuvent car certaines demandes sont tenues par le secret des enquêtes).
D'après une étude réalisée par Riskinsight-wavostone (109) : *« Amazon ne fournit pas d'informations détaillées concernant l'emplacement des données divulguées ou le pourcentage de données divulguées sur l'ensemble des demandes"*[8]

Google reçoit plus de demandes de la part des institutions que Microsoft et divulgue plus souvent des informations que Microsoft, ce qui peut s'expliquer par le fait que les services de Google sont davantage destinés aux particuliers qu'aux entreprises. »

Ils n'hésitent pas à conseiller aussi leurs clients sur les mesures supplémentaires à prendre pour protéger leurs données comme le chiffrement. Ils proposent bien sûr de vendre plus de services comme les solutions de chiffrement ou la gestion des clés, mais pour eux ces mesures permettraient aux clients de garder le contrôle sur leurs données.

Annexe 13
Questions réponses & recommandations avant de migrer dans le cloud (liste non exhaustive)

Ref. QR	QUESTIONS REPONSES & RECOMMANDATIONS AVANT DE MIGRER DANS LE CLOUD (LISTE NON EXHAUSTIVE)
	Qualification du besoin
QR1	**Quel est mon système d'information actuel ? Quel est le mode d'intégration ?** Cartographier son infrastructure et son parc applicatif et ses interfaces actuelles permettent d'en évaluer les performances et les limites en anticipant / priorisant les évolutions. Cela facilite également l'alignement stratégique. Connaitre son existant aide à mieux définir sa cible et à identifier les prérequis nécessaires afin de s'assurer des adaptations nécessaires pour migrer dans le cloud en termes de compatibilité avec les applications. La possibilité de faire des tests en amont pour déterminer les applications à transférer dans le cloud et d'en analyser les performances (test de latence, impact sur la bande passante de l'équipe…) peut faire partie des facteurs clés de succès du projet de migration. Il est important de comprendre en détail l'architecture de vos applications (tous les composants, leur dépendance et leur intégration) avant d'envisager leur migration vers le cloud.
QR2	**Qui seront les usagers du cloud ? (Interne DSI, métiers, partenaires externes, clients). Combien sont-ils ?** En répondant à cette question en amont, les parties prenantes seront impliquées à temps. Etablir une matrice de responsabilité de type RACI (Réalisateur, Approbateur, Consulté, et Informé) permettra de clarifier les rôles et responsabilités de chaque entité/personne. En définissant le nombre d'usagers, cela permet d'affiner le périmètre du projet et d'anticiper sur un des éléments du budget notamment pour les solutions SaaS où le paiement se fait à l'usage.
QR3	**Un audit de sécurité de mes systèmes d'information a-t-elle déjà été réalisé ? (Analyse de risques, tests d'intrusion…)** En procédant régulièrement à un audit de sécurité de son SI, l'entreprise est en capacité de révéler d'éventuelles failles ou dysfonctionnements qui pourraient compromettre ses activités. Elle vérifie ainsi qu'elle est alignée avec sa politique de sécurité et qu'elle est en conformité avec les référentiels en vigueur. Cela permet de s'assurer que la source de cette migration est saine et sécurisée. Si des audits ont déjà été réalisés, il faut les lister en précisant les dates de réalisation. Si le SI actuel n'est pas assez sécurisé, il faudrait prendre les bonnes dispositions.
QR4	**Quel est le modèle de cloud envisagé ? (Cloud public, cloud privé ou cloud hybride déployé en interne ou en externe) Quel est le type d'offre cloud envisagée ? (IaaS, PaaS, SaaS, etc.)** La rédaction d'une expression de besoin est une étape nécessaire qui décrit la situation actuelle (insatisfaisante) versus la situation future (satisfaisante) le tout combiné à une analyse fonctionnelle (fonction d'un domaine, d'un système…). Pendant cette étape, l'équipe à l'origine de ce besoin peut déjà envisagée le modèle de cloud qui pourrait répondant à sa problématique.
QR5	**Mes données hébergées seront-elles soumises au RGPD ? Ai-je des données sensibles/critiques à protéger ?** Se poser cette question en amont permet de restreindre la liste des fournisseurs et de s'assurer surtout que l'hébergeur est en conformité avec la réglementation en vigueur selon le lieu de stockage et traitement de vos données.

	Ma maîtrise d'œuvre est-elle externalisée ?
QR6	Il est primordial d'impliquer cette équipe dans ce projet en s'assurant qu'elle a toutes les compétences et la disponibilité pour vous accompagner lors de la migration. Il est également intéressant de se demander si elle doit évoluer après la migration et si elle est toujours nécessaire sous sa forme actuelle selon le cloud choisi.
	Mon pilotage économique (FinOps/TCO) est-il intégré dans ma transition ?
QR7	Avant de migrer vers le cloud, il est nécessaire de mener une analyse financière. Le modèle de déploiement SaaS est basé sur une solution de facturation à l'usage des services utilisés et en fonction du volume de ressources utilisées. Cela permet à l'entreprise d'avoir une flexibilité et d'anticiper ses coûts. En mettant en place des calculs du TCO (Coût total de possession, charges directes et indirectes) et du FinOps (monitorer et optimiser les coûts), l'entreprise réalise des économies d'échelle notamment à travers le nombre de jours nécessaires, ainsi que les coûts de licence et la formation par exemple réellement utilisés.
	Contrat & Choix de l'offre
	Est-ce que toutes les conditions d'évolution (tarifaires, techniques...) de la solution Cloud sont clairement détaillées dans le contrat ?
QR8	Les demandes de ressources supplémentaires peuvent survenir pour des raisons diverses (développement du projet ou lors de surcharge des ressources durant des périodes saisonnières par exemple). Il est important de connaître la capacité d'extension du fournisseur avant de choisir une option. Les options proposées auront un coût supplémentaire à prendre en compte dans le budget.
QR9	**Quelle est la durée du contrat et quelles sont les possibilités de rupture (même en cours de contrat) ?** Les détails du produit / service Cloud sont une aide précieuse pour vérifier les conditions de résiliation et s'assurer que l'entreprise ne se retrouve pas dépendante du fournisseur sans possibilité de rupture du contrat (110).
	Est-ce que le contrat est soumis au droit européen ou à d'autres réglementations ? Quelle est la politique et les engagements du fournisseur pour la protection des données personnelles ?
QR10	Le client a la responsabilité de s'assurer que le fournisseur de Cloud est conforme aux réglementations en vigueur pour la protection des données personnelles. Le RGPD s'applique aux fournisseurs de services Cloud et aux clients de ces fournisseurs. En cas de non-respect du RGPD, le client pourrait s'exposer à des sanctions administratives, civiles et pénales. Le fournisseur de Cloud doit fournir des mesures de sécurité techniques et organisationnelles suffisantes pour l'exécution du traitement des données collectées.
	Quelles sont les mesures prisent par le fournisseur pour garantir que les tiers/sous-traitant respectent et maintiennent les niveaux de sécurité et de services ?
QR11	Si le fournisseur Cloud sous-traite une partie de ses services, il doit garantir à l'entreprise cliente le bon fonctionnement de ces derniers. Cela peut passer par des certifications de conformité ou des audits, afin de rassurer le client sur la prise en compte des potentiels risques liés à la sous-traitance (111).
	Est-ce que l'offre inclut un service d'infogérance ou de télémaintenance ?
QR12	Le Cloud et l'infogérance sont deux services distincts. Ils sont indépendants l'un de l'autre, mais qui servent pourtant un intérêt commun. En fonction de l'offre, l'approche peut être différente. L'infogérance est généralement en supplément et l'option est souvent payante.

	Les services proposés et identifiés sont-ils couverts par l'assurance professionnelle du fournisseur en cas d'incident ?
QR13	Le cadre contractuel des services cloud est a priori déséquilibré en faveur des fournisseurs, dans certains contrats on peut lire par exemple : « aucune garantie que le contenu quel qu'il soit sera conservé de manière sécurisée et ne sera ni perdu ni endommagé… ». Les contrats des fournisseurs Cloud sont souvent des contrats d'adhésion. Le contrat d'adhésion est défini par l'article 1110 du Code civil : « le contrat d'adhésion est celui qui comporte un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties. » (112). Toutefois, il existe des assurances liées aux risques cyber dédiées pour protéger les entreprises.
	Le fournisseur s'engage-t-il à fournir les journaux d'événements ? quelles informations, leur format et fuseau horaire ?
QR14	Dans le cadre d'une enquête suite à un incident, il est nécessaire que les journaux d'audit soient exploitables et recevables devant un tribunal. Le fournisseur doit donc garantir leur disponibilité et leur intégrité. Le client doit savoir leur format, comment les utiliser et les informations enregistrées. Il doit aussi avoir une garantie de la part du fournisseur que ces journaux sont bien protégés contre toute intrusion ou falsification. Un des éléments aussi très important, c'est la source de temps utilisée. Les systèmes doivent être synchronisés afin de fournir un horodatage précis et exploitable des journaux d'audit.
	Quels sont les engagements du fournisseur en termes de communication sur les incidents de sécurité (fuite de données …) ?
QR15	Il est impératif de savoir quelles mesures un fournisseur de cloud a mis en place en cas d'un incident de sécurité (exemple : perte, effacement ou corruption de données). Les entreprises doivent s'informer sur le niveau de durabilité des données que le fournisseur peut garantir, et le nombre de copies de sauvegarde que le fournisseur conserve en cas d'incident de perte de données. (113)
	Le fournisseur/hébergeur accepte-t-il d'être audité ?
QR16	Certains fournisseurs mettent à la disposition de leurs clients (à la demande), le rapport de l'audit de la conformité des systèmes informatiques basés sur le Cloud. Ces preuves sont essentielles pour garantir des processus opérationnels, efficaces et sécurisés. Les clients peuvent donc prendre connaissance des rapports d'audits réalisés par des auditeurs indépendants et certifiés. Ils comprennent généralement : la compréhension de l'environnement de contrôle interne, l'accès à la piste d'audit du fournisseur et l'examen des fonctionnalités de gestion et de contrôle. (114)

Quelles sont les garanties de niveau de service ? (SLA, OLA) Est-ce que les rôles et responsabilités sont indiqués clairement dans le contrat ?

QR17

La répartition des responsabilités et des rôles doit être clairement défini dans le contrat. Selon le type de service Cloud, la répartition des responsabilités entre les parties prenantes varie grandement. Les TPE/PME n'ont généralement pas de possibilité de négociation, elles doivent donc vérifier en détail les items dont ils sont responsables. Pour les offres SaaS les responsabilités sont déléguées en grande partie au fournisseur Cloud.
Dans le cadre de la continuité et la reprise des activités suite à un incident, il est nécessaire d'avoir au minimum des accords sur les niveaux de services et des informations sur la durée minimale de disponibilité des systèmes, ainsi que la gestion et la réponse aux incidents. Il est donc primordial de savoir en amont si le fournisseur maintient un processus détaillant :
Les moyens de communication, ainsi que les rôles et les responsabilités lors de la gestion de l'incident
Les criticités des services avec leur RPO et RTO

- La prise en compte des priorités du client durant la restauration et si cette dernière prend en compte la sécurisation des données

La possibilité d'avoir un site secondaire si le site initial est indisponible
Le processus de détection, d'analyse et de réponse aux incidents. Ainsi que la méthode de test du processus.

- Les tests de reprise et de continuité des activités, les tests de vulnérabilité et leur fréquence, ainsi que l'implication du client dans le processus.

Les accords de niveau de service mis en place (SLA), entre le fournisseur et le client, protégeraient le client en cas de perturbation des services fournis. En cas de non-respect de ces accords, le fournisseur s'exposerait à des pénalités. (115)
OLA : Accords sur les niveaux opérationnels (Operational Level Agreement ou OLA), ce sont les accords internes à l'informatique. Ils supportent les SLA lorsqu'un service informatique dépend d'autres services fournis par un prestataire.

Fournisseur / Prestataire (obligations)

Quelle est la réputation du fournisseur ? Sa santé financière ? Fait-il partie d'un registre de référence de type CSA Star : https://cloudsecurityalliance.org/star/registry ?

QR18

Pour le choix d'un fournisseur, il est important de conduire une due diligence (Pour aller plus loin (116)) afin de savoir s'il est fiable et si ses capacités pourraient assurer un service à long terme. Pour faire confiance au fournisseur, il faut au minimum s'assurer de sa santé financière (Vérifier son bilan et résultats sur les 3 dernières années) et de sa réputation (Les avis des autres entreprises sont importants ou encore les registre de référence type CSA Star). Il ne faut pas se fier à la taille du fournisseur, ce n'est en aucun cas un indicateur sur sa viabilité à long terme.

Le prestataire fait-il appel à un SOC (Security Operations Center) ?

QR19

L'implantation d'un SOC -Security Operations Center ou Centre Opérationnel de Sécurité permettra de détecter et de remonter des alertes de qui n'étaient pas forcément indétectable auparavant. Il peut être installé dans l'entreprise ou confié à un prestataire. (113)

	Est-ce que le fournisseur externalise / sous-traite des services qui sont essentiels à la sécurité de mes opérations / données ?
QR20	Le fournisseur peut sous-traiter un accès à son infrastructure (à distance ou physique). Les sous-traitants du fournisseur peuvent réaliser certaines opérations ayant un impact direct sur la sécurité des opérations dans le Cloud. Par exemple, la sous-traitance des services de sécurité, ou encore la gestion des identités des systèmes d'exploitation. Il faudrait connaître les procédures utilisées par le fournisseur dans le cadre de la sous-traitance et de savoir si elle a les mêmes niveaux de garantie pour assurer le maintien des services. Par exemple, une présentation de preuves contractuelles confirmant que la même politique et les mêmes contrôles de sécurité sont appliqués à ses sous-traitants.
	Quels sont les accès qu'auraient mes sous-traitants / fournisseurs ?
QR21	Le sous-traitant aura accès aux infrastructures et aux données que si le responsable du traitement lui en a donné l'autorisation. Si le sous-traitant traite des données personnelles (RGPD) pour le compte du responsable du traitement. Dans ce cadre, il ne fera que suivre les instructions du responsable de traitement et ne peut pas, en principe, utiliser les données pour son propre.
	Les datacenters du fournisseur offrent-ils des garanties de sécurité suffisantes ? Quelles sont les assurances que le fournisseur peut communiquer pour la sécurité physique de son infrastructure ? Evaluation et gestion des risques, audits et contrôles ?
QR22	Le Guide sur le Cloud Computing et les Datacenters mise en ligne par la caisse des dépôts, la possession des labels et certificats de conformité ou du SecnumCloud de l'ANSSI traduit la mise en œuvre des critères prédéfinis par les nomes et référentiels requis. Il faudrait s'assurer que le fournisseur ait obtenu des certifications afin de garantir la sécurité physique de son infrastructure et qu'il procède éventuellement à la gestion des risques au niveau de son infrastructure. (117)
	Est-ce qu'un fournisseur / sous-traitant de remplacement en cas d'incident a été identifié ?
QR23	La Cnil dans sa recommandation n°3 (pour les entreprises qui envisagent de souscrire à des services de Cloud computing), conseille aux entreprises de conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles. La dépendance du fournisseur de Cloud est identifiée comme étant un risque que les entreprises doivent y penser en amont afin de prendre des mesures nécessaires pour l'atténuer si toutefois ce risque ne peut être supprimé. Comme mesure de traitement de ce risque, il convient donc d'identifier un fournisseur de remplacement, dans le cas où le fournisseur principal n'est pas en mesure d'assurer les services souscris. (117)
	Le fournisseur propose-t-il un Plan d'Assurance Sécurité (PAS) ?
QR24	Le PAS décrit l'ensemble des dispositions spécifiques que les fournisseurs s'engagent à mettre en œuvre pour garantir le respect des exigences de sécurité du client. Il est annexé au contrat et se substitue aux éventuelles clauses génériques de sécurité du prestataire. Le PAS à lui seul ne suffit pas, il doit être compléter avec une évaluation des risques Cloud et une annexe de clauses de sécurité des données. (118)

Réglementation & Sécurité des données/accès	
QR25	**Comment garantir l'isolation des données entre les clients dans le cas d'un cloud public ?** Généralement, les fournisseurs mettent en place les mesures nécessaires afin de garantir une isolation stricte entre les ressources partagées des clients d'un Cloud public. Cela permet de réduire / d'éviter le risque d'exploitation d'application ou de machines virtuelles appartenant à d'autres et de voir ses données compromises. Le fournisseur doit ainsi vous mettre à disposition une description détaillée des outils mis en place et garantissant que personne ne peut accéder à vos données (intentionnellement ou pas). L'une des solutions proposées, est l'utilisation d'un annuaire (Active Directory) et d'un contrôle d'accès. Ces derniers sont gérés à plus haut niveau par le fournisseur et permettent l'isolation des données et des informations d'identité des clients. Chaque utilisateur ou administrateur ne peut accéder qu'à son propre système isolé et peut gérer à ce niveau les rôles et les droits d'accès aux différentes informations et applications. (119) (120)
QR26	**Existe-t-il un processus d'archivage et de temps de rétention des données ?** Il est nécessaire de vérifier que le contrat contient des garanties quant à la durée de conservation des données par le fournisseur. Ce dernier doit s'engager à ne pas conserver les données au-delà d'une date (fixée conjointement) et à la fin du contrat. (106)
QR27	**Est-ce que le service Cloud utilisé implique le transfert de données vers un pays hors UE ? (Pour des raisons de support notamment)** Il est très important de savoir les pays par lesquels les données vont transiter et où est-ce qu'elles seraient stockées physiquement. Il faut garder à l'esprit que différentes réglementations seront appliquées aux données : selon les lois locales du pays de stockage ou encore selon les lois du pays auxquelles les responsables de traitement dépendent. (Voir *Chapitre 3 : Cadre réglementaire et normatif autour du Cloud)*
QR28	**Que se passe-t-il au niveau des données à la fin du contrat avec le fournisseur Cloud ? (Procédure de réversibilité et d'effacement des données)** Deux points sont très importants avant la signature d'un contrat avec un fournisseur Cloud : Le premier est de pouvoir garder le contrôle sur ses données et d'éviter de se retrouver dépendant du fournisseur Cloud. Il est primordial de s'assurer de la réversibilité et de l'interopérabilité, respectivement des données et des applications. En d'autres termes, il faut être capable de pouvoir exporter les données et les transférer chez un autre fournisseur Cloud sans rupture de service. Et de s'assurer que les systèmes du fournisseur sont compatibles avec d'autres systèmes comme les logiciels libres par exemple ou avec les solutions utilisées dans un Multicloud. Le deuxième point est de savoir si le fournisseur est capable de supprimer de manière définitive et sur demande les données. En effet, lors d'une demande de suppression ou destruction de données, certaines données peuvent ne pas être véritablement supprimées. Comme pour les systèmes d'exploitation et le principe de fragmentation des données, les plateformes Cloud utilisent souvent un mécanisme de stockage qui peut être parfois redondant avec un stockage en plusieurs copies sur des supports physiques différents. Ainsi, une suppression complète de données peut ne pas être possible soit parce que les copies supplémentaires stockées ne sont pas disponibles ou que les supports physiques à détruire contiennent également les données des autres clients dans le cas de la location multiple. Si tel est le cas, il faut prendre ce risque en compte est mettre les plans d'action nécessaires pour son traitement. (121) (122)

Comment les données seront-elles collectées, traitées et transférées ? Et comment seront-elles protégées et sécurisées ?

La sécurité des données dans le Cloud est essentielle, que ce soit la sécurisation des transferts ou la sécurisation des données dans le Cloud. Ces deux aspects doivent être pris en compte pour le choix du fournisseur. L'utilisation de la sécurisation des transferts de données dans le Cloud est une fonctionnalité qui est souvent plus sécurisée et moins coûteuse que les méthodes de transfert manuelles (Ex. protocole de transfert de fichiers sécurisé (SFTP) via un serveur sur une machine virtuelle du même fournisseur). Différentes options sont utilisées par les fournisseurs (Chiffrement en transit, Protocole TLS ou le chiffrement basé sur un proxy).

Quant à la sécurisation des données dans le Cloud, deux points sont importants à retenir et à vérifier auprès du fournisseur : les contrôles d'accès aux données et leur protection :

QR29

La plupart des fournisseurs Cloud proposent des politiques de contrôle d'accès par défaut, il faudrait vérifier si cette fonctionnalité est comprise dans l'offre. Il faudrait aussi identifier un potentiel besoin de couches de contrôle d'accès supplémentaires (Ex. Les données qui sont partagées en externe avec le public ou des partenaires et qui n'ont pas un accès direct à la plateforme Cloud). Si c'est le cas il faudra en tenir compte lors du choix ou de la négociation du contrat.

- Concernant la protection des données, deux technologies peuvent être utilisées selon les besoins, le chiffrement ou la tokenisation. Le client doit s'assurer de la possibilité de la mise en place des politiques et des procédures pour l'utilisation de protocoles de chiffrement. Notamment pour les données classifiées sensibles, ainsi que les données personnelles (stockées, utilisées en mémoire ou en transmission). Est-ce que je peux envoyer la bonne clé au bon endroit et au bon moment en respectant mes exigences de sécurité et de conformité ? Nous ne pouvons pas évoquer la protection des données et le chiffrement sans savoir comment seront gérées les clés. Il faudrait savoir si on peut avoir confiance au fournisseur pour la gestion de ces clés et comment ces dernières pourraient se retrouver exposées. Différentes solutions peuvent être mises en place pour la gestion des clés de chiffrement.
Dans le cas d'une gestion par le fournisseur, il faut bien comprendre son modèle de sécurité et les accords afin de savoir si les clés pourraient être exposées. Elles peuvent aussi être gérées par le client lui-même en utilisant soit un module de sécurité matériel (HSM) traditionnel ou un gestionnaire de clés et ensuite transmettre les clés au Cloud via une connexion dédiée, soit un logiciel / Appareil virtuel ou un gestionnaire de clés dans le Cloud. Au-delà du coût qu'il faudrait prendre en compte dans l'estimation du budget, selon la sensibilité des données stockées, il est préférable que le client gère ses clés avec un stockage à l'extérieur du Cloud et ne les transmettre qu'en cas de demande justifiée (procédure judiciaire par exemple).

Qui aura accès à mes données ?

QR30

Les fournisseurs Cloud sont conscients de l'importance du maintien de la sécurité, la confidentialité et la disponibilité des données. Généralement, ils disposent du savoir-faire et des meilleurs outils pour assurer la sécurité et réduire les risques humains. Il faut bien comprendre les politiques de protection que le fournisseur pourrait offrir. L'objectif étant de limiter les accès aux données sensibles, les politiques doivent indiquer les mesures à mettre en place pour contrôler les accès et pour détecter, voir bloquer les accès non autorisés. A cela, s'ajoute la classification efficace des données sensibles avec les différents niveaux d'accès selon la confidentialité des données dont l'entreprise est responsable.

QR31	**La gouvernance du prestataire est-elle en conformité avec le RGPD ?** Répondre aux questions ci-dessous permet de savoir si le prestataire est en conformité avec le RGPD. (Voir la *Partie 2 Réglementations françaises pour les données personnelles)* Quelles sont mes données personnelles traitées ? Qui assure le traitement de mes données personnelles ? Qui aura accès à mes données ? Pendant combien de temps vais-je conserver mes données ?
QR32	**Quelles sont les restrictions en termes d'accès et les informations fournies au client en cas de requête provenant d'une autorité administrative ou judiciaire étrangère ?** Dans certaines situations, les fournisseurs Cloud reçoivent des demandes de la part d'autorités administratives ou judiciaires étrangères afin de fournir des informations sur leurs clients. Comme détaillé dans la partie *Partie 3 - Quelques lois étrangères (Russes, chinoises et américaines*) encadrant la donnée, la transparence varie d'un fournisseur à un autre et ils ne sont pas obligés de communiquer sur ces informations (certaines demandes sont tenues par le secret des enquêtes). Dans ces cas, il faudra tenir compte de la portée des lois extraterritoriales (Ex. Cloud Act) et protéger les données sensibles / stratégiques en prenant les mesures nécessaires, soit au minimum avec un chiffrement des données ou au mieux en évitant de les stocker dans le Cloud selon la sensibilité des données.
	Les aspects techniques
QR33	**Quelle est la solution de chiffrement prévue par le prestataire pour les données, notamment les données sensibles/critiques ? (En transit, au repos ou en cours de manipulation). Même question pour les échanges sensibles (mails confidentiels)** Si vous voulez être certain que vos données sont correctement protégées, il est essentiel de comprendre : • Si le chiffrement est solide tout chiffrement inférieur à la norme de chiffrement avancée (AES) 256 bits ne sera pas suffisant Si les données sont cryptées au repos Si les données sont protégées contre le service (lecture par le Cloudeur) Les modalités de la gestion des clés de chiffrement.
QR34	**La migration est-elle réversible ?** Il est conseillé de s'assurer si on peut revenir en arrière en cas de mauvaise performance, non-compatibilité des applications, risques sécuritaires…C'est pourquoi, il est recommandé de faire des Backup. Le cas du SaaS est le plus simple et le plus compliqué à la fois. Aujourd'hui aucune norme n'existe pour l'exportation des données. Cependant, de nombreux fournisseurs de SaaS ont pensé une clause de réversibilité incluant la possibilité de réaliser à minima une extraction des données. Encore mieux, dans certains cas, l'API du fournisseur permet à des outils tiers de réaliser une migration automatisée vers un autre fournisseur. C'est le cas d'outils permettant de migrer par exemple de Salesforce.com vers Microsoft Dynamics et vice-versa.

Quelles sont les procédures de sauvegarde et de restauration des données ? Y a-t-il une redondance/copie prévue ? Si oui, sont-elles sauvegardées dans la même infrastructure de sauvegarde initiale ?

QR35

Le processus de sauvegarde dans le Cloud consiste à copier les données et à les stocker ensuite sur divers supports ou sur un système de stockage séparé qui permet un accès aisé en cas de besoin de restauration.
Voici les types de sauvegarde les plus couramment utilisés :
Sauvegarde complète
Sauvegarde incrémentielle
Sauvegarde différentielle

Il est nécessaire d'avoir un plan de reprise après incident (DR).
L'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO) sont deux mesures utilisées en DR et en cas d'incident (temps d'arrêt). (123)

Comment se passe la gestion des comptes à haut niveau de privilège ?

QR36

Pour répondre aux enjeux de sécurité du SI liés aux utilisateurs à privilèges, voici les 5 recommandations fondamentales de l'ANSSI aux RSSI/DSI :

Limiter le nombre de comptes à privilèges
Mot de passe individuel
Séparation des postes de travail (cette mesure est peu accessible aux TPE/PME)
Analyser les journaux d'évènements
Supprimer les anciens comptes

Comment sera gérée l'identification des utilisateurs et des comptes dans le Cloud ?

QR37

Généralement, les procédures de gestion des identifications des utilisateurs et des comptes dans le Cloud sont mises en place par le fournisseur, ces derniers ont développé leur propre procédure.
On peut y ajouter l'authentification multi facteurs (souvent proposée par le fournisseur) et on peut choisir aussi de mettre en place la fédération d'identité (pour les grosses PME uniquement). C'est-à-dire la possibilité d'utiliser une seule authentification sécurisée pour avoir accès à plusieurs ressources ou applications dans le Cloud.

Quelles sont nos limites de stockage dans le Cloud ?

QR38

Selon la solution Cloud choisie, l'entreprise peut allouer à ses collaborateurs un espace de stockage pour leurs données professionnelles illimité ou presque.

Comment maintenir un environnement cloud sécurisé ?

QR39

Pour maintenir un environnement sécurisé, il est essentiel de (124) :

Sécuriser la console de gestion du cloud
Sécuriser l'infrastructure virtuelle
Sécuriser les clés des API (Supervision, Gestion des identités)
Sécuriser les consoles d'administration et les outils DevOps
Sécuriser le code de la pipeline DevOps
Sécuriser les comptes administrateur pour les applications SaaS

Annexe 14
Scénario du Cabinet Conseil&ST

Cette étude de cas est propre au cabinet Conseil&ST **(entreprise fictive).** Les risques identifiés peuvent correspondre à des risques communs qu'une TPE/PME pourrait rencontrer dans le cadre d'un projet de migration Cloud, mais ils ne constituent pas une liste exhaustive de risques. D'autres risques peuvent être identifiés en fonction des activités de l'entreprise, de son écosystème et de son système d'information, ainsi que le modèle Cloud et les services identifiés…etc.

1. Description de l'entreprise Conseil&ST :

Le cabinet Conseil&ST est une PME lyonnaise dans le domaine du conseil en stratégie. Créée en 2019, la société a son siège social basé à Lyon dans lequel travaillent 44 salariés. Actuellement, elle est en phase de recrutement de personnel dans le cadre du développement de ses activités.
La société est composée d'une direction générale, d'un directeur adjoint, d'un pôle informatique avec un DSI, d'un pôle administratif et RH qui s'occupe de l'administration de la société et du recrutement, d'un pôle commercial pour la gestion commerciale et clientèle et pour finir, de Consultants.

Organigramme Conseil&ST :

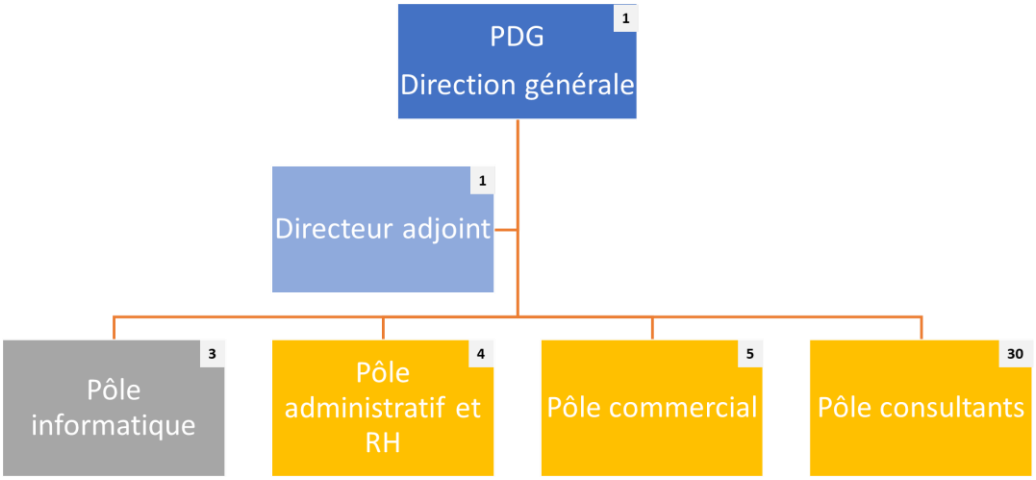


Figure 1 : Organigramme du cabinet Conseil&ST

2. Contexte et objet de l'étude :

Dans le cadre du développement de ses activités, le cabinet Conseil&ST souhaite réduire ses coûts fixes élevés liés à l'exploitation de son infrastructure On-Premise et augmenter sa productivité à travers les échanges d'informations, notamment des documents volumineux et confidentiels, entre ses salariés et ses clients.

Un audit interne du système d'information a été aussi réalisé par le DSI et son équipe. Voici la conclusion retenue sur les exigences et les points d'amélioration envisagés :

- Assurer une marge globale plus stable grâce à des coûts variables contrairement aux coûts fixes d'exploitation
- Améliorer la collaboration entre les équipes et les échanges de données sécurisés

- Gagner en flexibilité dans l'utilisation des capacités de stockage
- Instaurer un plan de continuité et de reprise des activités après sinistre.

Pour parvenir à ces résultats, l'usage du Cloud a été évoqué.

Ordre de mission :

Dans le cadre de son projet de migration Cloud, le cabinet Conseil&ST nous a sollicité afin d'effectuer une analyse de risques liés à ses données. Elle devra essentiellement traiter des risques liés à la réglementation et à la sécurité des données.

3. Analyse des risques

3.1 Objectif et étapes de l'étude

L'objectif de cette étude est de répondre à la demande du cabinet Conseil&ST. Pour cela, nous allons nous appuyer sur la méthode EBIOS Risk Manager qui est une des références en matière de management des risques liés à la sécurité de l'information.

Composée de cinq principales parties, l'analyse de risques se fera suivant le processus suivant :

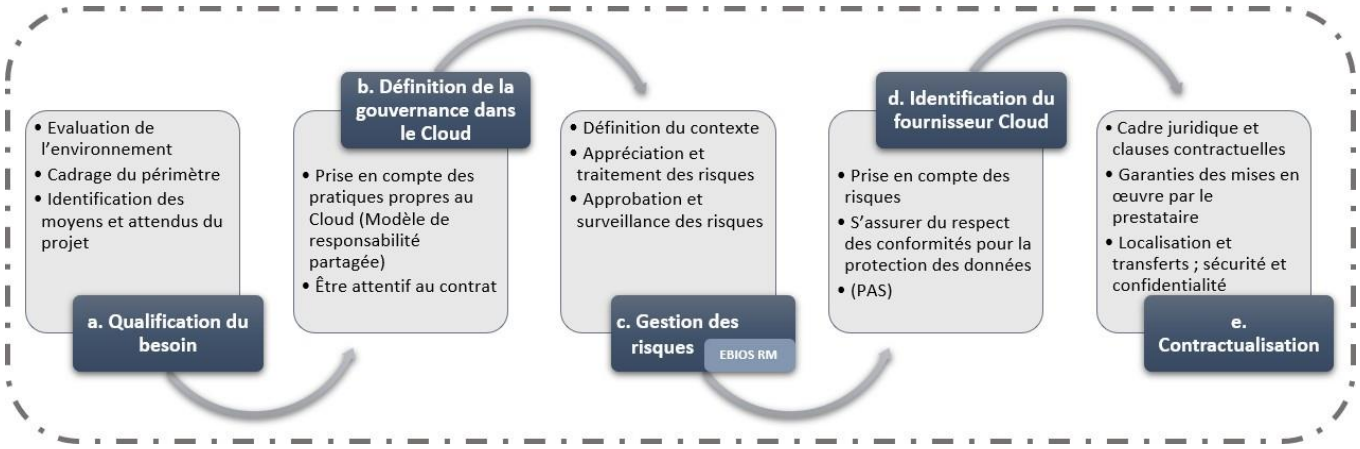


Figure 2 - Processus d'analyse de risques liés aux données dans le cadre d'un projet de migration Cloud

L'étude se fera avec le support de la Direction et quelques participants des différents services de l'organisation. En effet, il est important d'impliquer tous les métiers, ainsi que les décideurs afin de prendre compte : leurs besoins en termes d'actifs à protéger et leurs évaluations de ces derniers.

3.2 Déroulement du processus d'analyse de risques

3.2.1 Qualification du besoin

La première étape consiste à évaluer les besoins du projet de déploiement Cloud. Elle sera basée en partie sur l'étude interne réalisée par le cabinet Conseil&ST. Voici un rappel du système d'information actuel et les conclusions retenues :

Système actuel :

Les 44 postes Windows peuvent appartenir à 4 types d'utilisateurs :

- ✓ Les utilisateurs simples avec un accès limité aux données sensibles.
- ✓ Les utilisateurs managers, qui ont accès à l'ensemble des données de leur service.

- ✓ Les administrateurs systèmes qui ont un accès administrateur sur les postes de travail, les serveurs d'applications, l'Active Directory et les équipements réseau.
- ✓ Le DSI qui a un accès administrateur sur le contrôleur de domaine Active Directory et sur le Firewall.

- Le service informatique possède un serveur connecté au réseau sur lequel sont stockés les fichiers partagés entre les employés avec un dossier par service.
- Le service informatique effectue une sauvegarde du serveur une fois par semaine sur un disque dur stocké dans un coffre sécurisé à côté du serveur. Le site internet et le serveur email sont hébergés au siège.
- Toutes les données sont hébergées en local.

Prérequis : Possibilité de faire des tests en amont de la migration (analyse de la performance, latence…) ce qui permettra de confirmer les applications et services identifiés pour la migration.

Les utilisateurs des services Cloud seront des personnes internes à l'entreprise. Voici les accès qu'auraient les différentes personnes de chaque service :

Les futurs usagers du Cloud :

rvices Cloud et logiciels	PDG	irecteur adjoint	Pôle informatique	DSI	Pôle administratif et RH	Pôle commercial	Pôle consultants
pplications de bureautique (Word, Excel…)	x	x	x	x	x	x	x
Courrier électronique	x	x	x	x	x	x	x
Service RH et logiciel de paie	x	x	x	x	x	x	
Comptabilité	x	x	x	x	x	x	
.a gestion de la tion client (CRM)	x	x	x	x	x	x	
Gestion de l'identité			x	x			

Tableau 1 : Les futurs usagers des services Cloud du cabinet Conseil&ST

Audit de sécurité du système d'information :

Suite à l'audit interne réalisé par le DSI et son équipe, certains éléments pouvant compromettre les activités de l'entreprise ont été identifiés (Cf. 2. Contexte et objet de l'étude). Les principaux points à retenir sont liés aux mesures supplémentaires à mettre en place afin d'assurer un niveau plus élevé de la sécurité en termes de disponibilité, intégrité et confidentialité.

Le modèle de Cloud envisagé, type d'offre et les applications, services identifiés :

Suite à l'audit interne, des réunions entre la direction et le service informatique, en support d'un conseillé externe, ont été réalisées. Il a été proposé d'utiliser les services Cloud en mode SaaS afin de répondre aux exigences et aux besoins de Conseil&ST.
Les applications et les services identifiés et qui seraient concernés par cette solution sont :

- Applications bureautique (Word, Excel…)
- Courrier électronique et messagerie
- Service RH et logiciel de paie
- Comptabilité
- La gestion de la relation client (CRM)
- Espace de stockage partagé avec possibilité du travail collaboratif (Sharepoint)
- Gestion de l'identité
- Services de continuité et reprise des activités après sinistre

A noter que certaines applications font déjà l'objet de services en mode SaaS auprès d'un fournisseur Cloud comme le courrier électronique et la messagerie.
Un fournisseur Cloud, pour les services SaaS listés, a été identifié avec une offre Cloud public. En plus des éléments, ci-dessous, Il a été sélectionné en se basant sur sa réputation qui a été vérifiée (Due diligence).

  - Présentation des audits et de documents garantissant la sécurité de ses infrastructures. Notamment, un contrôle d'accès sécurisé, ainsi qu'une politique d'accès aux données justifiées par le besoin. L'accès sera notifié au client.
- Proposition de connexion sécurisée aux services via VPN (hors réseau entreprise)
- Conformité à la norme ISO 27001.
- Notification des violations (les rapports détaillés sont payants, comme par ex. les journaux des évènements).
- Contractuellement, les données peuvent être localisées en Europe et aux Etats-Unis.
- Mise en place de contrôle de sécurité comprenant (pare-feu, tests de pénétration, gestion des incidents…).

<u>Les données à héberger, données sensibles à protéger :</u>

Conseil&ST intervient dans le domaine de conseil et services. En plus des données internes de l'entreprise : données stratégiques, chiffres d'affaires, données personnelles des candidats…etc, elle traite principalement des données confidentielles de ses clients, principalement français, ainsi que leurs données personnelles permettant de les identifier. Les données personnelles traitées seront donc soumises au RGPD et les données stratégiques soumises au SDA.

L'entreprise déploie une classification de ses données selon les quatre niveaux :

- Confidentiel
- A usage interne restreint à un groupe d'employés
- A usage interne uniquement (accessible à tous les employés)
- Publique

<u>Maîtrise d'œuvre actuelle :</u>
La maîtrise d'œuvre actuelle n'est pas externalisée. La maintenance et la gestion du système d'information actuel sont réalisées par le DSI et son équipe. Il convient d'évaluer au préalable :

- Leurs compétences en matière de migration et utilisation des services Cloud
- Leur disponibilité tout au long du projet

Aussi, il est nécessaire de prévoir une formation de l'équipe aux services Cloud et le budget nécessaire pour avoir un support externe dans le cadre de la migration.

3.2.2 La gouvernance dans le Cloud

Il est important d'analyser le contrat proposé par le fournisseur Cloud identifié. Au vu de la taille de l'entreprise, les possibilités de négociation sont très réduites.

Aussi, une attention particulière doit être portée au niveau juridique. L'entreprise doit s'assurer que le fournisseur est en conformité avec la réglementation RGPD pour la protection des données personnelles.

Voici les points importants à prendre en compte pour l'adaptation de la gouvernance de l'entreprise au Cloud :

- Mettre en place des règles plus strictes pour les données sensibles (stratégiques, données personnelles)
- Gérer rigoureusement les rôles et les accès aux données sensibles
- Prendre en compte de la gestion financière pour le suivi des dépenses dans le Cloud afin d'éviter les mauvaises surprises
- Automatiser, dans la mesure du possible les processus afin de garantir une détection plus facile des violations de politiques de sécurité (Ex. système automatisé d'alerte pour les accès non autorisés)
- Vérifier au niveau du contrat et des CGU la gestion des données, le niveau de SLA et la possibilité de réversibilité/interopérabilité.

3.2.3 La gestion des risques

Identification des actifs et des besoins de sécurité :

Cette étape fait partie de l'Atelier 1 de la méthode EBIOS RM. L'objectif est d'identifier les missions de l'entreprise et d'évaluer les actifs et les biens supports.

Voici la liste des participants et des personnes sollicitées aux différentes étapes :

Les étapes de la gestion des risques	DSI	Représentants métiers/utilisateurs (les différents pôles)	Direction
Identification des actifs et des besoins de sécurité - Atelier 1 EBIOS RM	x	x	x
Identification des évènements redoutés et scénarios opérationnels - Atelier 1 EBIOS RM	x	x	x
Scénarios opérationnels - Atelier 4 EBIOS RM	x	x	
Traitement des risques identifiés - Atelier 5 EBIOS RM	x	x	x

Tableau 2 : Liste des participants aux différentes étapes d'analyse des risques

L'ensemble des missions et des valeurs métiers de la société Conseil&ST sont listées dans ce tableau :

Missions	Conseil et services			
Dénomination de la valeur métier	estion système informatique	ités de conseil et de services	dministratives et RH	Activités commerciales
Nature de la valeur métier (processus ou information)	Processus	Information	Information	Information
Description	Gestion des identités et des accès	Activités consistant à réaliser : - Rédaction de présentations et de documents divers d'analyse pour les entreprises - Traitement des courriers (envoie et réception, interne et externe)	Activités consistant à réaliser : - Rédaction des rapports et documents divers (contrats...) - Gestion et contrôle de la paie - Recherche de candidats, entretiens et recrutement - Traitement des courriers (envoie et réception, distribution aux différents services) - Commandes et gestion du stock de fournitures diverses	Activités consistant à réaliser : - La prospection de nouveaux clients - Les négociations des contrats
Entité ou personne responsable (INTERNE)	DSI	Expert-conseil	ministratif / RH	Responsable commercial
Dénomination du/des biens supports associés	Logiciel de gestion des identités 1 Ordinateurs portables	- Logiciels bureautiques (outils collaboratifs) - Courrier électronique et messagerie - Logiciel de gestion de la relation client (CRM) 30 Ordinateurs portables	- Logiciels bureautiques (outils collaboratifs) - Logiciel de paie - Logiciel de gestion de la relation client (CRM) - Courrier électronique et messagerie 4 Ordinateurs de bureau	- Logiciels bureautiques (outils collaboratifs) - Logiciel de paie - Logiciel de gestion de la relation client (CRM) - Courrier électronique et messagerie 5 Ordinateurs portables

Description	- Les logiciels de gestion des identités - Courrier électronique et messagerie	- Logiciels/applications bureautiques et collaboratifs permettant de stocker les données (rédaction de textes, calculs, gestion de données…) - Logiciel de gestion de la relation client (CRM) permettant la consultation des coordonnées et les informations sur les clients - Courrier électronique et messagerie pour la communication interne / externe	- Logiciel de paie permettant de calculer et d'établir les fiches de paie - Logiciels/applications bureautiques et collaboratifs permettant de stocker les données (rédaction de textes, calculs, gestion de données…) - Logiciel de gestion de la relation client (CRM) permettant l'édition des contrats et de répertorier les coordonnés des clients - Courrier électronique et messagerie pour la communication interne / externe	- Logiciel de gestion de la relation client (CRM) permettant l'édition des contrats et de répertorier les coordonnés des clients - Logiciel de paie permettant de calculer les coûts/budgets - Logiciels/applications bureautiques et collaboratifs permettant de stocker les données (rédaction de textes, calculs, gestion de données…) - Courrier électronique et messagerie pour la communication interne / externe
Entité ou personne responsable (INTERNE)	DSI	Expert-conseil	inistratif et RH	irecteur de proximité

Tableau 3 : Les missions et les valeurs métiers de la société Conseil&ST

Liste des actifs de la société Conseil&ST :

Actifs d'information	Patrimoine intellectuel : - Documents internes (contrats, fiche de paie…) - Documents contenants des informations des clients (Stratégie, contrats, devis, porte feuille client,…). Ces documents contiennent : Des données personnelles des clients et des salariés Des données stratégiques de l'entreprise - Journaux d'événements opérationnels/de sécurité
Actifs applicatifs	- Logiciels de bureautique - Application de courrier électronique et messagerie - Logiciels de comptabilité et de paie - Logiciel de gestion de la relation client CRM - Contrôle d'accès et interface de gestion des applications - Site internet Conseil&ST

- Sharepoint)		Application collaborative (stockage, partage de fichier..type
Actifs humains	-	Personnels décideurs (de direction)
	-	Personnels utilisateurs des différents pôles (salariés)
Actifs immatériels	-	Image de la société et confiance des clients
	-	Lien social interne (loyauté des employés et engagement)
Actifs physiques	-	Ordinateurs portables et stations fixes
Actifs financiers	-	Chiffre d'affaires
	-	Revenus

Tableau 4 : Les actifs de la société Conseil&ST

Dans le cadre d'un projet de migration dans le Cloud de type « SaaS », les actifs essentiels qui seront au cœur de la préoccupation de l'entreprise seraient les données à traiter. Elles sont sous la responsabilité du client.

Ci-dessous, les actifs identifiés comme précieux aux yeux de l'entreprise, ainsi que les besoins en termes de sécurité des données selon l'échelle suivante :

Niveau	Disponibilité	Intégrité	Confidentialité	Traçabilité
1	e disponibilité requise	Pas d'intégrité nécessaire	Les données sont accessibles publiquement	Pas de traçabilité nécessaire
2	La donnée ou le système ne peut être indisponible plus d'une semaine	grité doit être connue	accès doit être limité aux employés uniquement	Traçabilité nécessaire pour des besoins de qualité ou techniques
3	La donnée ou le système ne peut être indisponible plus d'une journée	L'intégrité doit être connue et récupérable	L'accès doit être limité à un groupe restreint d'employés uniquement	Traçabilité nécessaire pour des besoins métiers ou contractuels
4	La donnée ou le système ne peut être indisponible plus d'une heure	grité doit être garantie	doit être interdit pour tous.	Traçabilité nécessaire pour des besoins légaux ou réglementaires

Tableau 5 : Echelle d'évaluation des besoins de sécurité des données – Atelier 1 – Conseil&ST

Actifs	Disponibilité	Intégrité	Confidentialité	Traçabilité
ntrats et portefeuille client, fichier relation clientèle, liste, contacts	3	4	3	4
gestion de l'identité et des accès	4	4	4	4

Site internet Conseil&ST	**3**	**4**	**1**	**4**
Base de données RH contenant les informations personnelles des salariés et les fiches de paie des salariés	**2**	**4**	**3**	**4**
s informations d'études pour le conseil et services des clients	**4**	**4**	**3**	**4**

Tableau 6 : Evaluation des actifs importants selon le critère (DICT)

Identification des évènements redoutés :

Cette étape fait également partie de l'Atelier 1. Elle consiste à identifier les évènements redoutés (ER). Sous forme de scénarios, l'objectif est de permettre de comprendre facilement le préjudice lié à l'atteinte de la sécurité de l'information.

Le degré de l'impact est évalué selon une échelle de gravité :

G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégrade).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégrade).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Tableau 7 : Echelle de gravité ER EBIOS RM – Atelier 1

Les impacts identifiés sont (ils ne sont pas triés selon leur gravité) :

Références des impacts	Impacts
IMPACT_1	Impact sur l'image de l'entreprise et la confiance des clients
IMPACT_2	Impact sur les missions et services de l'organisme
IMPACT_3	Impact financier
IMPACT_4	Impact sur le patrimoine intellectuel
IMPACT_5	Impact matériel (Destruction de biens supports)
IMPACT_6	Impact juridique

IMPACT_7	Impact sur le lien social interne (Perte de confiance des employés dans la pérennité de l'organisme et baisse de l'engagement)
IMPACT_8	Impact culturel (perte de ressources humaines clés)
IMPACT_9	Impact sur la capacité de développement ou de décision

Tableau 8 : Liste des impacts

Les critères de sécurité des données, utilisés sont :

- La disponibilité **(D)** : Données (ou systèmes donnant accès) inaccessibles ou perdues
- L'intégrité **(I)** : Modification des données ou détournement d'usage d'un service
- La confidentialité **(C)** : Divulgation d'informations, accès non autorisé, compromission de secret
- La traçabilité **(T)** : Impossibilité de tracer la modification d'une information

Réf (ER)	Evènement redouté	Impacts	Gravité	DICT ntiellement atteint)
ER1	fuite des informations clients (coordonnées, contrats)	IMPACT_1 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6 ; IMPACT_7 ; IMPACT_9	G3	(C)
ER2	les comptes/autorisations d'accès	IMPACT_1 ; IMPACT_3 ; IMPACT_4 (Données de gestion des services Cloud, Données sensibles : stratégiques / personnelles) IMPACT_5 ; IMPACT_6 ; IMPACT_7 ; IMPACT_8	G4	(D) (I) (C) (T)
ER3	Défiguration du site internet de l'entreprise	MPACT_1 ; IMPACT_3 ; IMPACT_4 ; IMPACT_7	G2	(D) (I)
ER4	Destruction de la base de données RH contenant les informations personnelles des salariés et les fiches de paie des salariés	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_7 ; IMPACT_8	G3	(D)
ER5	Vol et destruction des informations d'études pour le conseil et services des clients contenant des informations confidentielles sur leur entreprise	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6 ; IMPACT_7 ; IMPACT_8 ; IMPACT_9	G4	(D) (C)
ER6	Perte de contrôle et de conformité aux exigences de sécurité (Manque de transparence de la part du fournisseur Cloud. Négligence et/ou mauvaise interprétation des responsabilités définies dans le contrat.)	IMPACT_1 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6 ; IMPACT_7 ; IMPACT_8 ; IMPACT_9	G4	(D) (I) (C) (T)

ER7	Changements de juridiction	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G4	(D) (C)
ER8	pect de la réglementation sur la protection des données	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G4	(C)
ER9	Verrouillage du fournisseur Cloud	MPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4	G4	(D)
ER10	(s) seule(s) sauvegarde(s) existante(s)	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6	G4	(D)

Tableau 9 : Les (ER) avec évaluation des impacts et selon le critère de sécurité (DICT)

Scénarios opérationnels :

Cette étape fait partie de l'atelier 4. A partir des évènements redoutés, l'objectif est d'élaborer des scénarios opérationnels (SO) que pourraient exploiter les sources de risques pour atteindre leurs objectifs. Ensuite, l'évaluation de la vraisemblance sera faite, en prenant en compte la gravité des impacts. Ces deux paramètres permettront de définir la criticité des risques par la suite.

Les sources de risques (SR) identifiées sont :

- Amateur / Individu isolé
- Salarié
- Hacktiviste
- Hacker
- Fournisseur

Les (SR) peuvent aussi provenir d'un manquement au niveau règlementaire, d'une non-conformité ou d'un non- respect des mesures de sécurité liés aux données.

Voici l'échelle utilisée pour l'évaluation de la vraisemblance des scénarios, ainsi que le tableau des (SO) correspondant aux risques identifiés :

V1 **Peu vraisemblable**	ue a très peu de chance d'atteindre son objectif visé en empruntant un des modes opératoires.
V2 **Vraisemblable**	risque est susceptible d'atteindre son objectif visé en empruntant un des modes opératoires.
V3 **Très vraisemblable**	isque va probablement atteindre son objectif visé en empruntant un des modes opératoires.

V4 quasi certain	risque va certainement atteindre son objectif visé en empruntant un des modes opératoires.

Tableau 10 : Echelle d'évaluation de la vraisemblance

Réf SO	stratégique associé au scénario opérationnel	Vraisemblance
SO1	Un attaquant se rapproche de l'un des employés de l'entreprise (ayant un accès aux données sensibles des clients), récupération de ses identifiants de connexion aux services Cloud via ingénierie social/Phishing. Vol et divulgation des données sensibles des clients	V2 - Vraisemblable
SO2	Vol ou divulgation des données stratégiques de l'entreprise par un salarié mécontent. Suite à une mauvaise gestion des accès, ce dernier avait accès par erreur à des répertoires contenant des données sensibles	V3 - Très vraisemblable
SO3	u site internet de l'entreprise par un Hacktiviste	V2 - Vraisemblable
SO4	Accès et altération/suppression des données RH (Fiches de paie, données personnelles des salariés…) par un employé mécontent de l'entreprise qui n'est pas censé accéder à ces données sensibles non classifiées	V3 - Très vraisemblable
SO5	Destruction des données d'étude destinées aux clients par un Hacker suite à une attaque par injection SQL (Méthode "Stacked queries" ou autres) sur les services du fournisseur Cloud --> Exploitation d'une faille au niveau des mécanismes de séparation du stockage dans le Cloud Public permettant d'accéder à la base de données	V3 - Très vraisemblable
SO6	Négligence et/ou mauvaise interprétation des responsabilités définies dans le contrat OU Manque de transparence de la part du fournisseur Cloud (sur les fonctionnalités, localisation pour le stockage des données...). Exemples de cas : Chiffrement non compris dans le contrat --> mauvaise interprétation du client. Le client qui croit que le fournisseur Cloud est responsable de toute la sécurité des données alors que ce n'est pas compris dans le contrat --> mauvaise interprétation du client. Le fournisseur Cloud sous-traite le chiffrement des données à un prestataire qui ne fournit pas les mêmes garanties initialement annoncées --> manque de transparence.	V3 - Très vraisemblable

SO7	Des données sensibles qui se retrouvent stockées dans un pays avec une juridiction différente et qui ne respecte pas les accords internationaux, ou la protection des données personnelles par exemple. Ou qui pourraient avoir accès ou saisir le matériel physique sans même avoir besoin d'une enquête.	**V4 - quasi certain**
SO8	Le fournisseur Cloud ne respecte pas la législation sur la protection des données personnelles, volontairement ou en perdant tout simplement le contrôle sur le traitement des données.	**V3 - Très vraisemblable**
SO9	Impossibilité d'exporter les applications existantes vers un autre fournisseur Cloud, ainsi que toutes les données au format standard (ou alors cela demanderait beaucoup de temps et un budget conséquent).	**V3 - Très vraisemblable**
SO10	ndie au niveau de l'infrastructure du fournisseur Cloud entraînant la perte de la sauvegarde des données	**V2 - Vraisemblable**

Tableau 11 : Les (SO) correspondant aux (ER) identifiés

Traitement des risques identifiés :

Cette partie présente le dernier Atelier 5 de l'EBIOS RM. Elle consiste à réaliser une synthèse des scénarios des risques identifiés, de définir la stratégie de traitement des risques, ainsi que les mesures de sécurité à mettre en place dans le cadre d'un plan d'amélioration continue de la sécurité.

Dans le cadre de notre étude, nous allons définir les mesures de sécurité pour le traitement des risques les plus élevés et réaliser ensuite une synthèse des risques résiduels. Des recommandations seront définies pour se protéger des risques identifiés.

Rappelons que les risques identifiés sont principalement liés à la sécurité des données et à la réglementation autour de ces dernières.

Synthèse des scénarios de risques :

Ci-dessous, les scénarios des risques identifiés avant traitement (initiaux) catégorisés, ainsi que leur matrice.

Le tableau suivant présente l'échelle choisie pour le seuil d'acceptation à trois niveaux :

Niveau du risque	Acceptabilité du risque	Intitulé des décisions et des actions
Faible	Acceptable en l'état	Aucune action n'est à entreprendre
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme

Elevé	Inacceptable	Des mesures de réduction du risque doivent impérativement être prises à court terme

Tableau 12 : Echelle d'acceptabilité des risques à trois niveaux

Réf. Risque	égories des risques	Risques	veau du risque	Sources de risque	(ER)	Gravité	(SO)	Vraisemblance
R1	Autres risques	Attaque avec usurpation d'identité (ingénierie sociale)	Moyen	Amateur / Individu isolé	ER1	G3	SO1	V2
R2	Risques liés aux vulnérabilités techniques	Mauvaise gestion des comptes/autorisations d'accès	Elevé	Salarié	ER2	G4	SO2	V3
R3	Autres risques	Attaque avec injection SQL (Défacement site web de l'entreprise)	Faible	Hacktiviste	ER3	G2	SO3	V2
R4	Autres risques	Accès aux données sensibles (personnelles, stratégiques) suite à une erreur ou absence de classification des données	Elevé	Salarié	ER4	G3	SO4	V3
R5	Risques liés aux vulnérabilités techniques	Défauts d'isolement des ressources	Elevé	Hacker	ER5	G4	SO5	V3
R6	Risques liés à la réglementation et la non-conformité	Perte de contrôle et de conformité aux exigences de sécurité	Elevé	Fournisseur	ER6	G4	SO6	V3
R7	Risques liés à la réglementation et la non-conformité	Changements de juridiction	Elevé	Fournisseur	ER7	G4	SO7	V4
R8	Risques liés à la réglementation et la non-conformité	Non-respect de la réglementation sur la protection des données	Elevé	Fournisseur	ER8	G4	SO8	V3

R9	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Verrouillage du fournisseur Cloud	Elevé	Fournisseur	ER9	G4	SO9	V3
R10	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Perte ou vol de(s) seule(s) sauvegarde(s) existante(s)	Moyen	Fournisseur	ER10	G4	SO10	V2

Tableau 13 : Liste des risques avant traitement

Matrice des risques avant traitement :

Vraisemblance / Gravité	V1 Peu vraisemblable	V2 Vraisemblable	V3 Très vraisemblable	V4 quasi certain
G1 MINEURE				
G2 SIGNIFICATIVE		R3		
G3 GRAVE		R1	R4	
G4 CRITIQUE		R10	R2 ; R5 ; R6 ; R8 ; R9	R7

Tableau 14 : Matrice des risques avant traitement

Stratégie de traitement des risques et mesures de sécurité :

La stratégie de traitement des risques consiste à choisir une option appropriée afin d'éviter, réduire, transférer ou accepter le risque :

- L'éviter permet d'en supprimer la cause en éliminant totalement l'incertitude
- Le réduire l'amène à un niveau acceptable en minimisant la probabilité d'occurrence
- Le transférer à une tierce partie qui est principalement une assurance qui en supporterait les conséquences
- L'accepter ne demande aucune action mais nécessite une supervision

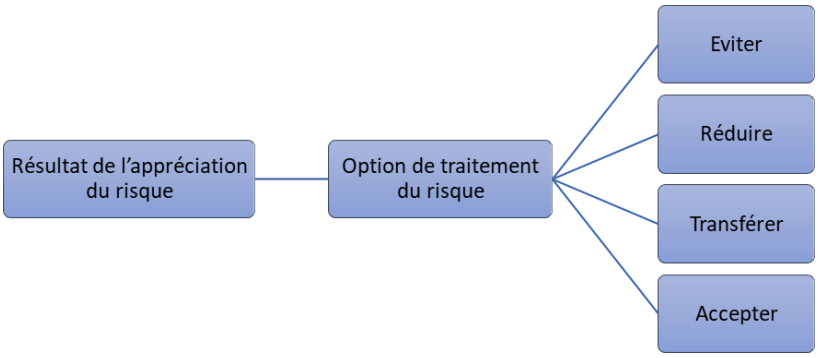


Figure 3 : Stratégie de traitement des risques

Suite au traitement des risques identifiés, il a été proposé de transférer le risque (R5) au fournisseur et de réduire le risque (R4). Ainsi, leur criticité est passée d'un niveau élevé à un niveau moyen.

Voici la synthèse des risques après traitement, ainsi que les recommandations des mesures de sécurité à mettre en place pour chaque risque.

Vraisemblance / Gravité	V1 Peu vraisemblable	V2 Vraisemblable	V3 Très vraisemblable	V4 quasi certain
G1 MINEURE				
G2 SIGNIFICATIVE		R3		
G3 GRAVE		R1 ; R4		
G4 CRITIQUE		R10 ; R5	R2 ; R6 ; R8 ; R9	R7

Tableau 15 : Matrice des risques après traitement

Réf. Risque	Catégories des risques	Risques	Niveau du risque	Traitement	Gravité	Vraisemblance	Traitement du risque / Mesures de sécurité
R1	Autres risques	Attaque avec usurpation d'identité (ingénierie sociale)	Moyen		G3	V2	- Sensibilisation des salariés aux bonnes pratiques et des risques Cyber. - Mise en place d'une charte informatique - Mise en place d'une authentification renforcée (authentification multi facteurs) - Protection renforcée des données sensibles avec un chiffrement par exemple et une détection des violations d'accès
R2	Risques liés aux vulnérabilités techniques	Mauvaise gestion des comptes/autorisations d'accès	Elevé		G4	V3	Généralement, les procédures de gestion des identifications des utilisateurs et des comptes dans le Cloud sont mises en place par le fournisseur, ces derniers ont développé leur propre procédure. On peut y ajouter l'authentification multi facteurs et on peut choisir aussi de mettre en place la fédération d'identité. C'est-à-dire la possibilité d'utiliser une seule authentification sécurisée pour avoir accès à plusieurs ressources ou applications dans le Cloud. Pour répondre à aux enjeux de sécurité du SI liés aux utilisateurs à privilèges, voici les 5 recommandations fondamentales de l'ANSSI aux RSSI/DSI : - Limiter le nombre de comptes à privilèges - Mot de passe individuel - Séparation des postes de travail - Analyser les journaux d'évènements - Supprimer les anciens comptes
R3	Autres risques	Attaque avec injection SQL (Défacement site web de l'entreprise)	Faible		G2	V2	- Procéder à un audit des stratégies de sécurité - Anticiper ce type d'attaque avec une mise en situation et préparation des réponses à apporter

R4	Autres risques	Accès aux données sensibles (personnelles, stratégiques) suite à une erreur ou absence de classification des données	Moyen	**Réduire**	G3	V2	Les fournisseurs disposent généralement du savoir-faire et des meilleurs outils pour assurer la sécurité et réduire les risques humains. Il faut bien comprendre les politiques de protection que le fournisseur pourrait offrir. L'objectif étant de limiter les accès aux données sensibles, les politiques doivent indiquer les mesures à mettre en place pour contrôler les accès et pour détecter, voir bloquer les accès non autorisés. A cela, s'ajoute la classification efficace des données sensibles avec les différents niveaux d'accès selon la confidentialité des données dont l'entreprise est responsable
R5	Risques liés aux vulnérabilités techniques	fauts d'isolement des ressources	Moyen	**Transférer**	G4	V2	Généralement, les fournisseurs mettent en place les mesures nécessaires afin de garantir une isolation stricte entre les ressources partagées des clients d'un Cloud public. Cela permet de réduire / d'éviter le risque d'exploitation d'application ou de machines virtuelles appartenant à d'autres et de voir ses données compromises. Le fournisseur doit ainsi vous mettre à disposition une description détaillée des outils mis en place et garantissant que personne ne peut accéder à vos données (intentionnellement ou pas). L'une des solutions proposées, est l'utilisation d'un annuaire (Active Directory) et d'un contrôle d'accès. Ces derniers sont gérés à plus haut niveau par le fournisseur et permettent l'isolation des données et des informations d'identité des clients. Chaque utilisateur ou administrateur ne peut accéder qu'à son propre système isolé et peut gérer à ce niveau les rôles et les droits d'accès aux différentes informations et applications.

R6	Risques liés à la réglementation et la non-conformité	Perte de contrôle et de conformité aux exigences de sécurité	Elevé		G4	**V3**	La répartition des responsabilités et des rôles doit être clairement défini dans le contrat. Selon le type de service Cloud, la répartition des responsabilités entre les parties prenantes varie grandement. Les TPE/PME n'ont généralement pas de possibilité de négociation, elles doivent donc vérifier en détail les items dont ils sont responsables. Pour les offres SaaS les responsabilités sont déléguées en grande partie au fournisseur Cloud (voir partie/figure). Dans le cadre de la continuité et la reprise des activités suite à un incident, il est nécessaire d'avoir au minimum des accords sur les niveaux de services et des informations sur la durée minimale de disponibilité des systèmes, ainsi que la gestion et la réponse aux incidents. Il est donc primordial de savoir en amont si le fournisseur maintient un processus détaillant : • Les moyens de communication, ainsi que les rôles et les responsabilités lors de la gestion de l'incident Les criticités des services avec leur RPO et RTO (Définition existante dans le doc ?) • La prise en compte des priorités du client durant la restauration et si cette dernière prend en compte la sécurisation des données La possibilité d'avoir un site secondaire si le site initial est indisponible Le processus de détection, d'analyse et de réponse aux incidents. Ainsi que la méthode de test du processus. • Les tests de reprise et de continuité des activités, les tests de vulnérabilité et leur fréquence, ainsi que l'implication du client dans le processus. Les accords de niveau de service mis en place (SLA), entre le fournisseur et le client, protégeraient le client en cas de perturbation des services fournis. En cas de non-respect de ces accords, le fournisseur s'exposerait à des pénalités

R7	Risques liés à la réglementation et la non-conformité	ıngements de juridiction	Elevé		G4	V4	Il est très important de savoir les pays par lesquels les données vont transiter et où est-ce qu'elles seraient stockées physiquement. Il faut garder à l'esprit que différentes réglementations seront appliquées aux données : selon les lois locales du pays de stockage ou encore selon les lois du pays auxquelles les responsables de traitement dépendent. Les obligations en termes de respect des lois dépendront aussi du type de données traitées. Par exemple, pour le transfert des données personnelles, il faudrait s'assurer que les pays concernés garantissent un niveau de protection à travers leur droit national ou les accords internationaux qu'ils ont signés. Le cas échéant, le client souhaitant transférer les données doit fournir les garanties adéquates prouvant le respect des droits et de la protection de données des personnes concernées. En outre, étant donné l'évolution du cadre juridique international (Ex. invalidation Shrems 1 ; Shrems 2), il est essentiel de contrôler les lois auxquelles le client dépendra et bien comprendre son implication. Les fournisseurs peuvent disposer de sites de secours en cas de nécessité, les mêmes questions doivent être posées pour définir les réglementations applicables dans cette situation.
R8	Risques liés à la réglementation et la non-conformité	Non-respect de la réglementation sur la protection des données	Elevé		G4	V3	Il faut s'assurer que le fournisseur est en conformité avec la réglementation en vigueur selon le lieu de stockage et traitement des données.

R9	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Verrouillage du fournisseur Cloud	Elevé		G4	**V3**	Il est important de pouvoir garder le contrôle sur ses données et d'éviter de se retrouver dépendant du fournisseur Cloud. Il est primordial de s'assurer de la réversibilité et de l'interopérabilité, respectivement des données et des applications. En d'autres termes, il faut être capable de pouvoir exporter les données et les transférer chez un autre fournisseur Cloud sans rupture de service. Et de s'assurer que les systèmes du fournisseur sont compatibles avec d'autres systèmes comme les logiciels libres par exemple ou avec les solutions utilisées dans un Multicloud. Il est conseillé de s'assurer si on peut revenir en arrière en cas de mauvaise performance, non-compatibilité des applications, risques sécuritaires… C'est pourquoi, il est recommandé de faire des Backup, opter pour du multicloud, l'interopérabilité des applications dans les différents écosystèmes Cloud. Le cas du SaaS est le plus simple et le plus compliqué à la fois. Aujourd'hui aucune norme n'existe pour l'exportation des données. Cependant, de nombreux fournisseurs de SaaS ont pensé une clause de réversibilité incluant la possibilité de réaliser à minima une extraction des données. Encore mieux, dans certains cas, l'API du fournisseur permet à des outils tiers de réaliser une migration automatisée vers un autre fournisseur. C'est le cas d'outils permettant de migrer par exemple de Salesforce.com vers Microsoft Dynamics et vice-versa.

R10	Risques liés aux fournisseurs (et tiers / clients parties prenantes)	Perte ou vol de(s) seule(s) sauvegarde(s) existante(s)	Moyen		G4	V2	Le processus de sauvegarde dans le Cloud consiste à copier les données et à les stocker ensuite sur divers supports ou sur un système de stockage séparé qui permet un accès aisé en cas de besoin de restauration. Voici les types de sauvegarde les plus couramment utilisés : Sauvegarde complète Sauvegarde incrémentielle Sauvegarde différentielle Il est nécessaire d'avoir un plan de reprise après incident (DR). L'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO) sont deux mesures utilisées en DR et en cas d'incident (temps d'arrêt). Il faut s'assurer de la disposition d'une autre sauvegarde dont les données ne sont pas stockées dans le même endroit que la sauvegarde initiale.

Tableau 16 : Liste des risques après proposition du traitement

Figure 4 : Cartographie des risques après proposition du traitement

4. Conclusion :

Suite à l'analyse de risques, cinq risques résiduels ont été maintenus et évalués avec un niveau élevé. Il convient à l'entreprise de prendre en compte ces risques et de s'assurer de mettre en place les contre-mesures adéquates avant de procéder au choix final du fournisseur et à la contractualisation.
Nous rappelons que le Cloud est basé sur un modèle de responsabilité partagée. L'entreprise est le responsable du traitement des données. Le fait d'externaliser certaines opérations ou de transférer les risques au fournisseur ne la dédouane en aucun cas de ses responsabilités, surtout au niveau des potentiels impacts suite aux risques identifiés : juridique, financier et atteinte à son image.

Voici les principales recommandations à retenir pour faire suite à cette étude :

- L'entreprise doit s'assurer de l'interopérabilité et de la réversibilité des données/applications, afin de garder le contrôle sur ses données
- Sensibiliser ses salariés aux potentiels risques
- Prévoir des formations aux utilisateurs, surtout aux administrateurs qui sont responsables de la gestion des accès afin d'éviter les mauvaises configurations
- Avoir une politique efficace de la gestion et de la classification des données
- Chiffrement des données sensibles
- Prévoir un plan de continuité et reprise des activités
- Avoir une stratégie de surveillance des risques avec une revue périodique et communiquer aux utilisateurs toute évolution
- Adapter sa gouvernance au Cloud

Annexe 15
Exemple d'Etude des Risques liés à la Sécurité de l'Information

Analyse des Risques du SSI

BSI CONSULTING

METHODE EBIOS RM

Date :04/12/2022
Statut :Approuvé
Classification :Diffusion restreinte
Nombre de pages :20
Responsable des travaux :TotoRisk
Validation :Groupe de travail
Approbation :Conseil d'administration

1. ORDRE DE MISSION

BSI-Consulting SAS est une PME parisienne dans le domaine de conseil en sécurité-sûreté et services, créée le 02 novembre 2020. La société a son siège à Paris où travaillent 30 personnes. Par ailleurs, elle est en phase de recrutement de personnel sur la zone Afrique dans le cadre du développement de ses activités.
La société est composée d'une direction générale, d'une direction de proximité et d'un RSSI, d'un pôle administratif qui s'occupe de l'administration de la société, d'un pôle commercial qui communique avec les clients, d'un pôle production qui s'occupe de la fabrication des puces et matériels technologiques et d'un pôle contrôle/qualité.
Le SI de BSI-Consulting est constitué de :

- 30 postes de travail Windows
- Un serveur Windows contrôleur de domaine Active Directory
- Un serveur d'application métier et de fichiers Windows
- Un serveur web et email Linux
- Un Firewall
- Trois Switch réseau
- Un routeur connecté à Internet

Les postes d'ordinateur sont répartis selon 4 types d'utilisateurs :

1. Les utilisateurs simples avec un accès limité de données
2. Les utilisateurs managers, qui ont accès à l'ensemble des données de leur service
3. Les administrateurs systèmes qui ont un accès administrateur sur les postes de travail ainsi que sur les serveurs (Active Directory, serveur d'application et de fichier, serveur web) et les équipements réseau.
4. Le responsable sécurité du système d'information (RSSI) a un accès administrateur sur le contrôleur de domaine Active Directory et sur le Firewall.

5. Le service informatique possède un serveur connecté au réseau sur lequel sont stockés les fichiers partagés entre les employés avec un dossier par service.

6. Chaque employé utilise un compte administrateur sur son ordinateur.

7. Le service informatique effectue une sauvegarde du serveur une fois par semaine sur une clé USB stockée dans un coffre sécurisé à côté du serveur. Le site internet et le serveur email sont hébergés au siège.

8. BSI-Consulting héberge en local, toutes ses données.

Dans un contexte de développement, la société souhaite se mettre en conformité avec la réglementation RGPD. Elle souhaite également réduire les coûts liés au système d'information en prévoyant une possibilité de migration dans le Cloud. **V**ous êtes embauché en tant que RSSI afin d'améliorer la sécurité du système d'information. Le PDG de BSI-Consulting vous demande de procéder à l'analyse des risques liés au système d'information.

2. Introduction

La société BSI-Consulting souhaite réaliser un audit de sécurité de son système d'information pour révéler d'éventuelles failles ou dysfonctionnements qui pourraient compromettre ses activités. Nous interviendrons afin de réaliser cet audit. Il est évident que nous nous adapterions à la structure même de l'entreprise pour définir ses objectifs. De ce fait, il pourrait en découler un nombre limité de risques à prioriser. Nous avons conscience que le budget peut être limité, il faudra donc investir les ressources à bon escient. Après un inventaire des risques

éventuels, il est nécessaire de les étudier et d'évaluer leur gravité potentielle, et enfin décider des actions préventives à mettre en place.

3. Contexte (structurel)

La société BSI-Consulting souhaite vérifier si ses objectifs de sécurité de son système d'information sont bien mis en œuvre, afin d'y apporter des améliorations et de se mettre en conformité avec la réglementation RGPD. Elle souhaite également réduire les coûts liés au système d'information tout en prévoyant une possibilité de migration dans le Cloud.
Le PDG de BSI-Consulting nous demande de procéder à l'analyse des risques informatiques de la société.
Dans un premier temps, nous détaillerons la structure du système d'information (SI). Il est ainsi constitué de : 30 postes de travail Windows, 1 serveur Windows contrôleur de domaine Active Directory, 1 serveur d'application métier et de fichiers Windows, 1 serveur web et email Linux, 1 Firewall, 3 Switch réseau, 1 routeur connecté à Internet.
Pour définir les objectifs ainsi que les risques, nous nous appuierons sur l'organisation de BSI-Consulting : la direction générale, l'architecture de son système informatique, son organigramme, les métiers, etc. Elle sera le socle même de notre étude.
Nous pouvons convenir d'identifier ce qui doit être protégé, de formuler des objectifs de sécurité et d'identifier, arbitrer et mettre en œuvre les mesures adaptées au juste niveau de sécurité retenu.

4. Objet du document

Le management des risques est un processus permanent qui irrigue toute organisation. Il est mis en œuvre par l'ensemble des collaborateurs, à tous les niveaux de l'organisation, en particulier au niveau du système d'information.
Le management des risques informatiques est un outil indispensable pour toute entreprise soucieuse de sa sécurité. Il permet d'obtenir une vision globale de l'exposition du système d'information aux risques et d'adopter les mesures nécessaires pour y remédier.
Dans un contexte de développement, BSI-Consulting décide de se mettre en conformité avec les référentielles de gestion liés à la sécurité des SSI, tout en réduisant les coûts. Le PDG de BSI-Consulting nous confie la mission en tant que RSSI de procéder à l'analyse des risques du système d'information de l'entreprise.

Pour cela, nous allons nous appuyer sur :

- la méthode EBIOS RM :
- Sur les recommandations CNIL/RGPD
  - ISO 31000, la pile ISO 270XX (27001, 27005, 27017, 27018, etc).

5. Présentation de la société

BSI-Consulting SAS est une PME parisienne dans le domaine de conseil en sécurité-sûreté et fabrication des puces et matériels technologiques. Créée le 02 novembre 2020, la société a son siège à Paris où travaillent 30 personnes. Par ailleurs, elle est en phase de recrutement de personnel sur la zone Afrique dans le cadre du développement de ses activités.

La société est composée d'une direction générale, d'une direction de proximité et d'un RSSI ; d'un pôle administratif qui s'occupe de l'administration de la société, d'un pôle commercial pour la gestion commerciale et clientèle, d'un pôle production et d'un pôle contrôle/qualité.

6. Organigramme BSI - Consulting

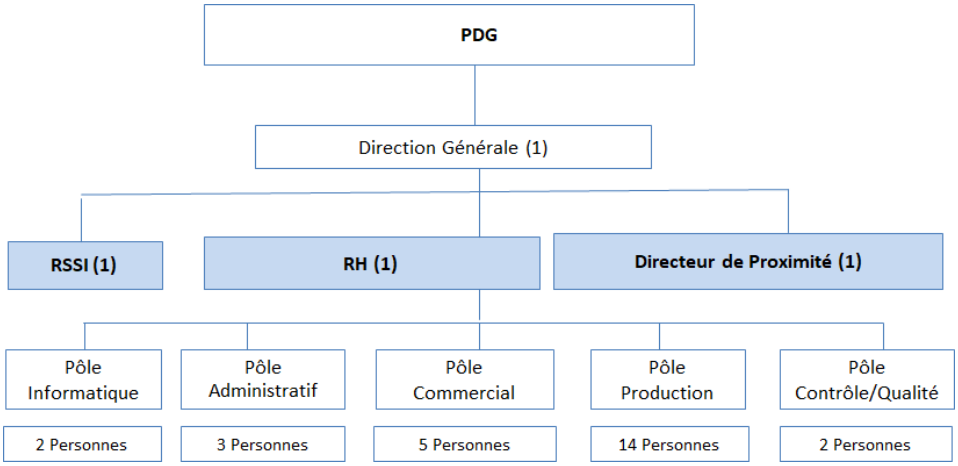


Figure 1 : Organigramme BSI – Consulting

7. L'architecture du système informatique

L'architecture du système informatique de la société est comme suit :

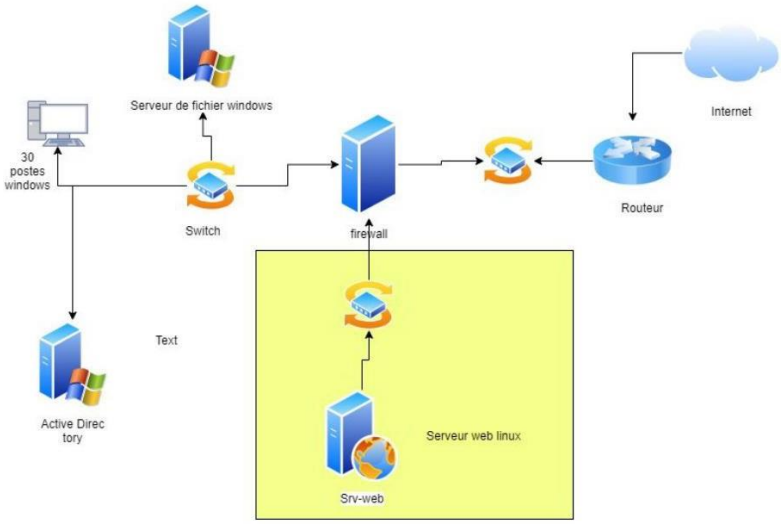


Figure 2 : Architecture du système informatique de BSI-Consulting

System Informatique

Le SI de BSI-Consulting est constitué de :
30 postes de travail Windows

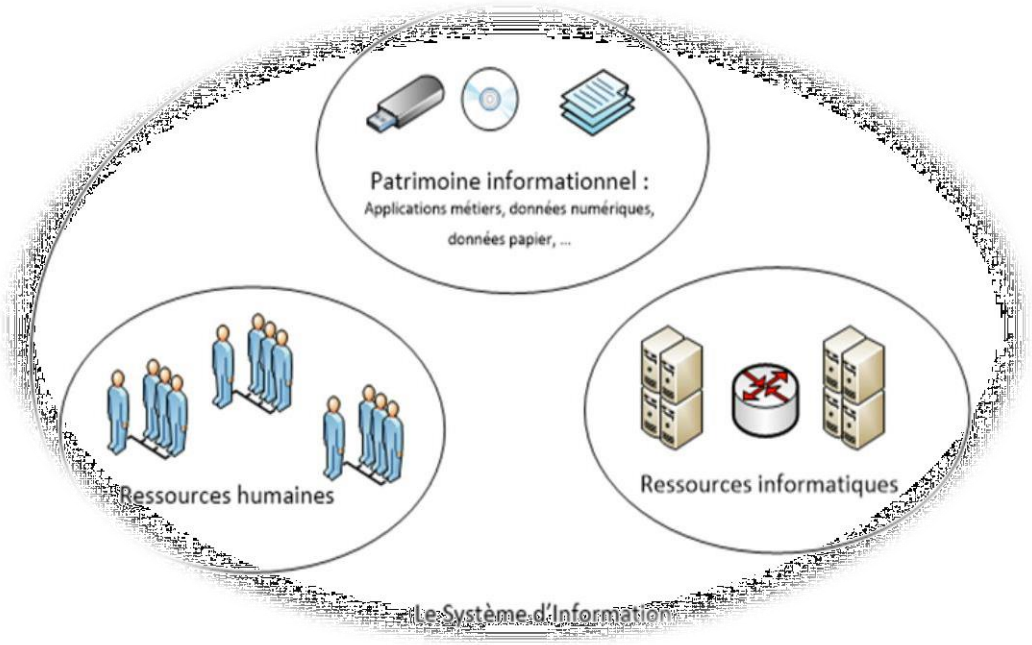
- Un serveur Windows contrôleur de domaine Active Directory
- Un serveur d'application métier et de fichiers Windows
- Un serveur web et email Linux
- Clés USB
- Un Firewall
- Trois Switch réseau
- Un routeur connecté à Internet

Les 30 postes Windows peuvent appartenir à 4 types d'utilisateurs :

1. Les utilisateurs simples avec un accès limité de données.
2. Les utilisateurs managers, qui ont accès à l'ensemble des données de leur service.
3. Les administrateurs systèmes qui ont un accès administrateur sur les postes de travail, les serveurs d'applications, l'Active Directory et les équipements réseau.
4. Le RSSI qui a un accès administrateur sur le contrôleur de domaine Active Directory et sur le Firewall.

5. Le service informatique possède un serveur connecté au réseau sur lequel sont stockés les fichiers partagés entre les employés avec un dossier par service.

6. Chaque employé utilise un compte administrateur sur son ordinateur.
7. Le service informatique effectue une sauvegarde du serveur une fois par semaine sur une clé USB stockée dans un coffre sécurisé à côté du serveur. Le site internet et le serveur email sont hébergés au siège.
8. BSI-consulting héberge en local, toutes ses données.



8. Les objectifs de la sécurité d'un système d'information

Les objectifs de la sécurité informatique regroupés en cinq grandes familles se rapportent souvent à :

1. **la Disponibilité**, elle permet l'accessibilité aux données à n'importe quel moment. Pour une entreprise, les retards dus à l'incapacité d'effectuer un traitement dans les délais peuvent donner lieu à des pénalités dans le cas de livraisons, voir la perte de clients face au non-respect des engagements.
2. **l'Intégrité**, elle garantit que les données n'ont subi aucune détérioration ou modification à l'insu de leur propriétaire ou utilisateur. Ces altérations peuvent amener à des conséquences diverses, telles que la corruption d'information ou l'ajout d'information supplémentaires et, sans oublier les coûts à de reconstruction que les données peuvent impliquer.
3. **la Confidentialité**, elle consiste à rendre l'information accessible par les personnes autorisées à y accéder seulement. Le vol d'information sensible peut être fatal à une entreprise, tant vis à vis de la concurrence que de l'image renvoyée par la société.
4. **la non – répudiation** (logs), outre l'utilité technique, une bonne gestion des traces permet l'identification, l'investigation et la conformité légale.

De nos jours la traçabilité est omniprésente et généralisée aux actes les plus communs.

5. **L'authentification** est une procédure permettant pour un système informatique de vérifier l'identité d'une personne ou d'un ordinateur et d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications).

Il nous faut garder en mémoire quatre critères lorsque l'on a la responsabilité d'un système d'information et que l'on souhaite le garantir en termes de DICP.

Pour aider les structures à mieux gérer les risques, elles peuvent s'appuyer sur la norme ISO 27005, qui contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

Cette norme s'intègre parfaitement à une démarche d'amélioration continue de type PDCA (la roue de Deming) et est donc conforme ISO 9001, ISO 31000, ISO 27001, ISO 27002, ISO 27004, 27005, ISO 27017, ISO 27018, EBIOS RM…

Dans la réalisation de cette mission, nous nous sommes basés sur les bonnes pratiques, la méthode EBIOS RM, les référentiels et les recommandations liées à la gestion des risques de système d'information.

9. EBIOS RM: Expression des Besoins et Identification des Objectifs de Sécurité – Risk Management

EBIOS Risk Manager (EBIOS RM) est la méthode d'appréciation et de traitement des risques numériques publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) avec le soutien du Club EBIOS. De ce fait, EBIOS permet de proposer une politique de sécurité adaptée aux besoins de l'entreprise ou d'une organisation.

La méthode EBIOS se compose de plusieurs guides (Introduction, Démarche, Techniques, Outillages) et d'un logiciel (plusieurs logiciels étant sur le marché par exemple Agile Risk Manager) permettant de simplifier l'application de la méthodologie explicitée dans ces guides.

Pour la suite de notre étude, nous nous référons au schéma EBIOS simplifié ci-dessous :

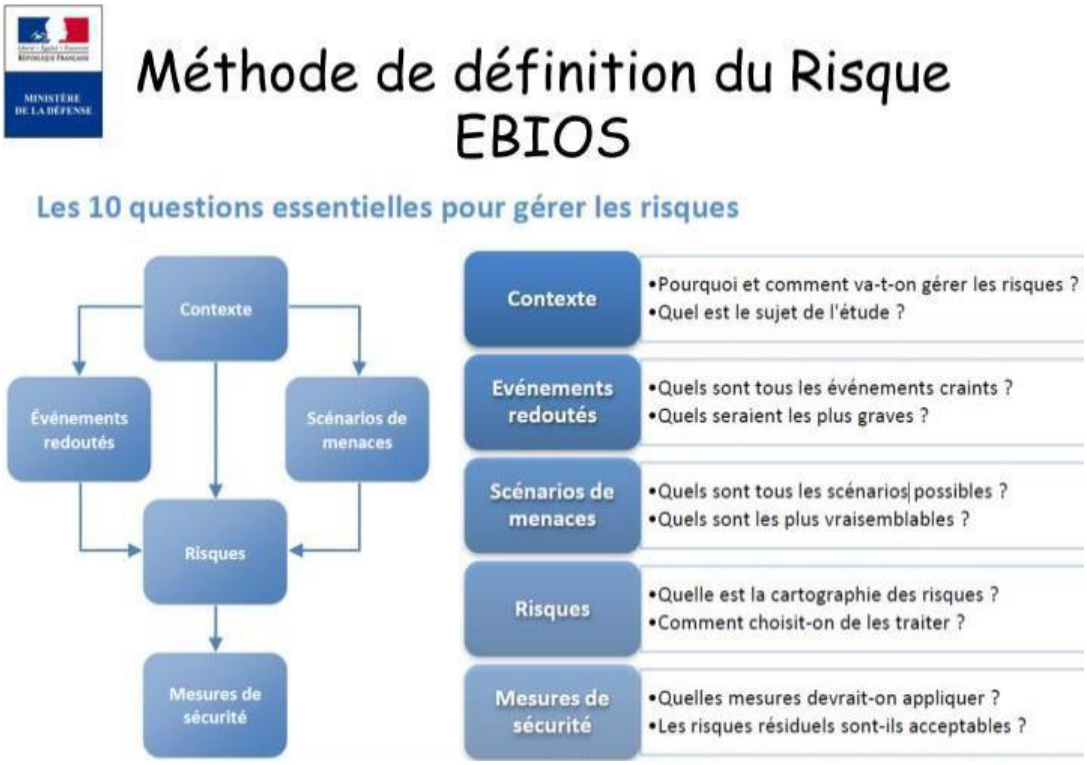


Figure 3 : Méthode de définition du Risque EBIOS

10. Réalisation de la Mission

Les activités EBIOS peuvent se résumer par le tableau ci-dessous :

Activités EBIOS	Le Commanditaire (PDG)	Le Réalisateur (RSSI)	Représentants métiers/utilisateurs (les différents pôles)
Définir le cadre de la gestion des risques	A	R	/
Préparer les métriques	/	R	C
Identifier les biens	/	R	C
Apprécier les événements redoutés	/	R	C
Apprécier les scénarios de menaces	/	R	C
Apprécier les risques	/	R	C
Identifier les objectifs de sécurité	/	R	C
Formaliser les mesures de sécurité à mettre en œuvre	A	R	C

Explications :
A : Approbateur (celui qui approuve ou non l'action qui a été réalisée)
R : Réalisateur (celui qui réalise)
C : Consulté (ceux que l'on peut faire participer sans qu'il n'ait les responsabilités liées aux autres fonctions).

10.1. Définition du Cadre de l'étude

Les Participants

- PDG /DG
- RSSI /RH / Direction de Proximité
- Pôle informatique/Pôle administratif/ Pôle production/ Pôle commercial/ Pôle Contrôle/Qualité)

11. Le contexte (Atelier 1 – Cadrage et socle de sécurité)

Les valeurs métiers représentent le patrimoine informationnel qu'une source de risque aurait intérêts à attaquer pour atteindre ses objectifs.

MISSION	FABRICATION DES PUCES ET MATERIELS TECHNOLOGIQUES				
DENOMINATION DE LA VALEUR METIER	Pôle informatique	Pôle administratif	Pôle production	Pôle commercial	Pôle Contrôle/Qualité
NATURE DE LA VALEUR METIER	Processus	Processus	Processus	Processus	Information
DESCRIPTION	Activité : Gestion de l'informatique	Activité : Tâches de gestion administrative	Activité : recherche, étude, approvisionnement, fabrication	Activité : Recherche de nouveaux clients, négociation et vente du produit	Activité : Tester les puces et matériels
ENTITE OU PERSONNE RESPONSABLE	RSSI	Responsable administration	Responsable production	Responsable Commercial	Responsable qualité
DENOMINATION DU/ DES BIENS SUPPORTS ASSOCIES	Serveurs / Logiciels / Réseaux / Clé USB de Backup /Site Web/ Serveur de Mail 2 PC portables	Logiciels bureautiques (outils collaboratifs) 3 Ordinateurs de bureau	Logiciels bureautiques (outils collaboratifs) 14 Ordinateurs de bureau Progiciels de production	Logiciels bureautiques (outils collaboratifs) 5 PC portable	Logiciels bureautiques (outils collaboratifs) 2 PC portable

DESCRIPTION	Infrastructure informatique (matériels et logiciels), services et solutions informatiques (stockage des données, accès aux ressources)…	Bureautique permettant de stocker les Créations réalisées (rédaction de textes, calculs, gestion de données…).	Appareil de production, découpage des cartes ; encartage de puces, laminage, collage, impression laser 3D, emballage, stockage,	Prospection, Achat/vente, gestion de portefeuille client…	Prélèvements des échantillons, vérification des paramétrages, conformité des produits…
ENTITE OU PERSONNE RESPONSABLE	RSSI	RH	RSSI + fournisseurs composantes	Directeur de Proximité	RSSI + Directeur de proximité

12. Evénements redoutés (Atelier 2 – Sources de Risque)

Un événement redouté est décrit sous la forme d'une expression courte ou d'un scénario permettant une compréhension facile du préjudice lié à l'atteinte de la valeur métier concernée.
L'évaluation préalable des besoins de sécurité peut aider à l'estimation de la gravité. Cette étape vise à répondre à la question suivante : qui ou quoi pourrait porter atteinte aux missions et valeurs métiers, et dans quels buts ?

12.1. Echelle de probabilité et Echelle de gravité

Avant de décrire les évènements redoutés relatifs à la sécurité des données, il est nécessaire de présenter les différentes échelles utilisées dans cette étude : l'échelle de probabilité et l'échelle de gravité.
L'échelle de probabilité sera évaluée selon leur niveau de probabilité et l'échelle de gravité selon leur niveau de gravité, sur la base de la grille de cotation suivante :

Echelles de probabilité (fréquence)		
P4	4	Très probable
P3	3	Probable
P2	2	Peu probable
P1	1	Improbable

Echelle de gravité (impact)		
G4	4	Très grave
G3	3	Grave
G2	2	Modéré
G1	1	Faible

Description de l'échelle de Probabilité

Echelle	DESCRIPTION
P4 Très probable	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La probabilité du scénario est très élevée.
P3 Probable	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La probabilité du scénario est élevée.
P2 peu probable	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La probabilité du scénario est significative.
P1 Improbable	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La probabilité du scénario est faible.

Description de l'échelle de Gravité

Echelle	Conséquences
G4 CRITIQUE	**Incapacité** pour la société **d'assurer** tout ou une partie de **son activité**, avec éventuels impacts grave sur la sécurité des personnes et des biens. La société ne surmontera pas vraisemblablement la situation (la survie de l'entreprise est menacée).
G3 GRAVE	**Forte dégradation des performances de l'activité**, avec éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec des sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	**Dégradation des performances de l'activité sans impacts** sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEUR	**Aucun impact opérationnel** sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop des difficultés (consommation des marges).

Evènements redoutes	Disponibilité	Intégrité	Confidentialité	Gravité	Retenu ?
Le dossier relatif au dernier conseil d'administration est perdu, ce qui porte atteinte à la traçabilité administrative et aux prises de décisions ultérieures (perte de temps).	X			**G1 MINEUR**	NON
Altération ou atteinte à l'intégrité de données du site Internet BSI-Consulting par la diffusion de messages inappropriés/illicites via l'un des réseaux sociaux ou la perturbation du meeting nuit à l'image BSI-Consulting		X		**G2 SIGNIFICATIVE**	OUI
Indisponibilité du portefeuille client, fichier relation clientèle, liste, contacts, procédure perdue / détruite.	X			**G2 SIGNIFICATIVE**	OUI
Fuite de données personnelles (BSI-Consulting) suite au vol ou divulguées, et exploitées dans le cadre d'attaques par phishing, ce qui nuit fortement à l'image/notoriété de l'entreprise et présente un risque juridique aux obligations légales (CNIL/RGPD).			X	**G3 GRAVE**	OUI
Usurpation des données d'identification d'un membre du siège (mail, identifiant et mot de passe, etc.) sont modifiées pour usurper le compte.		X		**G4 CRITIQUE**	OUI

Incendie : Arrêt d'activité, destruction du matériel de production, perte de données, processus…	X	X		**G4 CRITIQUE**	OUI

3. Scénarios (Atelier 3 - Scénarios Stratégiques)

Identification des sources de risques (scénarios, mode opératoire de l'attaquant, ou erreur ou négligence)

Les scénarios stratégiques sont un ensemble d'évènements et/ou d'attaque pouvant utiliser une source de risque pour atteindre son objectif. Cette étape vise à répondre à la question suivante : qui ou quoi pourrait porter atteinte aux missions et valeurs métiers, et dans quels buts ?

SOURCE DE RISQUE (SR)	OBJECTIFS VISES (OV)	CHEMIN ATTAQUES STRATEGIQUES	GRAVITE
Employé mécontent	Modification ou suppression des données en vue d'avoir des pots de vins ou par vengeance. Destruction ou compromission du système informatique (charge malveillante)/sabotage.	S'attaquer au serveur en usant de ses accès afin de modifier les données du serveur. Intrusion d'une clé USB infectée dans le système, exfiltration volontaire des données.	**G3 GRAVE**
Concurrent	Vol d'informations ou exfiltration des données, espionnage économique ou sabotage.	s'attaquer au serveur en usant des accès distant	**G3 GRAVE**
Hacker (Attaquant cyber criminel)	Ransonware, Altérer les données Divulguer des données.	Chiffrement des données / Attaque (l'homme du milieu), injection SQL, Attaque XSS (injection de script dans une page Web), attaque réseau wifi, Attaque Backdoor)/porte dérobée	**G4 CRITIQUE**
Hacktiviste (Attaquant cyber activiste)	Revendication idéologique/information/argent.	Phishing, Attaque au Président, Ransonware, DDoS ;	**G4 CRITIQUE**

4. Risques (Atelier 4 – Scénarios opérationnels)

Identification des risques

R	Risques	PROBABILITE
R1	Indisponibilité des données : Modification ou suppression des données en vue d'avoir des pots de vins ou par vengeance (employé mécontent).	**G2 Peu probable**
R2	Vol d'informations ou exfiltration des données, espionnage économique ou sabotage (concurrent).	**G3 Probable**
R3	Fuite de données personnelles, Usurpation d'identité (Hacker).	**G3 Peu probable**
R4	Perte des données/ détérioration image/ Attaque idéologique (Hacktiviste).	**G2 Peu probable**
R5	Perte ou destruction matérielle/données (incendie).	**G2 Peu probable**

Le calcul de la criticité des risques utilisés se fait par la multiplication de la probabilité et l'impact.
Criticité = Probabilité * Impact

	Risques (R)	PROBABILITE	GRAVITE	CRITICITE
R1	Modification ou suppression des données en vue d'avoir des pots de vins ou par vengeance (employé mécontent).	**P3 Probable**	**G4 CRITIQUE**	**12**
R2	Vol d'informations ou exfiltration des données, espionnage économique ou sabotage (concurrent)	**P2 Peu probable**	**G4 CRITIQUE**	**8**
R3	Fuite de données personnelles, Usurpation d'identité (Hacker)	**P3 Probable**	**G4 CRITIQUE**	**12**
R4	Perte des données, détérioration image/ Attaque idéologique (Hacktiviste)	**P2 Peu probable**	**G4 CRITIQUE**	**8**
R5	Perte matérielle (incendie)	**P2 Peu probable**	**G4 CRITIQUE**	**8**

5. Evaluation des risques

Dans cette étape, après une analyse minutieuse des contrôles mis en places, on se propose de quantifier les risques déjà identifiés par rapport à leurs impacts et à leurs degrés d'occurrence. Après l'évaluation des risques cités précédemment, on a pu élaborer la cartographie des risques suivants :

	Probabilité / Impact	**Improbable**	**Peu Probable**	**Probable**	**Très Probable**
4	**Très Grave**	4	R4, R5 (8)	R3 (12)	16
3	**Grave**	3	6	9	R1 (12)
2	**Modéré**	2	4	6	8
1	**Faible**	1	2	3	4
		1	2	3	4

1 à 4	Faible : Acceptable en l'état	5 à 8	Moyen : Tolérance sous contrôle	9 à 16	Elevé : Inacceptable

16. Mesures de sécurité (Atelier 5 – Traitement du Risque)

MESURE DE SECURITE	SCENARIOS DE RISQUES ASSOCIES	RESPONSABLE	FREINS ET DIFFICULTES DE MISE EN OEUVRE	COUTS/COMPLEXITE	ECHEANCE	STATUT
GOUVERNANCE						
Concilier les objectifs de l'entreprise et les besoins de chacun des employés	R1	PDG/DG/RSSI/RH / Directeurs Proximité, commercial, production, contrôle qualité.	Problème de communication	FinOPS/TCO	3 mois	En cours
Guide des bonnes pratiques, sensibilisation aux bonnes pratiques informatiques, risques cyber, Mise en place d'une charte informatique	R2, R3, R4	PDG/DG/RSSI/RH / Directeurs Proximité, commercial, production, contrôle qualité.	Cabinet extérieur pour personnaliser le Guide des bonnes pratiques	FinOPS/TCO	1 mois	En cours
Anticiper la violation ou la diffusion de données volées	R1, R2, R3, R4	PDG/DG/RSSI/RH	-	FinOPS/TCO		
PROTECTION						
Protection renforcée des données, Prévention contre les sinistres, lutte contre la malveillance.	R2, R3, R4, R5	PDG/DG/RSSI/RH		FinOPS/TCO	6 mois	A lancer
Sauvegarde instantanée des données, tolérance aux pannes	R1, R2, R3, R4, R5	PDG/DG/RSSI/RH	Engendre des coûts pour la mise en œuvre en local (cluster serveur, Réplication des données instantanées).	FinOPS/TCO	12 mois	A lancer
Procéder à un audit des stratégies de sécurité et de lutte contre les ransomwares, Élaborer une stratégie de protection des données solide	R2, R3, R4	PDG/DG/RSSI/RH/RSSI/ Directeurs Proximité, commercial, production, contrôle qualité		FinOPS/TCO	6 mois	A lancer
Chiffrement des données	R2, R3, R4	RSSI	Faire appel à un prestataire		6 mois	A lancer
DEFENSE						
La mise en place d'un SIEM pour la gestion des événements et des informations de sécurité. Tester	R2, R3, R4	PDG/DG/RSSI/RH/RSSI/ Directeurs Proximité, commercial, production, contrôle qualité	Achat outil SIEM à budgétiser	FinOPS/CTO	12 mois	A lancer

les systèmes mais aussi les employés						
RESILIENCE						
Plan de résilience. PCA/PRA Instaurer un plan de sauvegarde et de reprise après sinistre (RTO)	R2, R3, R4, R5	PDG/DG/RSSI/RH/RSSI/ Directeurs Proximité, commercial, production, contrôle qualité		FinOPS/CTO	immédiat	A lancer

SIEM : Security Information and Event Management, ou « Gestion des événements et des informations de sécurité »

Évaluer le risque inhérent

Le risque inhérent correspond à un calcul qui provient de l'évaluation d'un risque non traité. Il s'agit du risque brut auquel BSI-Consulting est confrontée si aucun contrôle ou tout autre facteur d'atténuation n'est mis en place. Évaluer le risque résiduel implique l'indication d'un pourcentage de traitement afin de définir la valeur selon laquelle le traitement réduit le risque inhérent.

16.2. Calculs du risque inhérent

Le risque opérationnel concerne les pertes directes ou indirectes dues à une inadéquation ou à une défaillance des procédures, du personnel et des systèmes internes.

Risques opérationnels		Probabilité	Impact	Score de Risque Inhérent
R3	Fuite de données personnelles - Usurpation d'identité (Hacker)	P3 Probable	G4 GRAVE	12 (3x4)
R1	Indisponibilité des données (employé)	P3 Probable	G4 CRITIQUE	12 (3x4)
				Risque inhérent = 24 (12+12)

16.3. Les risques résiduels

Estimation des risques résiduels : un risque résiduel est un risque qui reste après l'application des mesures de sécurité. Ce risque peut être accepté si la criticité a été réduite et l'impact est moins fort après le traitement.

LIBELLE DES RISQUES RESIDUELS
Description et analyse des risques résiduels : Description sommaire d'un impact à craindre : Les risques liés à l'indisponibilité, la confidentialité et l'intégrité des données. Vulnérabilité résiduelle susceptibles d'être exploitées par la source de risque : l'absence des mises à jour des systèmes ou logiciels. Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc. : mot de passe non robuste, utilisation des navigateurs non sécurisés, cliquer sur un lien malveillant.
Evènements redoutés concernés : Evènement redouté 1 : R3 - Fuite de données personnelles - Usurpation d'identité (Hacker) Evènement redouté 2 : R1 - Indisponibilité des données (employé)
Mesures de traitement du risque existantes et complémentaires : Mesure 1 – R1 : suivre les guides recommandés par l'ANSSI en matière de sécurité des systèmes d'information (SSI) et les référentiels ISO. Mesure 2 – R3 : suivre les guides recommandés par l'ANSSI en matière de sécurité des systèmes d'information (SSI).
Evaluation du risque résiduel : Gravite initiale : Probabilité initiale : Niveau de risque initial : Gravité résiduelle : Probabilité résiduelle : Niveau de risque résiduel :
Gestion du risque résiduel : Mesures particulières de suivi et de contrôle du risque résiduel

- Méthode de calcul du risque résiduel

Le risque résiduel est calculé selon la formule suivante : ScoreRisqueInhérent x (1-%traitement)

- Cadre des scores de risque

L'évaluation du risque inhérent se fait à l'aide du cadre de score de risque suivant :

Facteur pour le score de risque	pourcentage	Barème de gravité
Probabilité	100 %	échelle à 3 point : 1 = Faible, 2 = Moyen, 3 = Élevé
Impact	100 %	échelle à 3 point : 1 = Faible, 2 = Moyen, 3 = Élevé

- Carte de Stratégie

Dans le cadre de cette étude, nous prendrons en compte 2 risques : R1, R3

16.4. Traitement

L'évaluation préliminaire, basée sur l'efficacité attendue des efforts de traitement mis en œuvre, est la suivante :

Risques opérationnels		Traitement	
R3	Fuite de données personnelles - Usurpation d'identité (Hacker)	Traitement 1	diminue la probabilité de risque de 25 %
		Traitement 2	diminue l'impact de risque de 15 %
R1	Indisponibilité des données (employé)	Traitement 3	diminue la probabilité de risque de 40 %
		Traitement 4	diminue l'impact de risque de 20 %

16.4.1. Calcul du risque résiduel

Le tableau suivant présente le mode de calcul du niveau de risque résiduel.

Secteur opérationnel et traitement	Probabilité	Impact	Score de risque résiduel
R3 Fuite de données personnelles - Usurpation d'identité (Hacker)	**3x(1-25%) = 2,25 (risque résiduel)**	**4x(1-15%) = 3,4 (risque résiduel)**	**7,65** (2,25x3,4)
	Traitement 1 = 25%	Traitement 1 = 0%	
	Traitement 2 = 0%	Traitement 2 = 15%	
R1 Indisponibilité des données (employé)	**3x(1-40%) = 1,8 (risque résiduel)**	**4x(1-20%) = 3,2 (risque résiduel)**	**5,76** (1,8x3,2)
	Traitement 3 = 40%	Traitement 3 = 0%	
	Traitement 4 = 0%	Traitement 4 = 20%	
Niveau de risque résiduel = score de risque résiduel total / score de risque inhérent total			

Risques	Evaluation brute	Moyens de maîtrise	Evaluation nette
R3 Fuite de données personnelles - Usurpation d'identité (Hacker)	levée (12)	La mise en place d'un SIEM pour la gestion des événements et des informations de sécurité. Protection renforcée des accès réseaux et systèmes. Élaborer une stratégie de protection des données solides (chiffrement des données), lutte contre la malveillance, mesures d'hygiène informatique et sensibilisation aux menaces cyber /Recommandations ANSSI/conformité ISO/CNIL/RGPD Instaurer un plan de sauvegarde et de reprise après sinistre (RTO), Plan de résilience PCA/PRA Etudier l'opportunité de désigner au moins une personne en charge de la protection de la vie privée (prévoir une décision du CA)	yenne (6)
R1 Indisponibilité des données (employé)	levée (12)	Prendre les mesures préventives pour éviter l'interruption de services (utilisation du clustering actif-actif pour la tolérance aux pannes) et les mesures curatives. Sauvegarde instantanée des données. Plan de résilience PCA/PRA	yenne (8)

16.5. Evaluation des risques résiduels

	Probabilité / Impact	Improbable	Peu Probable	Probable	Très Probable
4	Très Grave	4	R4, R5 (8)	R3 (12)	16
3	Grave	3	6	9	R1 (12)
2	Modéré	2	4	6	8
1	Faible	1	2	3	4
		1	2	3	4

1 à 4	Faible : Acceptable en l'état	5 à 8	Moyen : Tolérance sous contrôle	9 à 16	Elevé : Inacceptable

	Probabilité / Impact	Improbable	Peu Probable	Probable	Très Probable
4	Très Grave	4	**R1** R2, R4, R5 (8)	12	16
3	Grave	3	6	9	12
2	Modéré	2	4	**R3** (6)	8
1	Faible	1	2	3	4
		1	2	3	4

1 à 4	Faible : Acceptable en l'état	5 à 8	Moyen : Tolérance sous contrôle	9 à 16	Elevé : Inacceptable

Grâce aux mesures mises en place :

- le niveau du risque «Fuite de données personnelles - Usurpation d'identité (Hacker)» est passé d'élevé à tolérance sous contrôle ;
- le niveau du risque « Indisponibilité des données (employé)» est passé d'élevé à tolérance sous contrôle.

N.B. : Il est important de réévaluer les risques chaque année et de les ajuster si nécessaires. Nous conseillons la mise en place d'un logiciel de suivi des risques et des contrôles. Enfin, une entreprise sans risque n'existe pas, c'est pourquoi il est mieux de les connaitre afin de les maitriser si possible.

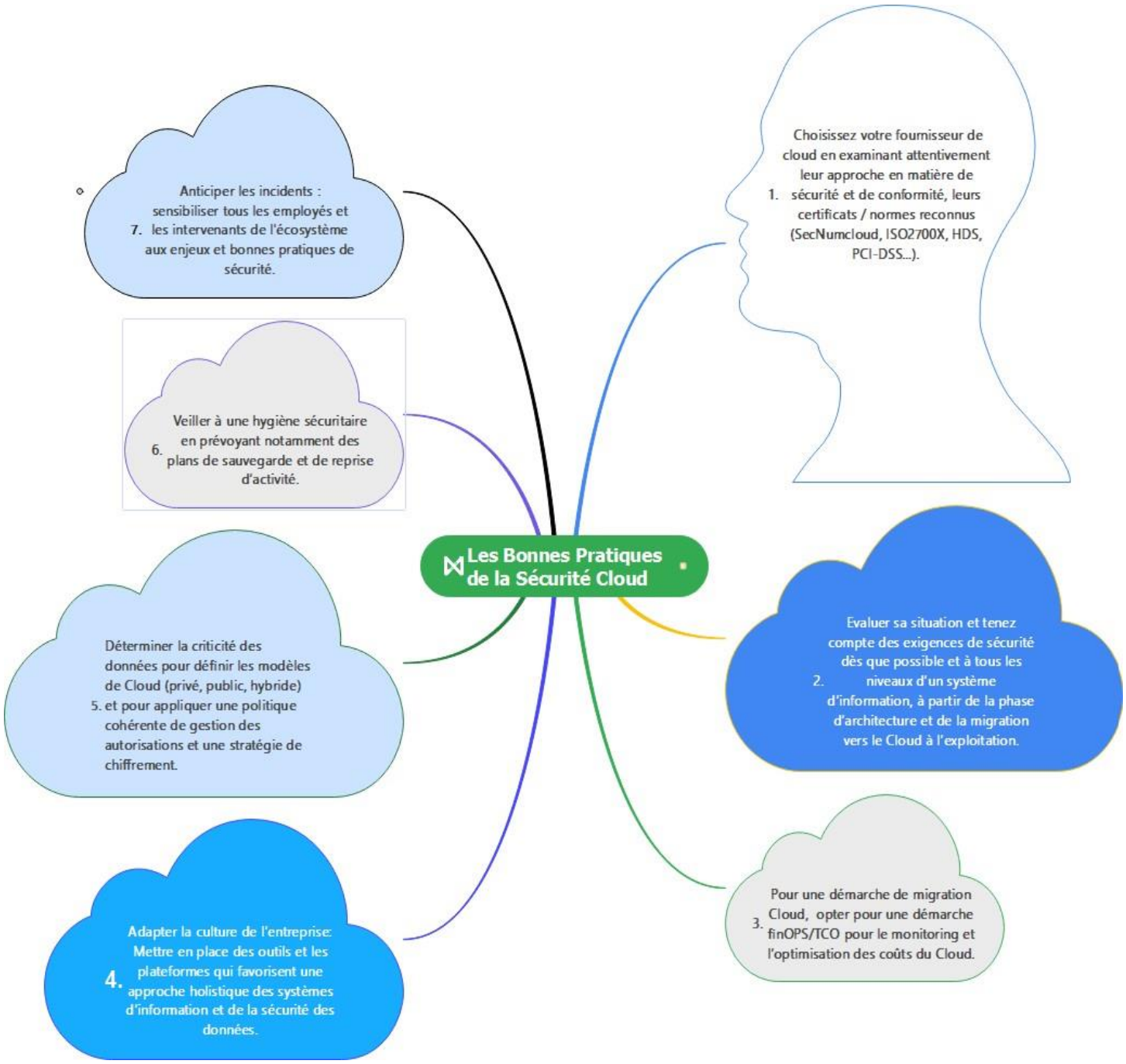
17. Conclusion

BSI-Consulting est dans la nécessité de protéger son système d'information contre toutes menaces qui pourraient affecter la confidentialité, l'intégrité et la disponibilité de ses données.

Le système d'information est devenu une ressource très précieuse pour l'entreprise, il lui permet de comprendre son environnement, de gérer ses activités au quotidien, de gagner en production et de prendre des décisions stratégiques. Cela passe prioritairement par la définition et la mise en place au sein de BSI-Consulting d'une « Politique de Sécurité des Systèmes d'Information » (PSSI). La PSSI doit découler d'une vision stratégique de BSI- Consulting et traduire un engagement fort de la direction générale sur le long terme.

En somme, compte tenu des contraintes budgétaires, nous conseillons à BSI-Consulting dans sa démarche de migration cloud d'opter pour une démarche finOPS/TCO pour le monitoring et l'optimisation des coûts.

Enfin, souhaitant adopter une démarche de migration vers le Cloud, ci-dessous quelques bonnes pratiques de Sécurité Cloud (liste non exhaustive) de la sécurité Cloud soumises à BSI Consulting.


Les Bonnes Pratiques de la Sécurité Cloud
1. Choisissez votre fournisseur de cloud en examinant attentivement leur approche en matière de sécurité et de conformité, leurs certificats / normes reconnus (SecNumcloud, ISO2700X, HDS, PCI-DSS...).
2. Evaluer sa situation et tenez compte des exigences de sécurité dès que possible et à tous les niveaux d'un système d'information, à partir de la phase d'architecture et de la migration vers le Cloud à l'exploitation.
3. Pour une démarche de migration Cloud, opter pour une démarche finOPS/TCO pour le monitoring et l'optimisation des coûts du Cloud.
4. Adapter la culture de l'entreprise: Mettre en place des outils et les plateformes qui favorisent une approche holistique des systèmes d'information et de la sécurité des données.
5. Déterminer la criticité des données pour définir les modèles de Cloud (privé, public, hybride) et pour appliquer une politique cohérente de gestion des autorisations et une stratégie de chiffrement.
6. Veiller à une hygiène sécuritaire en prévoyant notamment des plans de sauvegarde et de reprise d'activité.
7. Anticiper les incidents : sensibiliser tous les employés et les intervenants de l'écosystème aux enjeux et bonnes pratiques de sécurité.

Annexe 16
Liste et catégories des biens support selon EBIOS RM

SYSTÈME D'EXPLOITATION, HYPERVISEUR	Windows, Linux, MacOS, Xen.
MICROGICIEL (*FIRMWARE*)	*Basic Input Output System* (BIOS), *Unified Extensible Firmware Interface* (UEFI), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur.
LOGICIEL DE SÉCURITÉ	Outil de gestion d'évènements *Security Information and Event Management* (SIEM).
RÉSEAUX/CANAUX INFORMATIQUES ET DE TÉLÉPHONIE	
RÉSEAU/CANAL INFORMATIQUE	Câble réseau, fibre optique, liaison radio (Wi-Fi, Bluetooth, etc.).
RÉSEAU/CANAL TÉLÉPHONIQUE	Ligne téléphonique.
ORGANISATIONS	
PERSONNE	Employé, stagiaire, prestataire, personnel d'entretien.
SUPPORT PAPIER	Document manuscrit ou imprimé.
ÉCHANGE VERBAL	Réunion, échange informel.
ÉLÉMENT D'INGÉNIERIE SOCIALE	Information partagée sur les réseaux sociaux.
LOCAUX ET INSTALLATIONS PHYSIQUES	
SITE/BÂTIMENT/SALLE	Siège social, usine, site de stockage, bâtiment industriel, salle de réunion, salle serveur.
SYSTÈME DE SÉCURITÉ PHYSIQUE	Système d'accès par badge, système de détection d'intrusion, système de vidéo-protection.
SYSTÈME DE SÛRETÉ DE FONCTIONNEMENT	Climatisation, sécurité incendie, alimentation électrique.

BIEN SUPPORT	**EXEMPLES (LISTE NON EXHAUSTIVE)**
SYSTÈMES INFORMATIQUES ET DE TÉLÉPHONIE	
MATÉRIELS[i]	
TERMINAL UTILISATEUR	Ordinateur fixe, ordinateur portable, tablette, téléphone mobile.
PÉRIPHÉRIQUE	Imprimante, scanner, clavier, souris, caméra, microphone, objet connecté.
TÉLÉPHONE	Téléphone fixe ou mobile analogique ou IP.
ÉQUIPEMENT DE STOCKAGE	Clé USB, disque dur, CD-ROM, carte mémoire.
SERVEUR	*Mainframe*, serveur lame, serveur *rack*.
MOYEN D'ADMINISTRATION	Poste d'administration, serveur outils d'administration, bastion.
ÉQUIPEMENT RÉSEAU	Commutateur, routeur, passerelles d'entrée depuis l'extérieur, borne WI-FI.
ÉQUIPEMENT DE SÉCURITÉ	Pare-feu, sonde (IDS/IPS), passerelle VPN.
ÉQUIPEMENT INDUSTRIEL	Automate programmable industriel, capteur, actionneur, système SCADA, système instrumenté de sécurité.
LOGICIELS	
SERVICE D'INFRASTRUCTURE	Service d'annuaire, service de gestion d'adresse IP (DHCP), service de nom de domaine (DNS), contrôleur de domaine, serveur d'impression.
APPLICATION/SERVICE APPLICATIF	Serveur web, service web, serveur d'application, serveur de courrier électronique, serveur de bases de données, progiciels (RH, relation client, ERP).
INTERGICIEL (*MIDDLEWARE*)	*Entreprise Application Integration* (EAI), *Extract-Transform-Load* (ETL), *Open DataBase Connectivity* (ODBC).

Annexe 17
La liste des impacts selon EBIOS RM

Impact	Exemples (listes non exhaustives)
Impacts sur les missions et services de l'organisme	
Conséquences directes ou indirectes sur la réalisation des missions et services.	Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé.
Impacts sur la gouvernance de l'organisme	
Impacts sur la capacité de développement ou de décision Conséquences directes ou indirectes sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement.	Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisme, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés.
Impacts sur le lien social interne Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation.	Perte de confiance des employés dans la pérennité de l'organisme, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, affaiblissement/perte de sens des valeurs communes.
Impacts sur le patrimoine intellectuel ou culturel Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes.	Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés.
Impacts humains, matériels ou environnementaux	
Impacts sur la sécurité ou sur la santé des personnes Conséquences directes ou indirectes sur l'intégrité physique de personnes.	Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire.
Impacts matériels Dégâts matériels ou destruction de biens supports.	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels.
Impacts sur l'environnement Conséquences écologiques à court ou long terme, directes ou indirectes.	Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère.
Impacts financiers	
Conséquences pécuniaires, directes ou indirectes.	Perte de chiffre d'affaire, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées.
Impacts juridiques	
Conséquences suite à une non-conformité légale, règlementaire, normative ou contractuelle.	Procès, amende, condamnation d'un dirigeant, amendement de contrat.
Impacts sur l'image et la confiance	
Conséquences directes ou indirectes sur l'image de l'organisation, la notoriété, la confiance des clients.	Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte d'avance concurrentielle, perte de notoriété, perte de confiance d'usagers.

Annexe 18
La liste complète des (ER) étudiés

Ref (ER)	Evènement redouté	Impacts	Gravité	DICT (potentiellement atteint)
ER1	Perte des clés de chiffrement nécessaires pour l'accès aux données	MPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4	G3 Dépendra des informations chiffrées (possibilité de récupération…)	(D)
ER2	Attaque via une élévation de privilèges	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6	G3	(D) (I) (C) (T)
ER3	Attaque avec usurpation d'identité (ingénierie sociale)	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6 ; IMPACT_7	G3	(D) (I) (C) (T)
ER4	Perte ou vol de(s) seule(s) sauvegarde(s) existante(s)	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6	G4	(D)
ER5	Interception des données sensibles (personnelles, stratégiques) en transit	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6	G4	(C)
ER6	Accès aux données sensibles (personnelles, stratégiques) suite à une erreur ou absence de classification des données	IMPACT_1 ; IMPACT_3 ; IMPACT_4 (Données de gestion des services Cloud, Données sensibles : stratégiques / personnelles) ; IMPACT_6 ; IMPACT_7 ; IMPACT_8	G4	(D) (I) (C) (T)
ER7	Perte de contrôle et de conformité aux exigences de sécurité (Manque de transparence de la part du fournisseur Cloud. Négligence et/ou mauvaise interprétation des responsabilités définies dans le contrat.)	IMPACT_1 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6 ; IMPACT_7 ; IMPACT_8 ; IMPACT_9	G4	(D) (I) (C) (T)
ER8	Suppression inefficace des données	IMPACT_1 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G3	(C)
ER9	Divulgation forcée des données	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G4	(C)

ER10	Changements de juridiction	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G4	(D) (C)
ER11	Non-respect de la réglementation sur la protection des données	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sensibles : stratégiques / personnelles) ; IMPACT_6	G4	(C)
ER12	Verrouillage du fournisseur Cloud	MPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4	G4	(D)
ER13	Défaillance de la chaîne d'approvisionnement	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6	G3	(D) (I) (C) (T)
ER14	Exploitation illégitime des données par le fournisseur Cloud (Personnel malveillant du fournisseur Cloud)	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6	G4	(D) (I) (C) (T)
ER15	Faille au niveau de la sécurité physique de l'infrastructure du fournisseur	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 (Données sauvegardées) ; IMPACT_5 (Supports de sauvegarde) ; IMPACT_6	G4	(D) (I) (C) (T)
ER16	Acquisition du fournisseur Cloud (Possibilité de changement des conditions du contrat …)	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6	G3	(D)
ER17	Défauts d'isolement des ressources	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6	G4	(D) (I) (C) (T)
ER18	Compromission de l'interface de gestion des clients du fournisseur Cloud (Disponibilité de l'infrastructure, manipulation)	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6	G4	(D) (I) (C) (T)
ER19	Perte ou compromission des journaux d'événements / sécurité (Besoin en cas d'enquête médico-légale)	MPACT_1 ; IMPACT_3 ; IMPACT_4 ; IMPACT_6	G4	(D) (I)
ER20	Mauvaise gestion des comptes/autorisations d'accès : Mauvais paramétrage / mauvaise configuration (Vulnérabilité au niveau du système d'exploitation, Erreur humaine, administrateur non formé ou mauvaise application des procédures de sécurité de base et de renforcement)	IMPACT_1 ; IMPACT_3 ; IMPACT_4 (Données de gestion des services Cloud, Données sensibles : stratégiques / personnelles) IMPACT_5 ; IMPACT_6 ; IMPACT_7 ; IMPACT_8	G4	(D) (I) (C) (T)
ER21	Utilisation d'application sans l'approbation de la Direction et du service IT (Shadow IT)	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6	G4	(D) (I) (C) (T)

ER22	Catastrophe naturelle	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6	G4	(D)
ER23	Vol de matériel informatique	IMPACT_1 ; IMPACT_2 ; IMPACT_3 ; IMPACT_4 ; IMPACT_5 ; IMPACT_6	G4	(D) (I) (C) (T)

Annexe 19
La liste complète des (SO)

Ref SO	Chemin d'attaque stratégique associé au scénario opérationnel	Vraisemblance globale
SO1	Perte d'accès au gestionnaire des clés de chiffrement suite à une attaque sur le service dédié chez le fournisseur Cloud	V2 - Vraisemblable
SO2	Connexion au service Cloud par un ex-salarié mécontent ayant accès à son un ancien compte encore actif. Elévation de privilèges et vol d'informations sensibles et divulgation de ces dernières	V2 - Vraisemblable
SO3	Un attaquant se rapproche de l'un des employés de l'entreprise (ayant un accès aux données stratégiques), récupération de ses identifiants de connexion aux services Cloud via ingénierie social/Phishing. Destruction des données stratégiques	V2 - Vraisemblable
SO4	Incendie au niveau de l'infrastructure du fournisseur Cloud entraînant la perte de la sauvegarde des données	V2 - Vraisemblable
SO5	Récupération des données stratégiques de l'entreprise par un concurrent ou une personne malveillante pour divulgation. Interception du trafic réseau à l'aide d'outils de reniflage (renifleur de paquets) ou attaque de l'homme du milieu (HDM).	V3 - Très vraisemblable
SO6	Accès et altération/suppression de données stratégiques (données d'un projet, brevet…) par un employé mécontent de l'entreprise qui n'est pas censé accéder à ces données sensibles non classifiées	V3 - Très vraisemblable
SO7	Négligence et/ou mauvaise interprétation des responsabilités définies dans le contrat OU Manque de transparence de la part du fournisseur Cloud (sur les fonctionnalités, localisation pour le stockage des données...). Exemples de cas : Chiffrement non compris dans le contrat --> mauvaise interprétation du client. Le client qui croit que le fournisseur Cloud est responsable de toute la sécurité des données alors que ce n'est pas compris dans le contrat --> mauvaise interprétation du client. Le fournisseur Cloud sous-traite le chiffrement des données à un prestataire qui ne fournit pas les mêmes garanties initialement annoncées --> manque de transparence.	V4 - quasi certain
SO8	Suite à une suppression inefficace des données personnelles des employés des entreprises, un client du même fournisseur Cloud pourrait avoir accès aux données personnelles.	V2 - Vraisemblable

SO9	Divulgation forcée des données sensibles. Suite à une enquête et une demande, par les forces de l'ordre d'un état étranger, de confiscation de matériel physique (stockage centralisé, partagé avec d'autres clients du fournisseur Cloud) contenant les sauvegardes de données.	**V3 - Très vraisemblable**
SO10	Des données sensibles qui se retrouvent stockées dans un pays avec une juridiction différente et qui ne respecte pas les accords internationaux, ou la protection des données personnelles par exemple. Ou qui pourraient avoir accès ou saisir le matériel physique sans même avoir besoin d'une enquête.	**V4 - quasi certain**
SO11	Le fournisseur Cloud ne respecte pas la législation sur la protection des données personnelles, volontairement ou en perdant tout simplement le contrôle sur le traitement des données.	**V3 - Très vraisemblable**
SO12	Impossibilité d'exporter les applications existantes vers un autre fournisseur Cloud, ainsi que toutes les données au format standard (ou alors cela demanderait beaucoup de temps et un budget conséquent).	**V3 - Très vraisemblable**
SO13	Impossibilité d'accéder aux services Cloud. L'application (externalisée par le fournisseur Cloud) qui gère les identités pour l'accès aux services Cloud a été compromise.	**V2 - Vraisemblable**
SO14	Vol des données sensibles (stratégiques) de l'entreprise par l'administrateur (corrompu travaillant pour le compte d'un concurrent déloyal) du fournisseur Cloud.	**V3 - Très vraisemblable**
SO15	Destruction des données (stratégiques) de l'entreprise par une personne malveillante qui a pu accéder aux locaux de l'infrastructure du fournisseur Cloud.	**V2 - Vraisemblable**
SO16	Arrêt d'un service ne figurant pas dans le contrat. Ce service pourrait impacter le respect des exigences de sécurité (Sécurité des interfaces des logiciels utilisés, antivirus…) suite à l'acquisition du fournisseur Cloud.	**V2 - Vraisemblable**
SO17	Destruction de données sensibles stratégiques par un Hacktiviste suite à une attaque par injection SQL (Méthode "Stacked queries" ou autres) sur les services du fournisseur Cloud --> Exploitation d'une faille au niveau des mécanismes de séparation du stockage dans le Cloud Public permettant d'accéder à la base de données	**V3 - Très vraisemblable**
SO18	Attaque par un Hacktiviste en exploitant une faille (Par Ex. Zero-Day) au niveau de l'accès à distance aux services Cloud du fournisseur --> Suppression de toutes les bases de données du Cloud et altération de l'interface de gestion des clients du fournisseur Cloud public.	**V3 - Très vraisemblable**

SO19	Manque d'éléments dans le cadre d'une enquête médico-légale --> Impossibilité de récupérer les journaux d'évènements / de sécurité de la part du fournisseur Cloud	**V2 - Vraisemblable**
SO20	Vol ou divulgation des données stratégiques de l'entreprise par un salarié mécontent. Suite à une mauvaise gestion des accès, ce dernier avait accès par erreur à des répertoires contenant des données sensibles	**V3 - Très vraisemblable**
SO21	Un salarié utilise son compte personnel et passe par une application sur internet (non autorisée par l'entreprise) pour stocker les données de l'entreprise afin d'y avoir accès chez lui. Il s'est fait pirater son compte, l'hackeur a récupéré ses identifiants de connexion aux services Cloud et des informations stratégiques sur l'entreprise ont été divulguées.	**V3 - Très vraisemblable**
SO22	Suite à des inondations le site principal du fournisseur Cloud est fortement atteint. Tous les services sont HS et les données sont irrécupérables.	**V2 - Vraisemblable**
SO23	Un des salariés s'est fait voler son ordinateur portable. Les voleurs (engagés par un concurrent déloyal) ont pu se connecter à sa session Cloud et ont pu récupérer des données sensibles (stratégiques)	**V2 - Vraisemblable**