LES DOSSIERS TECHNIQUES

INTEGRER LA SECURITE DANS LES PROJETS CLOUD

Juin 2021

CLUSIF

Table des matières

INTEGRER LA SECURITE DANS LES PROJETS CLOUD 1

1 QU'EST-CE QUE LE CLOUD ? 6

1.1 Présentation des types d'offres cloud : IaaS, PaaS, SaaS, CaaS, FaaS, SASE 6
1.1.1 Infrastructure as a Service 7
1.1.2 Platform as a Service 8
1.1.3 Software as a Service 8
1.1.4 Containers as a Service 9
1.1.5 Function as a Service 9
1.1.6 Secure Access Service Edge 10

1.2 Présentation des modèles de déploiement cloud (public, privé, communautaire, hybride) 14
1.2.1 Cloud public 14
1.2.2 Cloud privé 15
1.2.3 Cloud communautaire 16
1.2.4 Cloud hybride 17

2 BIEN GERER SON PROJET CLOUD 18

2.1 L'importance des différentes phases dans un projet cloud 18

2.2 Étapes d'un projet cloud 18

3 SECURITE DANS LE CLOUD 21

3.1 Fondamentaux de la cybersécurité dans le cloud 21

3.2 Introduction à la gestion des risques 21
3.2.1 L'approche par les risques, pourquoi ? 21
3.2.2 Méthodologies 22
3.2.3 Processus de définition d'une gestion du risque 22

3.3 Risques liés à un déploiement non maîtrisé dans le cloud 23
3.3.1 Maîtriser la complexité de l'offre cloud 23
3.3.2 Sécuriser la configuration et le paramétrage 24
3.3.3 Maîtriser sa consommation de services cloud 25
3.3.4 Rester libre 25
3.3.5 Ne pas oublier… 25

3.4 Amélioration de la sécurité de ses applications cloud 26
3.4.1 Rédiger un cahier de bonnes pratiques 26
3.4.2 Sécurisation des accès 26
3.4.3 Menaces et fuite de données 28
3.4.4 Réglementation, normes et certifications 28

ANNEXES 30

1 GLOSSAIRE 31

2 QUESTIONNAIRE POUR LES PROJETS CLOUD 34
1. Résumé du projet 35
2. Fiche d'identité du projet 35
3. Acteurs du projet 35
4. Historique du périmètre projet 36
5. Hébergement 36
6. Contrat 37
7. Sécurité des données et des accès 39

3 ÉVALUATION DES BESOINS DE SECURITE 41

4 INTRODUCTION A L'IDENTIFICATION DES ACTIFS ET LEUR EVALUATION 44

4.1 Préambule 44

4.2 Identification des actifs 44

4.3 Évaluation des actifs 45

5 CHECKLIST DES CLAUSES CONTRACTUELLES 46

5.1 Recommandations de la CNIL 46

5.2 Pour aller plus loin 47

6 MATRICE DES RACI D'UN SOC 48

7 EXEMPLES D'IMPLEMENTATION D'UN PROJET CLOUD 49

7.1 Préambule 49

7.2 Cas concret : Implémentation d'une infrastructure IaaS/PaaS sur Azure 49

7.3 Cas concret : Authentification unique sur Docusign *via* Okta 52

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Baptiste	**HAMON**	SSI Conseil
Jean-Marc	**JACQUOT**	Lexaura

Les contributeurs :

Xavier	**AIT-YAHIATENE**	SYNETIS
Hervann	**ALLEGRE**	FLOW LINE TECHNOLOGIES
Pierre	**BAILLY**	ELIADE
Alban	**CAOUREN**	INOTYKO
Olivier	**GILLET**	ANOMALI
Valentin	**JANGWA**	BITGLASS
Mehdi	**KEFI**	HARMONIE TECHNOLOGIE
Yann	**KERNANEC**	ELIADE
Hervé	**MAFILLE**	UVU GROUP
Christophe	**MOISAN**	MEDERI
Hervé	**SCHAUER**	HS2
Eric	**TETELIN**	MINISTERE DE LA TRANSITION ECOLOGIQUE
François-Xavier	**VINCENT**	OODRIVE

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Qu'est-ce que le cloud ?

1.1 Présentation des types d'offres cloud : IaaS, PaaS, SaaS, CaaS, FaaS, SASE

Le *cloud computing* ou « informatique dans le nuage » consiste à consommer des ressources de traitement et de stockage des données mises à disposition par des fournisseurs *via* Internet.

À l'image de la puissance électrique, la puissance informatique est ainsi proposée à la demande, sous forme d'abonnements tarifés en fonction des ressources utilisées.

Le cloud peut se découper en trois services « historiques[1] » :

- le **IaaS** *(Infrastructure as a Service)* met à disposition les ressources de calcul, de stockage et de bande passante ;
- le **PaaS** *(Platform as a Service)* regroupe les services nécessaires pour exécuter des applications ;
- le **SaaS** *(Software as a Service)* désigne justement les applications construites au-dessus de l'édifice et généralement commercialisées directement par des éditeurs de logiciels (Microsoft 365[2], Google Workspace[3], gestion ressources humaines, gestion financière, gestion de la chaîne logistique, ERP…).

Les offres de *cloud computing* se sont enrichies au fil du temps.

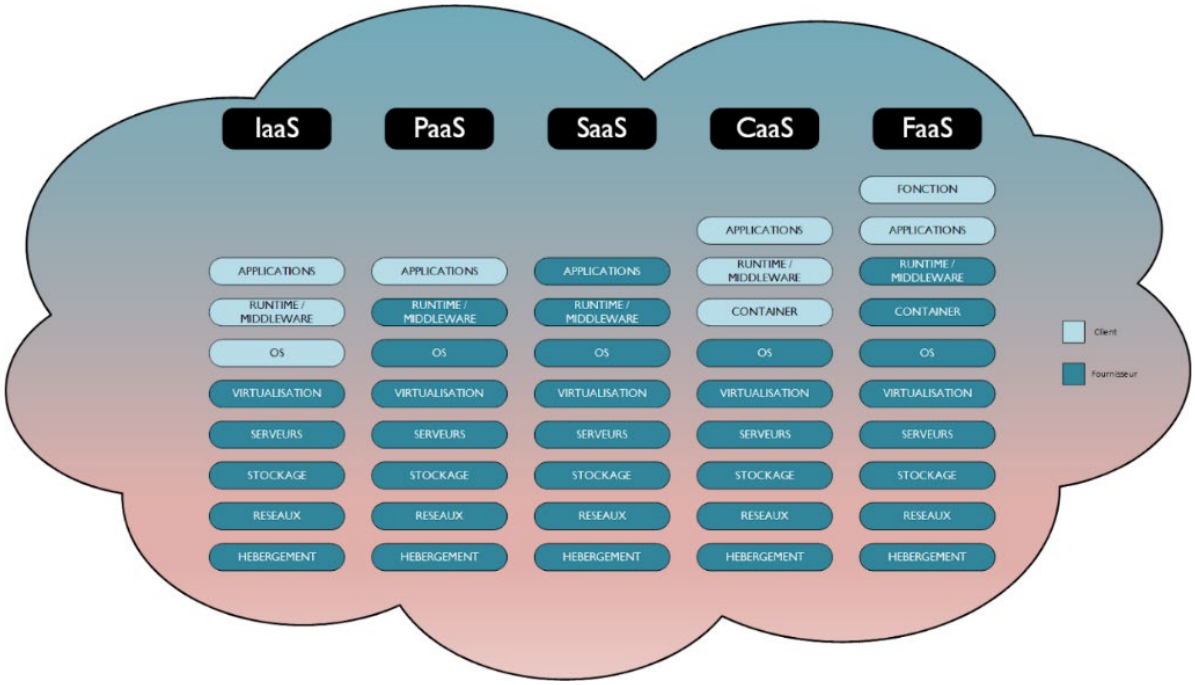
- Aux couches de calcul et de stockage sont venues se greffer des bases de données de tout type, capables de gérer jusqu'au *big data,* mais aussi des services d'*auto-scaling* permettant d'adapter les ressources en temps réel en fonction des amplitudes de trafic.
- Des environnements sans serveur *(serverless)* ou **FaaS** *(Function as a Service)* sont apparus pour automatiser l'infrastructure sans avoir à se préoccuper de la couche inférieure (serveurs, système d'exploitation, réseau, etc.) et ainsi permettre de faire abstraction de l'environnement d'exécution. Des briques de **CaaS** *(Container as a Service)* permettent quant à elles de bâtir des architectures applicatives portables d'un cloud à un autre. Et enfin le **SASE** (Secure Access Service Edge) associe connectivité réseau définie par logiciel (SD-WAN) à des services de sécurité réseau afin de garantir un accès sécurisé et dynamique aux ressources de l'entreprise.

[1] National Institute of Standards and Technology (NIST). NIST SP 800-144: *Guidelines on Security and Privacy in Public Cloud Computing,* Chapitre 2.2 *(Services Models)* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[2] Anciennement « Office 365 »

[3] Anciennement « G Suite »

Schéma de partage des responsabilités client/fournisseur selon le type d'offre cloud :



1.1.1 Infrastructure as a Service

L'infrastructure en tant que service ou *Infrastructure as a Service* (IaaS) permet l'externalisation de l'infrastructure matérielle (*datacenter,* réseau, stockage et serveur) chez un fournisseur tiers.

Les infrastructures peuvent être dédiées au client, partiellement mutualisées (partage du réseau, des dispositifs de sauvegarde, de sécurité…) ou entièrement mutualisées. L'accès aux ressources (VMs) se fait *via* une connexion Internet sécurisée ou un lien dédié.

Dans ce modèle, l'entreprise dispose d'un abonnement payant à une infrastructure (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur qui en assure la maintenance et la sécurisation physique. Le contrat souscrit avec le prestataire détermine les engagements de services associés à la plateforme.

Avantages

- Gain de temps et financier : plus d'installation et de maintenance du matériel informatique en interne.
- Niveau de sécurisation (ISO 27001, ISO 27017, SecNumCloud, HDS, SOC 1, SOC 2, SOC 3, etc.) après vérification des points évoqués au 3.4.4.
- Meilleure flexibilité : des ressources matérielles ajustables sur demande selon les besoins du client.
- Accès et gestion des ressources à distance (créer, démarrer, arrêter ou configurer une machine virtuelle).
- Localisation des données généralement plus simple à maîtriser.

Inconvénients

- La gestion du système d'exploitation, des bases de données, du *middleware* et des applications reste à la charge des équipes IT du client.
- L'interconnexion réseau entre les sites du client et l'infrastructure IaaS devient souvent un point important supplémentaire à gérer et à surveiller.

Cible

Pour les entreprises disposant d'une DSI en capacité de construire et gérer leurs propres plateformes IT mais souhaitant plus de flexibilité pour ajuster l'infrastructure à leurs besoins.

1.1.2 Platform as a Service

La plateforme en tant que service ou *Platform as a Service* (PaaS) permet d'externaliser chez un fournisseur tiers l'infrastructure matérielle (comme pour le IaaS) mais également une partie de l'environnement logiciel : système d'exploitation, bases de données, couches d'intégration *(middleware), runtimes* (ex. : Java, libc++)…

Dans ce modèle, l'entreprise concentre ses ressources IT internes sur les applications métiers qui lui sont le plus utiles.

Avantages

- Apporte les mêmes bénéfices que l'IaaS.
- Permet aux entreprises de se concentrer sur le développement sans avoir à se soucier de l'infrastructure sous-jacente.
- Le fournisseur gère la sécurité des moyens impliqués dans le service, les systèmes d'exploitation, bases de données, sauvegardes…
- Les ressources IT internes conservent la maîtrise de l'environnement logiciel métier.
- En termes de sécurité des données, l'entreprise contrôle la diffusion, le niveau de protection et la sauvegarde de ses données.

Inconvénients

- Dépendance accrue au fournisseur qui maîtrise l'infrastructure et l'environnement logiciel (Hors applications métiers).
- Flexibilité moindre sur le choix des couches logicielles intermédiaires (version des moteurs de bases de données, *middleware*…).
- Possibles mises à jour du *middleware* imposées par le fournisseur au client ce qui est susceptible d'engendrer des dysfonctionnements si le client ne gère pas correctement ses tests de non-régressions pour ses applications.
- L'interconnexion réseau entre les sites du client et l'infrastructure PaaS devient souvent un point d'attention supplémentaire à gérer et à surveiller.

Cible

Pour les entreprises souhaitant conserver la maîtrise de leurs applications métiers tout en s'affranchissant des contraintes de gestion de l'infrastructure matérielle et de l'environnement logiciel intermédiaire.

1.1.3 Software as a Service

Le logiciel en tant que service ou *Software as a Service* (SaaS) permet de disposer d'une solution logicielle dans un environnement totalement hébergé et maintenu chez et par un tiers.

Les applications et les données sont disponibles *via* un navigateur Web, au travers d'APIs (interfaces de programmation) voire des applications « client lourd » disponibles sur le poste client ou au travers de connexions à distance.

Les clients ne paient pas de licence d'utilisation pour une version, mais souscrivent à un abonnement.

Avantages

- Affranchissement total de la gestion de l'infrastructure et de l'environnement logiciel.

- Plus d'investissement dans des licences logicielles : paiement à l'usage (le prix par utilisateur englobe le coût des licences, de la maintenance et de l'infrastructure).
- Même version logicielle pour l'ensemble des utilisateurs et mises à jour automatiques.
- Rapidité de déploiement.

Inconvénients

- Dépendance totale envers le fournisseur : le contrat de service est essentiel pour définir le niveau de qualité de service (SLA).
- Sécurité des données : localisation des applications et des données plus complexes à appréhender selon les fournisseurs.
- Adaptation nécessaire du plan de continuité de l'activité à l'intégration de solutions SaaS.
- Difficulté d'intégration et de récupération des données.

Cible

Toutes les organisations peuvent être intéressées par le modèle SaaS qui représente une grosse part des ventes de solutions cloud (Salesforce, Google Workspace, Workday…).

1.1.4 Containers as a Service

Les conteneurs en tant que service ou *Containers as a Service* (CaaS) sont une catégorie de services cloud regroupant tout le nécessaire pour permettre aux utilisateurs et développeurs de déployer et de gérer des containers de logiciels. Ils constituent une forme de virtualisation située entre le IaaS et le PaaS dans laquelle les moteurs, l'orchestration et les ressources de traitement sont fournis sous la forme d'un service entièrement géré par le fournisseur.

Un container est une unité « standardisée » regroupant le code, les configurations et les dépendances d'une application afin de pouvoir l'exécuter de la même manière, quelle que soit l'infrastructure sous-jacente.

Avantages

- La plupart des fournisseurs de services cloud proposent des offres CaaS « clé en main » qui regroupent tout le nécessaire pour déployer et gérer des containers, des clusters et des applications.
- Modèle de facturation basé sur l'utilisation des ressources.
- Facilité de déploiement et de gestion : possibilité de créer un container d'application *on-premise* pour ensuite le transférer en production sur le cloud public. L'application fonctionnera toujours de la même façon.

Inconvénients

- Selon le fournisseur, il peut y avoir des limites en matière de technologies disponibles (outils d'orchestration notamment).
- Sécurité des données : localisation des applications et des données plus complexes à appréhender selon les fournisseurs.

Cible

Développeurs de logiciels ou entreprises souhaitant atteindre un haut niveau d'agilité et avoir la capacité de déployer, le plus rapidement possible, de nouvelles ressources de traitement.

1.1.5 Function as a Service

La fonction en tant que service ou *Function as a Service* (FaaS) repose sur le concept d'architecture sans serveur *(serverless).* Les développeurs peuvent s'en servir pour exécuter

une ou plusieurs fonction(s) individuelle(s).

Par exemple une requête Web peut rédiger un message dans une file d'attente, qui sera traité par une autre fonction. La fonction démarre presque instantanément, exécute le traitement, puis le processus s'achève.

Ce modèle est fréquemment utilisé pour créer des microservices (requêtes Web, files de messages, *batchs,* tâches planifiées, gestion des flux d'IoT, etc.).

Avantages

- Le *cloud provider* s'assure que la fonction répond systématiquement chaque fois qu'elle est appelée *(autoscaling).*
- Les clients sont facturés sur la base du volume de fonctions exécutées et du temps d'exécution (mesuré en millisecondes).
- Diminution du coût de gestion de l'infrastructure : une architecture *serverless* permet au développeur de se concentrer sur le code.
- Architecture agnostique.

Inconvénients

- Nécessité de penser (ou repenser) l'application pour la découper en fonctions autonomes.
- Compatibilité du code avec le fournisseur de service choisi : chaque *cloud provider* a son propre *framework* (langages supportés, version des *runtimes,* limite de temps d'exécution…) ; il faudra adapter l'application aux évolutions de la plateforme.
- Coûts difficiles à prévoir et à intégrer aux budgets en raison du modèle de paiement à l'utilisation.
- Dépendance aux outils mis à disposition par le *cloud provider* (*monitoring,* débuggage…).

Cible

Développeurs de logiciels ou entreprises développant des applications IoT ou mobiles, gros consommateurs de traitements par lots…

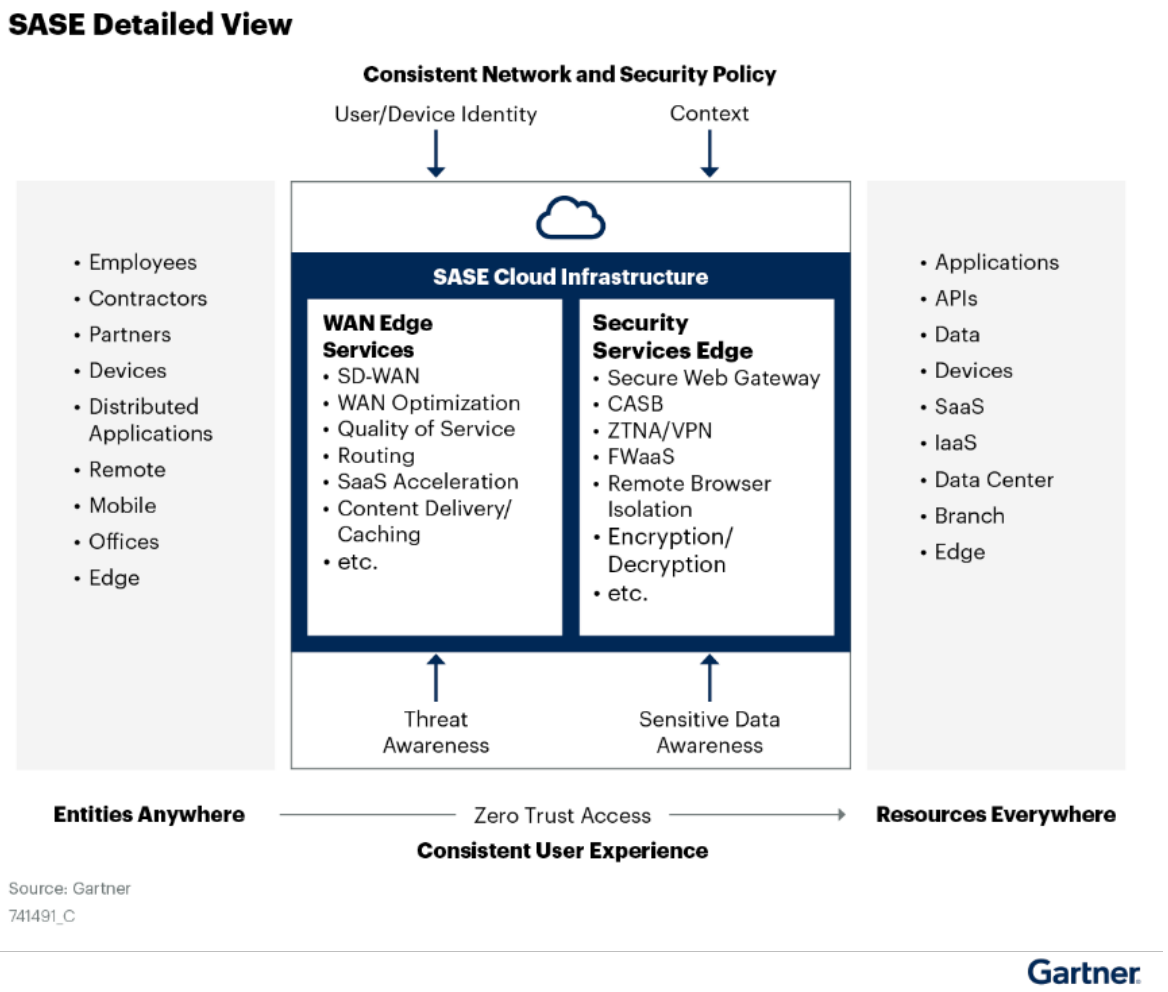
1.1.6 Secure Access Service Edge

Dans un article intitulé "le futur de la sécurité des réseaux est dans le cloud" le Gartner introduisait dès 2019 le nécessaire changement de barycentre de la sécurité, glissant d'un modèle centré sur le datacenter de l'entreprise (interne ou externe) vers un modèle décentralisé multicloud.

Les utilisateurs et les services étant de plus en plus mobiles et externalisés, les besoins en sécurité ne sont plus périmétriques (protection centrée sur le datacenter de l'entreprise), mais attachés à l'utilisateur à travers son équipement et son identité. Le trafic doit être sécurisé tout au long de son parcours, de l'utilisateur à l'application, indépendamment du lieu où se trouve l'utilisateur ou de l'endroit où l'application est hébergée.

Il s'agit d'une vraie rupture avec l'approche traditionnelle centrée sur le réseau, désormais la sécurité sera centrée sur l'utilisateur.

Ce changement donne naissance à un nouveau paradigme, que le Gartner appelle SASE « Secure Access Service Edge » qui regroupe le SD-WAN ainsi qu'un certain nombre de fonctions de sécurité réseau (SWG CASB, DLP, FWaaS, ZTNA…), toutes accessibles et gérées à partir d'une seule plate-forme située dans le cloud. Tous ces nouveaux acronymes sont détaillés dans la suite de ce chapitre.



Lors de l'établissement du modèle SASE (Secure Access Service Edge), le Gartner a répertorié les fonctionnalités « clés », « recommandées » et « optionnelles » suivantes :

Fonctionnalités clés :

SD-WAN « Software-defined wide area network » : Le SD-WAN permet une connectivité résiliente et à faible latence sur tout type de réseau.

Le SD-WAN permet notamment de :

- Utiliser un ensemble de liens hétérogènes ;
- Disposer d'une classification de flux applicatives ;
- Router les flux par application ;
- Intégrer l'interconnexion avec les environnements Cloud ;
- Permettre un contrôle et un déploiement centralisés.

SWG « Secure Web Gateway » :

La Passerelle web sécurisée est une solution de cybersécurité généralement mise en œuvre sous la forme d'un service cloud entre les utilisateurs et le Web.

Les SWG permettent de lutter contre les cybermenaces et les fuites de données en filtrant les contenus indésirables du trafic web, en bloquant les comportements indésirables des utilisateurs et en forçant l'application des politiques de sécurité de l'entreprise.

CASB « Cloud Access Security Broker » : Le CASB permet de gérer le contrôle d'accès pour toutes les applications SaaS, approuvées et non approuvées.

Les solutions de CASB adressent quatre grands axes :

- Améliorer la visibilité sur les applications (y compris le Shadow IT)
- Sécuriser les données sensibles grâce au contrôle des accès et à un système de lutte contre la fuite de données (DLP « Data Leak/Loss Prevention »)
- Protéger contre les menaces grâce à une analyse comportementale
- Simplifier la conformité réglementaire en matière de confidentialité des données

ZTNA « Zero Trust Network Access » :

Le Zero Trust est un modèle stratégique de cybersécurité qui part du principe qu'il n'existe aucune zone de confiance lorsqu'il s'agit de protéger le système d'information et les données de l'entreprise.

Il prend le contre-pied du modèle traditionnel de sécurité, qui considère le système d'information de l'entreprise comme un périmètre de confiance à protéger contre les menaces extérieures (Firewall, DMZ, VPN…).

Le ZTNA est une dénomination plus récente utilisée par les principaux analystes IT qui décrit des produits appliquant une politique de « Zero Trust », ou de moindre privilège, dans le domaine des accès externes.

L'objectif est de fournir les accès strictement indispensables à un utilisateur externe pour qu'il puisse réaliser les tâches nécessaires dans le cadre de son travail sans lui donner de droits ou d'accès superflus pouvant représenter un risque pour la sécurité du système d'information.

Les politiques d'accès sont principalement définies en fonction de :

- L'identité de l'utilisateur, éventuellement renforcée par des mécanismes d'authentification multi-facteurs,
- Les conditions de connexion, comme son lieu de connexion ou « la santé » du terminal utilisé pour la connexion (versions installées, comportements précédents, certificats…)

Le ZTNA permet donc de positionner des accès granulaires sur le système d'information en fonction de l'utilisateur, qu'il soit un collaborateur interne en télétravail ou un prestataire. Cette approche permet de limiter fortement les risques d'intrusion ou d'infection du système d'information.

FWaaS (Firewall-as-a-Service) : Le terme FWaaS désigne les pare-feux fournis en tant que service via le cloud. Une solution FWaaS peut intégrer des fonctions de détection des menaces, d'isolation du réseau, des logiciels anti-malwares et des systèmes IDS/IPS.

DLP « Data Leak/Loss Prevention » Des fonctions de protection/prévention contre la perte de données sont intégrées à l'architecture. Un moteur de protection permet d'obtenir de la visibilité sur les données utilisées, en mouvement et au repos. Il est capable de mettre en quarantaine les données ou les activités à risque, et d'envoyer des alertes de sécurité afin de réduire le risque global d'une violation de données.

Fonctionnalités recommandées :

- Protection des applications Web et des API
- Isolation de navigateur à distance dans le cloud :
- Isolation réseau
- Prise en charge d'appareils gérés et non gérés
- Protection DNS

Fonctionnalités optionnelles :

- Protection des points d'accès Wi-Fi
- Dissimulation/dispersion du réseau

- VPN
- Protection de l'informatique en périphérie

En conclusion, l'extension des réseaux et des ressources des organisations vers le cloud public, nécessite de mettre en place des politiques de sécurité unifiées pour avoir une meilleure visibilité et un contrôle plus efficace.

Divers éléments rendent nécessaire l'approche Zero Trust et SASE :

- Les interactions entre le cloud privé et le cloud public ainsi que le caractère collaboratif entre les deux réseaux,
- Les suites bureautiques peuvent se trouver à la fois dans le système d'information privé et dans le cloud public.
- Les utilisateurs peuvent se connecter de n'importe où, avec tout type d'appareil (Android, PC, iOS, etc.) personnel ou fourni par l'organisation, via n'importe quel réseau privé ou public, domestique, ou professionnel.

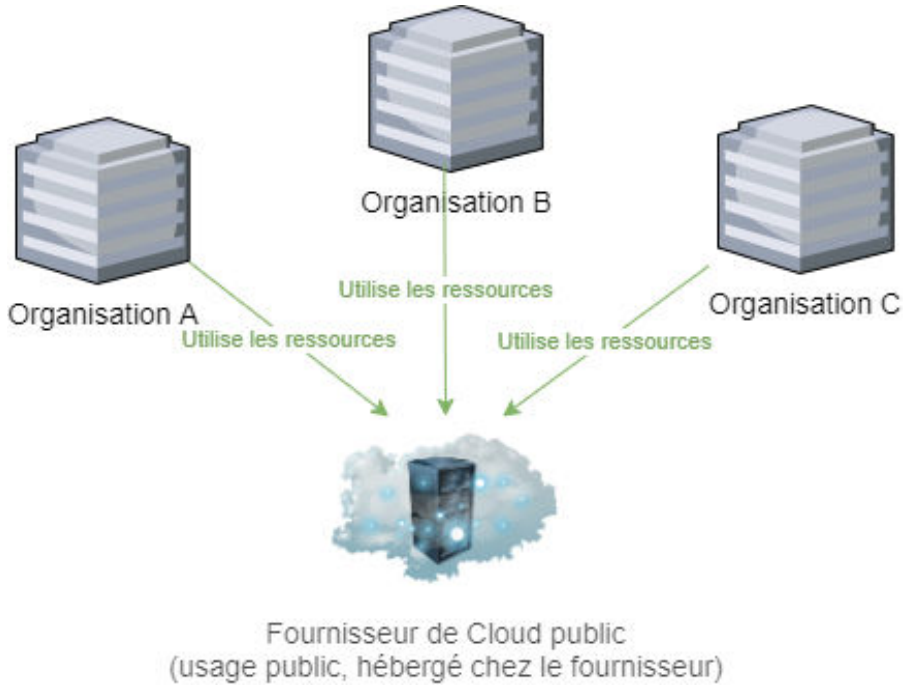
Les niveaux de sécurité des multiples applications SaaS ou internes à l'organisation sont variables selon leurs conceptions, d'où la nécessité d'enrichir la sécurité by design.

1.2 Présentation des modèles de déploiement cloud (public, privé, communautaire, hybride)

Le National Institute of Standards and Technology (NIST) définit quatre modèles de déploiement du cloud[4]. Ces modèles s'appliquent à l'ensemble des types d'offres cloud (IaaS, PaaS, SaaS, etc.) et indiquent comment les technologies sont déployées et consommées. Il s'agit des clouds public, privé, communautaire et hybride.

1.2.1 Cloud public

L'infrastructure cloud et ses ressources de calcul sont accessibles au public à travers Internet. Le cloud public est détenu et opéré par un fournisseur de cloud ; il est donc externe aux organisations. Les infrastructures sont ainsi partagées entre les différents clients du fournisseur bien que les données restent séparées de manière logique (machines virtuelles ou bases de données différentes, par exemple).



Avantages

- Services flexibles (capacité d'évolutivité).
- Utilisation simple (maintenance assurée par le fournisseur).
- Paiement à l'usage.

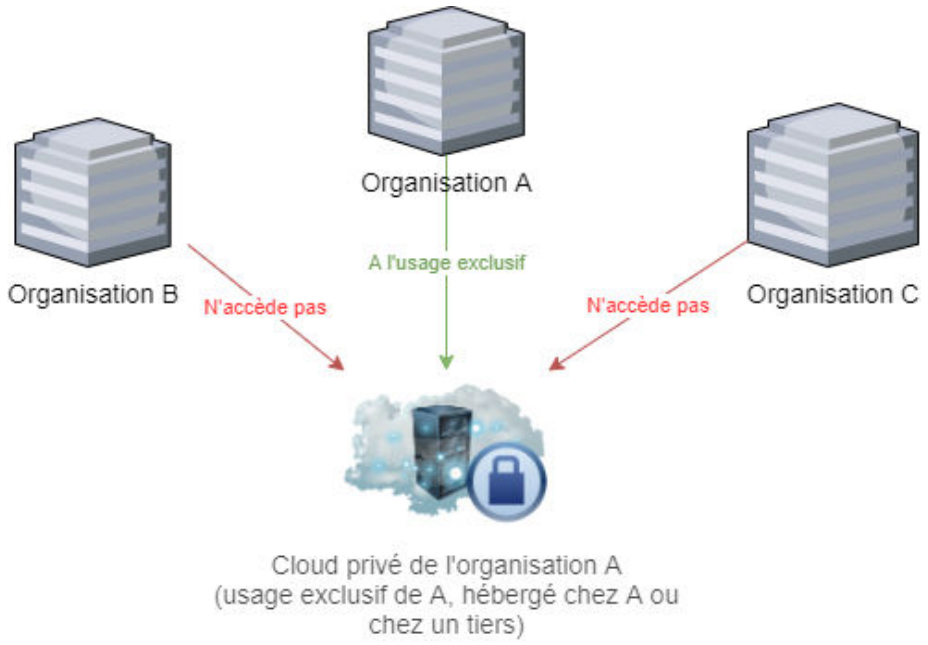
Inconvénients

- Intégration au SI.
- Serveurs externes.
- Difficulté à maîtriser le cycle de vie des données.

[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

1.2.2 Cloud privé

Les ressources de calcul sont opérées exclusivement pour une seule organisation. Elles peuvent être gérées par l'organisation ou par un tiers et peuvent être hébergées au sein des *datacenters* de l'organisation (cloud privé interne) ou à l'extérieur (cloud privé externe). Le cloud privé donne à l'organisation un meilleur contrôle de l'infrastructure, des ressources de calcul et des consommateurs du cloud que dans le cloud public.



Avantages

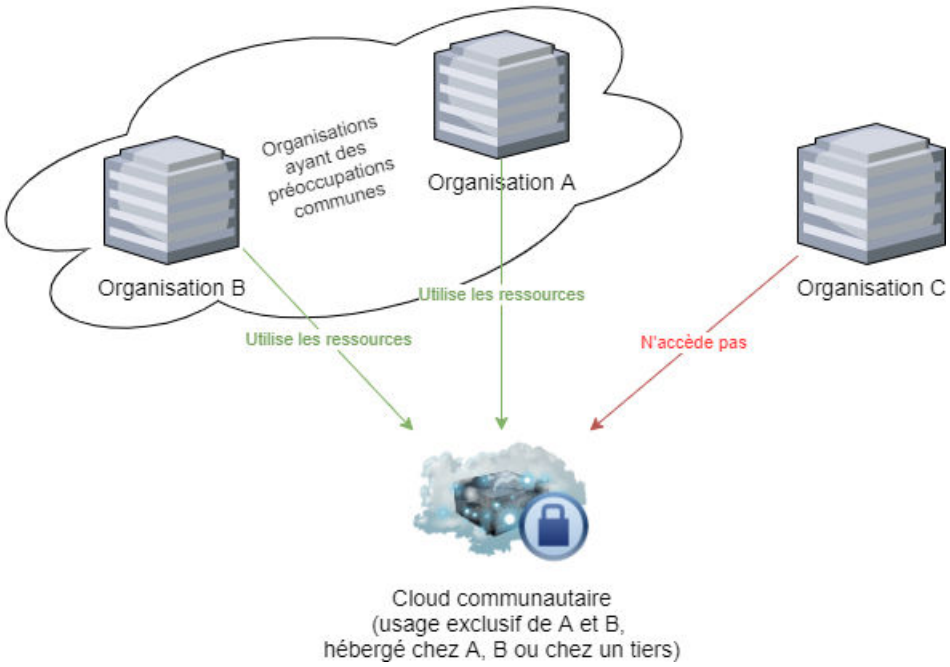
- Contrôle total sur la sécurité des données (configuration du matériel et de l'infrastructure).
- Infrastructure sur mesure pour répondre à des contraintes spécifiques.
- Intégration au SI.

Inconvénients :

- Coût d'installation (investissement important) et coût de possession.
- Scalabilité limitée : limitations liées à l'espace physique disponible et au matériel installé.

1.2.3 Cloud communautaire

Ce type de cloud est relativement similaire au cloud privé excepté le fait que les infrastructures et les ressources de calcul sont partagées par plusieurs organisations qui ont les mêmes considérations réglementaires, de sécurité ou de protection de la vie privée.



Avantages

- Partage du coût de l'infrastructure.

Inconvénients

- Organisation complexe à mettre en place.
- Risque de manque de ressources si l'autre organisation surconsomme et que la capacité totale est insuffisante.

1.2.4 Cloud hybride

L'infrastructure cloud est composée d'au moins deux des types de cloud précédents (public, privé ou communautaire). Les différents modèles de déploiement peuvent être connectés les uns aux autres afin de bénéficier de leurs avantages respectifs (flexibilité, sécurité, coût). Le cloud hybride est communément utilisé pour décrire un datacenter *on-premise* relié directement à un fournisseur de cloud.

Cloud hybride (composition de Cloud privé, Cloud public ou Cloud communautaire)

Avantages

- Scalabilité étendue.
- Possibilité de conserver les données critiques en interne.
- Sur-mesure.

Inconvénients

- Connexion complexe entre cloud privé et cloud public

2 Bien gérer son projet cloud

2.1 L'importance des différentes phases dans un projet cloud

Comme dans tout projet, une fois les phases d'étude (DESIGN) et de planification (PLAN) terminées, un projet cloud peut être décomposé en trois phases principales :

- déploiement (BUILD) : phase de mise en place du projet (installation, paramétrage, rédaction des procédures, etc.) ;
- exploitation (RUN) : phase d'utilisation (vie courante du projet, utilisation de l'outil) ;
- sortie (OUT) : phase de sortie du projet (arrêt complet ou migration vers un système tiers).

Les phases situées en amont et aval du RUN (BUILD et OUT) sont bien souvent oubliées alors qu'elles se révèlent pourtant critiques et ce, potentiellement, d'autant plus dans le cadre d'un projet cloud.

En effet, selon le type de projet cloud (voir chapitre 1.1 « Présentation des types d'offres cloud : IaaS, PaaS, SaaS, CaaS, FaaS »), vous allez peut-être importer et/ou générer beaucoup de données (métier, exploitation, journaux d'événements, etc.) pendant la vie du projet, données qui peuvent se révéler d'une importance capitale pour la société (clients, fournisseurs, contrats, etc.). Or, si pour quelque raison que ce soit, vous souhaitez changer de prestataire cloud, il est fortement recommandé de s'assurer dès le départ que vous allez pouvoir les récupérer dans un format exploitable (réversibilité).

2.2 Étapes d'un projet cloud

Le tableau suivant propose une démarche de déploiement d'un projet cloud. Il souligne l'importance des étapes de cadrage pour s'assurer que le projet est aligné avec les objectifs et priorités métiers, qu'il capitalise les services existants, qu'il est économiquement viable et qu'il réponde aux exigences de sécurité et de réversibilité.

Phases	Objectif
• **Identification du contexte** ○ Besoin métier ○ Typologie des données ○ Typologie des utilisateurs ○ Politique de l'entreprise ○ Politique de sécurité du SI ○ Exigences réglementaires/juridiques	Identifier quelles sont les données sensibles devant être isolées du cloud (*i.e.* : toute fuite ou altération d'information qui amènerait à des risques critiques pour la pérennité de l'entreprise). Identifier les contraintes liées à la protection des données personnelles telle que la vérification de la nécessité de réaliser une étude d'impact sur la vie privée (PIA).
• **Alignement du projet avec la stratégie de l'entreprise** ○ Budget/ROI ○ Degré de dépendance	Choix du type d'offre et modèle de déploiement cloud en fonction des contraintes, des services existants, de la stratégie et des besoins métiers.

• **Définition de la gouvernance projet** (Plan d'assurance qualité)	Définir les rôles, les responsabilités, les actions de gouvernance (existantes ou nouvelles) et les métriques utiles au pilotage.
• **Appréciation des risques** (Système d'Information, service ou application à externaliser)	Identifier les actifs, définir les exigences de sécurité (DICT/P), identifier les menaces et vulnérabilités, estimer les niveaux de risques, accepter ou remédier aux risques. À titre d'exemple, il faut notamment réaliser l'étude de la sensibilité des données qui seront transférées dans le cloud.
• **Choix du prestataire** o Certifications o Flexibilité contractuelle o Périmètre d'intervention o Niveau d'engagement/SLA o Niveau de sécurité o Juridiction(s) applicable(s) o Localisation des données o Coût	Mise en concurrence afin de choisir la meilleure offre selon les critères définis précédemment. Certifications : ISO 27001, HDS (pour les données de santé), SecNumCloud, SOC, etc. permettant d'avoir une évaluation objective du niveau de sécurité. Flexibilité contractuelle : possibilité de négocier/modifier les termes du contrat. Périmètre d'intervention : services proposés par le prestataire, définition claire des responsabilités (prestataire/client). Niveau d'engagement : exigences claires en termes de niveau de qualité de service (coût, délai, résultat). Niveau de sécurité : voir la synthèse des principaux critères en annexe ou le questionnaire d'auto-évaluation du Cloud Security Alliance (CSA) récent et référencé sur l'annuaire STAR[5]. Juridiction(s) applicable(s) : 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. Localisation des données : possibilité de connaître et/ou choisir la localisation des données afin d'être en conformité avec la politique de l'entreprise et les contraintes réglementaires.
• **Contractualisation**	• Vérification du cadre juridique et réglementaire des données du client hébergées et traitées par l'opérateur cloud. • Mise en place d'un plan d'assurance sécurité (PAS). • Les clauses sont à analyser selon quatre axes : o Prix du service ; o Engagement sur les délais ; o Engagement sur le service rendu (renvoi au CSA, partie 3, international et RGPD) ; o Modalités du règlement des litiges (voir partie « risques juridiques »). Pour une analyse plus complète, se référer à « Checklist des clauses contractuelles » en annexe.

[5] https://cloudsecurityalliance.org/star/registry

• **Mise en place du projet (BUILD) et configuration de la sécurité**	Ne pas oublier le paramétrage de la sécurité dont la responsabilité revient au client (fortement dépendant du type d'offre et du modèle de déploiement cloud). Mise en place des services de sécurité (sauvegarde, chiffrement, anonymisation, prévention des menaces, prévention de la fuite de données, supervision, hygiène (gestion des vulnérabilités, *patch management*)). Définition de la gouvernance incluant la matrice de responsabilité (RACI) et la nécessité éventuelle de l'accompagnement au changement. Évolutivité : prévoir l'extension du service.
• **Maintien opérationnel de la sécurité dans le cloud (RUN)** o Déclinaison opérationnelle des exigences de sécurité o Visibilité sur la gestion et traçabilité sur les incidents o Gouvernance mise en place pour y répondre. o Maintien des certifications à isopérimètre.	Déclinaison opérationnelle des exigences de sécurité : • Sécurité fournie par le fournisseur ; • Sécurité à la responsabilité du client : o Compétences internes pour la gestion de la sécurité dans le cloud externe. Sécurité : voir liste des services évoqués dans le BUILD, revue régulière des habilitations, etc. Selon la sensibilité des données, contrôle du niveau de sécurité. Transparence : relative aux événements de sécurité (communication des rapports d'incidents, des journaux d'événements, etc.), possibilité de contrôle (audits, tests d'intrusion, etc.), actualisation du plan d'assurance sécurité (PAS). Gouvernance : exécution de la matrice de responsabilité RACI (voir explication + équipe type en annexe), suivi de la prestation et des niveaux de service. Suivi des usages pour s'assurer de l'adhérence des utilisateurs à la solution.

3 Sécurité dans le cloud

3.1 Fondamentaux de la cybersécurité dans le cloud

La sensibilité d'un actif (information, processus) est usuellement caractérisée selon trois critères : disponibilité, intégrité et confidentialité, avec parfois un quatrième critère de traçabilité ou de preuve (se référer au tableau DICT/P en annexe 3 pour une description plus complète de ces derniers).

Dans un contexte cloud, il convient d'ajouter au DICT/P deux critères de sécurité supplémentaires : la réversibilité et la capacité à localiser les droits applicables.

La **réversibilité** est l'opération de retour de responsabilité technique, par lequel le pouvoir adjudicateur reprend les prestations qu'il avait confiées au titulaire du marché d'infogérance arrivant à terme (Art. 31-4 du CCAG-TIC). C'est la capacité du prestataire à rendre l'intégralité des données et métadonnées, à conserver les données dans un format ouvert, exploitable, et réutilisable par soi ou un autre prestataire.

La **capacité à localiser les droits applicables** est la propriété d'être géographiquement localisable afin de contribuer à la détermination des législations potentiellement applicables. C'est la capacité du prestataire à pouvoir localiser les données, les fixer en un lieu déterminé, à lister exhaustivement les pays hébergeant les données et ne pas en changer, et à identifier où se situent les intervenants agissant pour son compte sur les données.

Sans ces critères, la sécurité de l'information n'est pas correctement caractérisée pour l'appréciation des risques et la décision de la direction face aux enjeux.

3.2 Introduction à la gestion des risques

Bien que la gestion des risques n'ait rien de spécifique au cloud, elle nous a semblé en être un aspect particulièrement important, d'où la présence d'un chapitre dédié au sein duquel nous avons tenté de vulgariser et simplifier la démarche.

3.2.1 L'approche par les risques, pourquoi ?

Face à un événement redouté, une réaction improvisée menée sans coordination entre les différents acteurs conduit souvent à des préjudices importants pouvant aller jusqu'à remettre en cause l'existence même d'une entreprise. C'est pourquoi le management du risque doit faire partie intégrante de la gouvernance des organismes et de leurs systèmes d'information. Il permet aux organisations d'anticiper des décisions à prendre en fonction d'événements redoutés et de scénarios de menaces qui pèsent sur l'organisation.

L'ensemble des mesures, postures, solutions à mettre en place pour définir une gestion de risques peut viser à :

- réduire le risque ou minimiser ses conséquences (*cf.* notion de « plan de prévention ») ;
- placer une entreprise dans un état dégradé mais stable lorsqu'une attaque a été subie (*cf.* notion de « plan de continuité d'activité » ou « PCA ») ;
- rétablir la situation antérieure (*cf.* notion de « plan de reprise d'activité » ou « PRA »).

Ainsi, une approche par la gestion des risques permet de prendre en compte ceux qui sont liés à l'organisation, ses activités et d'apporter des réponses adaptées (financières, humaines, techniques, etc.) en fonction des niveaux de risques.

3.2.2 Méthodologies

Plusieurs méthodologies de gestion des risques existent, qui se distinguent par leur approche spécifique des risques adaptée à l'organisation (EBIOS 2010, EBIOS-RM, ISO 27005, MEHARI, etc.).

L'avantage d'utiliser une méthode est de disposer d'un cadre permettant de réussir l'analyse de risques et bénéficier de référentiels, notamment dans la nature des risques et des menaces. La connaissance et l'utilisation de ces méthodes sont particulièrement utiles lorsque vous souhaitez structurer votre approche.

3.2.3 Processus de définition d'une gestion du risque

Comme précisé au paragraphe précédent, il existe de nombreux référentiels pour gérer les risques, nous donnons ici un processus général de gestion des risques afin d'illustrer nos propos.

Étape	Objectif
Établir le contexte	Définir le contexte de l'organisation : chaque organisation est différente, notamment dans son approche à la gestion des risques. Définir son contexte interne et externe (y compris les réglementations applicables) permet ainsi d'adapter sa gestion des risques en fonction de son environnement et d'y associer les responsabilités.

Définir les métriques	Définir les métriques de l'organisation : en fonction de son historique, il convient que cette activité se réalise avec l'ensemble des entités de l'organisation pour définir ces critères.
	
	Métriques à prendre en considération :
	
	• Critères de sécurité (DICT/P) :
	  ○ Niveaux de disponibilité (D),
	  ○ Niveaux d'intégrité (I),
	  ○ Niveaux de confidentialité (C),
	  ○ Niveaux de traçabilité/Preuve (T/P) ;
	• Niveaux de gravité ;
	• Niveaux de vraisemblance.

Identifier les actifs à protéger	Identifier les actifs essentiels de l'organisation : que cherche-t-on à protéger ? Cette question est le fondement de l'analyse de risques, l'identification des actifs est une activité à réaliser avec l'ensemble des entités de l'organisation. Une proposition d'approche est disponible en Annexe : Identification des actifs.
Identifier les événements redoutés	Identifier les événements que l'organisation redoute, qu'elle ne veut pas voir se produire, ils peuvent être de plusieurs ordres : légaux, d'image, financier, technique, etc.
Identifier les sources de menaces	Identifier les sources de menaces qui pèsent sur l'organisation, avec des facteurs humains, techniques, légaux, etc.

Analyser et déterminer les niveaux de risques	Déterminer le niveau de chaque risque permet de le situer à un instant T et de suivre son évolution dans le temps. Il conviendra de prendre en compte l'évolution de chaque risque dans le processus d'amélioration continue.
Traitement du risque	Traiter les risques, compte tenu des spécificités du contexte : • Acceptation du risque ; • Réduction du risque ; • Élimination du risque ; • Partage du risque acceptable.
Déterminer les mesures à mettre en œuvre	Une fois le risque apprécié, l'organisation va mettre en place des mesures techniques et organisationnelles, avec un suivi par des indicateurs (ou métriques), pour réduire ses probabilités de survenance.
Déterminer le risque résiduel	Le risque résiduel est celui qui subsiste après avoir mis en œuvre le traitement du risque.
Approbation	L'objectif est d'approuver l'analyse des risques et des risques résiduels associés par leurs propriétaires. Cette étape doit être réalisée par des personnes ayant suffisamment d'autorité au sens légal du terme (*i.e.* : dirigeants de l'entreprise).
Surveillance et réexamen des risques	Les risques ne sont pas figés. Les menaces, les vulnérabilités, la vraisemblance ou les conséquences peuvent changer en fonction du contexte. Par conséquent, une surveillance adaptée est nécessaire pour identifier les changements et les vulnérabilités quotidiennes. Le management du risque est une activité itérative qui aide à atteindre les objectifs et prendre des décisions en adéquation avec le contexte de l'organisation.

3.3 Risques liés à un déploiement non maîtrisé dans le cloud

3.3.1 Maîtriser la complexité de l'offre cloud

Il est d'usage d'avoir peur de ce qui n'est pas compris. Depuis la montée en puissance des technologies cloud, des mots à la mode (« *buzzwords »)* se sont multipliés, positionnant les néophytes dans un brouillard de terminologies.

Par conséquent, il est difficile de construire une relation de confiance, même avec les plus gros fournisseurs comme Microsoft, Google et Amazon. Alors qu'ils ne comprennent que partiellement le fonctionnement de ces nouveaux outils, les utilisateurs se laissent pourtant tenter. D'autres refusent de franchir le pas du *cloud*, faute de confiance et prétextant bien souvent des technologies défaillantes d'un point de vue de la sécurité.

Maîtriser le vocabulaire que nous impose notre fournisseur de cloud est donc indispensable.

Bien qu'une base commune existe, à commencer par les typologies de cloud (IaaS, SaaS, PaaS etc.), chaque fournisseur y va de ses appellations pour des services similaires dans les usages.

Prenons l'exemple de la machine virtuelle :

- Amazon Web Services (AWS) : Instance EC2 ;
- Google Cloud Platform (GCP) : Compute Engine ;
- Microsoft Azure : Virtual Machine.

Et le vocabulaire se complexifie rapidement avec la multiplication des services proposés par chacun des fournisseurs. Pour ne prendre que l'exemple d'AWS et à titre d'information, plus de 175 services étaient proposés fin 2019. Régulièrement, de nouvelles fonctionnalités sont ajoutées ou modifiées, demandant aux utilisateurs un travail de veille et d'adaptation constant.

Fort heureusement, les solutions de type SaaS nécessitent généralement un apprentissage moindre. Les grandes plateformes simplifient les codes d'utilisation pour rendre accessibles leurs applications au plus grand nombre. Les plus grands consommateurs de ces applications de type « *as a Service* » ne sont plus uniquement des professionnels de l'informatique.

3.3.2 Sécuriser la configuration et le paramétrage

La compréhension et la sécurisation d'un environnement cloud se résument en un partage des responsabilités qui dépendent du type d'offre cloud (voir schéma du chapitre 1.1 « Présentation des types d'offres cloud : IaaS, PaaS, SaaS, CaaS, FaaS ») qui ne doit laisser subsister aucune zone d'ombre.

Pour ce qui est des éléments de sécurité portés par le fournisseur, les engagements sont souvent tenus. Pour vous en assurer, vérifiez les éléments contractuels, renseignez-vous sur les déclarations d'intention et les actions de sécurité engagées (voir chapitre « Éléments contractuels »). N'hésitez pas à consulter l'annuaire STAR du site de Cloud Security Alliance[6] pour vérifier si le fournisseur que vous convoitez n'a pas déjà rempli le questionnaire d'auto-évaluation *(self-assessment),* cela vous permettra le cas échéant et si le questionnaire est suffisamment récent d'avoir une idée précise du niveau de maturité du fournisseur. Si vous le pouvez, n'hésitez pas à auditer. Les engagements et investissements en matière de cybersécurité des fournisseurs cloud sont généralement à la hauteur de leurs responsabilités. Et même si la sécurité absolue n'existe pas et que des incidents ont déjà été relevés, il en va de leur image de marque et leur modèle économique. Une cyberattaque qui impacterait ou compromettrait fortement les services cloud de ces fournisseurs engendrerait inéluctablement une perte de confiance non négligeable des clients associée à des conséquences financières importantes.

En revanche, pour ce qui n'est pas à la charge du fournisseur (voir schéma du chapitre 1.1 « Présentation des types d'offres cloud : IaaS, PaaS, SaaS, CaaS, FaaS »), il est de la responsabilité du consommateur de services cloud de s'assurer du bon niveau de sécurité par rapport à ses besoins.

Pour cela, une analyse doit être menée afin de jauger du niveau de sécurité auquel le consommateur doit se soumettre. Les contraintes peuvent provenir d'un contexte réglementaire fort, des propres clients des consommateurs de services cloud, ou des risques business.

Opérationnellement, il revient au consommateur de cloud de configurer de manière sécurisée son environnement. Bien souvent, une panoplie complète de fonctionnalités de sécurité est proposée. Il convient alors d'évaluer la pertinence des services de sécurité du fournisseur et l'efficience de chacun d'entre eux. Dans le cas où ces derniers ne seraient pas estimés à la hauteur, des alternatives acceptables doivent être identifiées. Elles peuvent être d'ordre organisationnel, technique ou motivées par la limitation des usages sur le cloud concerné.

Il est certain que les réflexions de sécurisation des configurations doivent être menées le plus en amont possible d'un projet de migration vers le cloud afin d'éviter des retours en arrière

[6] https://cloudsecurityalliance.org/star/registry

souvent fastidieux, si ce n'est impossibles.

Mais attention, la sécurité n'est pas qu'une affaire de spécialistes de la technique et cela peut souvent demander l'implication combinée des équipes juridiques et métiers en plus des équipes techniques.

3.3.3 Maîtriser sa consommation de services cloud

Les fournisseurs cloud proposent de nombreux moyens de consommer leurs services.

Sur des modèles SaaS, les usages sont souvent simples : une plateforme est mise à disposition de l'utilisateur qui va consommer les outils mis à sa disposition. Il lui faut alors disposer de moyens de superviser ces consommations afin de détecter tout écart par rapport à sa politique de sécurité. La maîtrise de la sécurité dans le cloud repose donc sur deux outils indispensables : un tableau de bord couplé à un système de détection. Les indicateurs générés sont souvent utilisés pour sensibiliser les utilisateurs aux bons comportements à adopter, ces statistiques provenant directement de leurs usages et non d'études généralistes effectuées au niveau mondial.

L'autre aspect de la maîtrise de la consommation est directement lié à la gestion financière, nombreux sont en effet les utilisateurs s'étant retrouvés avec des factures mensuelles bien plus élevées que ce qui avait été prévu en amont du projet. De nouveaux métiers ont d'ailleurs émergé de ces problématiques : derrière l'appellation « FinOps », on retrouve ainsi pléthore de spécialistes de l'estimation et de l'optimisation des coûts des services cloud capables d'établir des prévisions de manière très fine pour, *in fine,* recommander d'utiliser telle offre plutôt qu'une autre et dans telle configuration.

3.3.4 Rester libre

Les promesses et les avantages du cloud sont nombreux. Performance, simplicité des usages, haute disponibilité, accessibilité, des fonctionnalités en perpétuelle amélioration, etc.

Bien que certains responsables de la sécurité, voire certains DSI soient encore parfois réticents à faire ce choix, les décideurs et les métiers n'hésitent pas à franchir le pas et à opter pour une consommation généralisée de services cloud.

En revanche, la problématique d'un retour en arrière ou la possibilité de migrer vers un autre fournisseur cloud sont souvent peu abordées ou trop tardivement dans le déroulé d'un projet. Quand la bascule est faite, la dépendance au fournisseur est souvent très forte.

C'est un point qui doit pourtant être abordé en amont de tout projet. Les fournisseurs de cloud le savent, si la migration vers leurs services est simple, le retour en arrière l'est souvent moins.

Cette dépendance au fournisseur ne permet pas d'échapper aux possibles conséquences suivantes : augmentation des tarifs, dégradation de la fiabilité des services, voire fermeture autoritaire d'un service.

Même si cela est complexe, rendre ses applications cloud « agnostiques » peut s'envisager. Il faut considérer la manière et les conditions contractuelles et juridiques de récupérer ses données, de tester la capacité du fournisseur à exporter des infrastructures et des services vers un autre environnement, et de se rapprocher d'un autre fournisseur cloud enclin à vous offrir des formations pour anticiper une prochaine migration.

3.3.5 Ne pas oublier…

Les accès à des services cloud sont logiquement bien plus dépendants de la qualité de la connexion réseau que des services situés sur le même réseau local *(on-premise)*. Aussi, il est primordial d'anticiper les aspects relatifs à la bande passante, la latence et la disponibilité de la connexion réseau reliant les utilisateurs et le(s) service(s) cloud.

Un autre aspect trop souvent négligé est lié à tout ce qui concerne la journalisation rattachée à la question de la gestion des traces. En effet, il est important de bien définir ses besoins en matière de traçabilité des actions effectuées (types d'événements, durée de rétention, etc.) au sein du service cloud et de s'assurer que la solution convoitée y réponde soit nativement, au travers d'une interface, soit à la demande, lorsque les données sont sous la responsabilité du fournisseur. Cela, *a minima,* afin d'anticiper les besoins associés à d'éventuelles analyses forensiques qui pourraient s'avérer nécessaires à la suite d'un incident de sécurité par exemple.

3.4 Amélioration de la sécurité de ses applications cloud

3.4.1 Rédiger un cahier de bonnes pratiques

Le recours aux applications cloud est de plus en plus fréquent, et leur simplicité d'utilisation ne doit pas faire oublier qu'elles peuvent héberger un certain nombre de données sensibles de l'entreprise.

Il est dans ce cadre recommandé de déterminer les règles qui doivent être suivies par les différents fournisseurs des applications cloud implémentées au sein d'une même structure. L'ensemble de ces règles sont à rappeler dans le cahier des charges de chaque nouvelle application.

Le contenu du cahier des charges dépendra de chaque entité, ses éléments pourront être résumés en trois grandes catégories :

- sécurisation des accès ;
- protection contre la perte de données ;
- respect des réglementations.

Ce cahier des charges pourra utilement être complété à l'occasion de retours d'expérience d'exercice ou de cas concrets de gestion de crise.

Pour ceux qui souhaitent aller dans le détail des mesures à appliquer, il est par exemple possible de se référer au MITRE ATT&CK[7] ou au référentiel SecNumCloud[8].

3.4.2 Sécurisation des accès

1. Gestion des permissions

Comme pour toutes les ressources numériques d'une entreprise, les applications cloud doivent être protégées par une solution de gestion des permissions et des accès. Au sein de chaque application, il est indispensable de distinguer les profils d'utilisateurs et de déterminer pour chacun les permissions à accorder :

- administration technique de la plateforme ;
- gestion des profils utilisateurs et administration fonctionnelle ;
- utilisation classique ;
- limitation des accès aux données.

[7] https://attack.mitre.org/matrices/enterprise/cloud/

[8] https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf

Une fois ces éléments déterminés, les différents rôles des utilisateurs peuvent être créés et leur être attribués (modèle RBAC).

Une bonne coopération entre la direction des ressources humaines et la DSI est primordiale de façon à être synchrone et en capacité de gérer les mouvements de personnel ainsi que les droits accordés sur les données et les applications métiers.

2. Centralisation de l'authentification

L'ajout d'application ne doit pas être synonyme de multiplication des comptes mis à disposition des utilisateurs. La création d'un compte sur chaque application présente en effet de multiples inconvénients :

- format d'identifiant et mot de passe pouvant différer d'une application à l'autre ;
- multiplication des identités à créer/sécuriser/superviser/désactiver, ce qui complexifie le cycle de vie de ces identités et la gestion des entrées/sorties des utilisateurs.

De nombreuses solutions (Okta, Pingfederate, Azure AD, Google Identity Platform…) permettent à ce jour de centraliser l'authentification des utilisateurs. On parle alors de « fédération ». Les applications peuvent disposer d'une base de comptes et de permissions locales, mais l'étape de connexion est déléguée à un système tiers *via* l'un des protocoles supportés (SAML, OAuth…). Cette authentification centralisée peut être réalisée hors Cloud (ie : ADFS), par un service Cloud souscrit par l'entreprise (ie : Azure AD) ou par un service Cloud géré par un tiers (ie : OpenID Connect).

Cette centralisation de l'étape de connexion permet alors de répondre aux inconvénients listés ci-dessus :

- l'utilisateur s'authentifie sur une plateforme unique, centralisée, avec un format d'identifiant unique ;
- lors du départ d'un utilisateur, la désactivation de son compte bloque automatiquement l'accès à toutes les applications ;
- l'administration des comptes est centralisée sur l'outil de fédération.

3. Authentification forte

D'après Microsoft, 99,9 % des attaques de compte pourraient être évitées grâce à l'authentification à deux facteurs[9].

Ce type de connexion impose à l'utilisateur de fournir deux éléments différents permettant de prouver son identité. Ces éléments doivent être sélectionnés au sein de deux catégories distinctes dans la liste suivante :

- Ce que je sais (mot de passe, PIN…) ;
- Ce que je possède (téléphone, badge, clé USB, périphérique d'entreprise, *token*…) ;
- Ce que je suis (empreinte digitale, reconnaissance faciale…) ;

L'activation de ce type de connexion ne doit toutefois pas entraver la connexion aux différents outils et applications de l'utilisateur en lui demandant sans cesse de saisir des codes à usage unique. La combinaison avec la centralisation de l'authentification permet de limiter le nombre de demandes envoyées à l'utilisateur sans pour autant en diminuer le niveau de sécurité.

4. Provisionnement des comptes

L'authentification des utilisateurs de manière centralisée ne permet pas de se dédouaner de la gestion du compte utilisateur. L'utilisateur doit en effet être connu pour disposer des permissions qui lui sont accordées, et être identifié lors de ses différentes actions.

---

[9] https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

La méthode de provisionnement et de suppression des comptes des utilisateurs doit être déterminée et automatisée au maximum pour simplifier les processus d'arrivée, de mobilité et de départ des utilisateurs.

Un seul compte centralisé permettant d'accéder à plusieurs services, il est d'autant plus important de réaliser des revues de compte régulières.

5. Connexion réseau

Lorsque le nombre et/ou le niveau de sensibilité des services cloud utilisés par un organisme est critique, il peut être intéressant de réfléchir, lorsque le fournisseur le propose, à mettre en place des connexions privées depuis l'organisme vers les services cloud.

Ce type de solution permet d'améliorer le niveau de sécurité ainsi que la qualité de connexion vers les services cloud.

On peut notamment citer Azure ExpressRoute Direct chez Microsoft, AWS Direct Connect chez Amazon et Google Interconnect chez Google.

3.4.3 Menaces et fuite de données

Les applications cloud hébergeant une partie des données de l'entreprise, celles-ci doivent respecter les mêmes exigences que celles du SI interne :

- protection des données (y compris des données personnelles) ;
- sécurisation des accès (voir ci-dessus) ;
- maîtrise des lieux de stockage des données ;
- protection contre l'exfiltration et les transferts de données inter-applications ;
- etc.

La protection contre la fuite des données et la lutte contre les menaces peuvent, entre autres, être implémentées *via l'utilisation de services tels que le* CASB *(Cloud Access Security Broker),* le DLP (Data Loss/Leak Prevention) ou encore le XDR (eXtended Detection and Response) qui viennent se positionner entre l'utilisateur et le fournisseur du service cloud ou directement sur l'équipement à protéger. Ce type de services permet :

- d'analyser les applications utilisées, les données accédées et le comportement de l'utilisateur :
- d'acter le respect des règles de sécurité de la structure :
- d'alerter les administrateurs :
- d'effectuer les remédiations.

La classification et le chiffrement des données permettent également de cadrer leur diffusion notamment dans le cas des données sensibles. Dans le cadre du chiffrement, il est important de noter que celui-ci peut se baser sur des clés détenues par le fournisseur de cloud ou par l'organisation.

3.4.4 Réglementation, normes et certifications

Chaque entreprise, en fonction de son activité et de sa localisation, est soumise au respect de certaines normes et/ou réglementations (liste non exhaustive).

Réglementations

- DSP2 (Directive européenne sur les Services de Paiement v2) : prestataires de service de paiement (dont ceux sans carte de crédit).
- LPM (Loi de Programmation Militaire) : loi applicable aux opérateurs d'importance vitale (OIV).

- RGPD (Règlement Général pour la Protection des Données personnelles) : traitement des données de citoyens européens ou organismes exerçant leur activité sur le territoire européen et manipulant des données personnelles.
- NIS *(Network and Information System Security)* : directive européenne s'appliquant aux opérateurs de services essentiels (OSE) et fournisseurs de services numériques (FSN).
- RGS (Référentiel Général de Sécurité) : référentiel applicable aux SI de l'Etat.
- Etc.

Certaines réglementations étrangères peuvent avoir un impact sur la confidentialité des données, on peut notamment citer le Cloud Act et le Patriot Act qui permettent aux autorités américaines (avec ou sans mandat) d'avoir accès aux données des sociétés américaines qu'elles soient situées sur le territoire américain ou non ainsi que des sociétés étrangères situées sur le territoire américain.

Normes

- ISO 27001 : permet d'attester la mise en œuvre de processus dans le cadre d'un système de management de la sécurité de l'information (SMSI).
- ISO 27018 : définit les règles de sécurité à appliquer pour les fournisseurs de cloud public afin d'assurer la protection des données personnelles, garantir la transparence et se conformer à leurs obligations réglementaires.
- PCI-DSS *(Payment Card Industry Data Security Standard)* : normes de sécurité des données applicables à l'industrie des cartes de paiement.
- Etc.

Certifications

Il n'existe à ce jour que quelques certifications applicables au cloud telles que SOC 1, SOC 2, SecNumCloud, HDS (Hébergement de données de santé), etc.

La mise en avant des certifications par un éditeur ne doit pas pour autant être synonyme de confiance totale. Il est donc important de contrôler les points suivants pour chacun des éléments présentés :

- Quel est le périmètre couvert par la certification ?
- Quelle est la date de la certification (n'est-elle pas expirée) ?
- Quel organisme est à l'origine de la certification présentée, son accréditation est-elle encore valable ?
- Ces certifications correspondent-elles aux réglementations s'appliquant à mon environnement ?

A noter qu'au niveau de l'ANSSI, il existe une différence entre certification et qualification, à titre d'exemple SecuNumCloud est catégorisé en tant que qualification.

ANNEXES

1 Glossaire

- **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) : autorité nationale (France) en matière de sécurité et de défense des systèmes d'information.
- **API** *(Application Programming Interface)* : ensemble normalisé de classes, de méthodes, de fonctions et de constantes par laquelle un logiciel propose des services à d'autres logiciels. Elle est offerte par une bibliothèque logicielle ou un service Web, le plus souvent accompagnée d'une description qui spécifie comment des programmes consommateurs peuvent se servir des fonctionnalités du programme fournisseur.
- **API REST** : style architectural et méthodologie fréquemment utilisés dans le développement de services Internet, tels que les systèmes hypermédias distribués. Par exemple, lorsqu'un développeur demande à l'API Twitter de récupérer l'objet d'un utilisateur (une ressource), l'API renvoie l'état de cet utilisateur, son nom, ses abonnés et les publications partagées sur Twitter.
- **AWS** *(Amazon Web Services)* : plateforme de services cloud du fournisseur Amazon.
- **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.
- **CaaS** *(Container as a Service)* : voir « Présentation des types d'offres ».
- **CCAG** *(Cahier des Clauses Administratives Générales)* : recueil de clauses fixant les principaux aspects contractuels applicables à toutes les prestations d'une même nature pour les acheteurs publics.
- **CMS** *(Content Management System)* ou système de gestion de contenu en français : solution visant à faciliter la création, l'édition, la publication et la diffusion d'informations sur les sites Web, les blogs et les portails Internet.
- **CNIL** *(Commission Nationale de l'Informatique et des Libertés)* : autorité administrative indépendante et régulatrice chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
- **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 ».
- **DLP** (Data Leak/Loss Prevention) : le DLP fait référence à un ensemble de techniques qui permettent d'identifier, de contrôler et de protéger l'information grâce à des analyses de contenu approfondies.
- **DMZ** *(DeMilitarized Zone)* : zone démilitarisée, sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Contient généralement les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.
- **DSP2** *(Directive européenne sur les Services de Paiement v2)* : directive européenne à destination des organismes proposants des services de paiement et visant à garantir un accès équitable et ouvert aux marchés des paiements et à renforcer la protection des consommateurs.
- **DSI** : Directeur des systèmes d'information ou Direction des systèmes d'information
- **EBIOS** *(Expression des Besoins et Identification des Objectifs de Sécurité)* : méthode d'évaluation des risques maintenue par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

- **EC2** *(Amazon Elastic Compute Cloud)* : Service AWS proposant la location de machines virtuelles
- **ERP** *(Enterprise Resource Planning)* : système d'information qui permet de gérer et suivre au quotidien, l'ensemble des informations et des services opérationnels d'une entreprise.
- **FaaS** *(Function as a Service)* : voir « Présentation des types d'offres ».
- **Fédération d'identité (service de)** : concept qui vise à mettre en place une centralisation des données, notamment des données d'identité, au sein d'un domaine informatique. Ainsi, un utilisateur ne se connectera qu'une unique fois par session auprès d'une structure reconnue qui lui fournira la preuve de son identité.
- **FinOps :** approche, méthodologie, contraction des termes finance et opération, qui vise à monitorer et optimiser les coûts en matière de *cloud computing*.
- **FWaaS** (Firewall-as-a-Service) : le terme FWaaS désigne les pare-feux fournis en tant que service via le cloud.
- **GCP** *(Google Cloud Platform)* : plateforme de services cloud du fournisseur Google.
- **HDS** (hébergeurs de données de santé) : la certification HDS est obligatoire pour l'hébergement et l'infogérance des services et applications contenant des données de santé identifiables et personnelles.
- **IaaS** *(Infrastructure as a Service)* : voir « Présentation des types d'offres ».
- **IP** *(Internet Protocol)* : Famille de protocoles de communication de réseaux informatique conçus pour être utilisés sur Internet, les plus courants sont les versions 4 (IPv4) et 6 (IPv6).
- **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.
- **LPM** *(Loi de Programmation Militaire)* : loi visant à établir une programmation pluriannuelle des dépenses que l'État français consacre à ses forces armées.
- **MEHARI** *(Méthode Harmonisée d'Analyse des Risques)* : méthode de gestion de risque développée par le Clusif.
- **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.
- **NIS** : directive « Network and Information System Security » adoptée en juillet 2016 dont l'objectif principal est d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne.
- **NIST** *(National Institute of Standards and Technology)* : agence du département du Commerce des États-Unis dont le but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie.
- **OAuth** : protocole libre qui permet d'autoriser un site Web, un logiciel ou une application (dite « consommateur ») à utiliser l'API sécurisée d'un autre site Web (dit « fournisseur ») pour le compte d'un utilisateur. OAuth n'est pas un protocole d'authentification, mais de « délégation d'autorisation ».
- **OIV** *(Opérateur d'Importance Vitale)* : en France, organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.
- **On-Premise** : littéralement « dans les locaux » ou « sur site ». Modèle d'utilisation ou de licence s'appliquant à tout ou partie d'un SI et/ou d'une infrastructure lorsque cette dernière est physiquement située dans les locaux de l'entreprise.
- **OSE** *(Opérateur de Service Essentiel)* : en France, opérateur tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

- **PaaS** *(Platform as a Service* : voir « Présentation des types d'offres ».
- **PAS** *(Plan d'Assurance Sécurité)* : document contractuel décrivant l'ensemble des dispositions que les prestataires s'engagent à mettre en œuvre pour garantir les exigences de sécurité du client.
- **RACI** *(Responsible, Accountable, Consulted, Informed)* : matrice de responsabilité indiquant les rôles et responsabilités des intervenants dans le projet cloud.
- **RBAC** *(Role Based Access Control)* : modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est associé.
- **RGPD** (règlement général sur la protection des données) : règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il régule notamment le fait que des données personnelles soient stockées à l'étranger.
- **RGS** (référentiel général de sécurité) : cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens, il s'impose spécifiquement aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et dans leurs relations avec les usagers.
- **ROI** *(Return On Investment)* : retour sur investissement en français, indicateur qui indique si une opération a été une réussite ou non en termes de revenu financier.
- **SAML** *(Security Assertion Markup Language)* : standard ouvert qui permet aux fournisseurs d'identité (IdP) de transmettre des données d'identification aux fournisseurs de service.
- **SaaS** *(Software as a Service)* : voir « Présentation des types d'offres ».
- **SD-WAN** (Software-defined wide area network) : le SD-WAN permet une connectivité résiliente et à faible latence sur tout type de réseau.
- **SecNumCloud** : Référentiel ANSSI associé à une qualification pour les prestataires de services en nuage (cloud)
- **SI** *(Système d'Information)* : ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs.
- **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.
- **SOC** *(Security Operation Center)* **:** service en charge d'analyser les traces en lien avec la sécurité et de réaliser les premières étapes de correction.
- **SOC 1, 2 et 3** *(Service Organization Controls)* : cadre de référence pour rendre compte et contrôler les mesures de sécurité en place. On peut classer les SOC par niveau et par type (exemple SOC 2 type 2), ces deux éléments indiquent l'exhaustivité des critères retenus et s'il s'agit d'une auto-évaluation ou d'une évaluation par un organisme tiers.
- **SSO** *(Single Sign On)* : permet de s'authentifier une seule fois et d'accéder à plusieurs applications.
- **SWG** (Secure Web Gateway) : la Passerelle web sécurisée est une solution de cybersécurité généralement mise en œuvre sous la forme d'un service cloud entre les utilisateurs et le Web.
- **VM** *(Virtual Machine)* : machine virtuelle.
- **VPN** *(Virtual Private Network)* : système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.
- **ZTNA** (Zero Trust Network Access) : le Zero Trust est un modèle stratégique de cybersécurité qui part du principe qu'il n'existe aucune zone de confiance lorsqu'il s'agit de protéger le système d'information et les données de l'entreprise.

2 Questionnaire pour les projets cloud

Dans un souci de bonne gouvernance et afin de sécuriser les projets de déploiement de nouvelles solutions dès leur phase de lancement, il est important de s'interroger sur ses besoins, sur la capacité des fournisseurs à les adresser et sur la réponse à apporter aux enjeux de sécurité.

Il est entendu que la volonté de l'organisme et de ses dirigeants quant à l'utilisation de ressources dans le cloud a été validée en amont, volonté idéalement associée à la réalisation préalable d'une appréciation des risques.

Ce questionnaire est l'opportunité de créer plus de liens entre les équipes métiers (marketing, relation client…) et les équipes sécurité et de partager les informations nécessaires et suffisantes pour que les équipes sécurité soit en soutien du projet.

La proposition suivante de questionnaire vise à aider votre organisation à évaluer les besoins d'une architecture cloud, en suivant une approche orientée risque. Par exemple, une entreprise pourrait imposer aux chefs de projet métiers de remplir ce questionnaire et le renvoyer à destination de la DSI ou des équipes sécurité afin que ces derniers puissent donner leur avis sur le projet et s'assurer du bon niveau de sécurité tout au long de la vie du projet.

Ce questionnaire se compose des parties suivantes :

1. Résumé du projet
2. Fiche d'identité du projet
3. Acteurs du projet
4. Historique du SI
5. Hébergement
6. Contrat
7. Sécurité des données et des accès

À noter : l'évaluation des besoins de sécurité (DICT/P) a été intégrée dans un chapitre distinct qui peut potentiellement être joint au questionnaire.

Chaque organisme n'ayant pas le même degré d'exigences en matière de protection de l'information, nous avons tenté de classer chaque ligne du questionnaire selon le niveau d'audience et les exigences en matière de sécurité :

● Niveau 1	Recommandé pour les organismes avec des ressources et une expertise en cybersécurité limitées, combinées à un environnement où la sensibilité des données traitées est relativement faible (ex. : TPE, startup ou PME ne traitant pas des données sensibles ou une quantité modérée de données personnelles)
● Niveau 2	Recommandé pour les organismes avec un niveau de ressources et une expertise en cybersécurité modérés ou élevés (ex. : startup, PME, ETI, grand compte traitant des données sensibles et/ou une quantité importante de données personnelles)

1. Résumé du projet

Audience	Question	Réponse
🟢🔵	**Description du projet** *(ex. : Création d'une application mobile)*	
🟢🔵	**Finalité du projet** *(ex. : Proposer un nouveau canal d'accès à nos clients)*	
🟢🔵	**Solution technique envisagée** *(Si applicable)*	

2. Fiche d'identité du projet

Audience	Question	Réponse
🟢🔵	**Maîtrise d'ouvrage** *(Qui est le donneur d'ordres/sponsor ?)*	
🟢🔵	**Quelle est la couverture du projet ?** *(International, national ou local)*	
🟢🔵	**Contraintes projet** *(Préciser les exigences d'utilisation, les contraintes particulières d'exploitation (ex. plages horaires pour exécution de traitements, etc.)*	
🔵	**Type de solution technique envisagé** *(Transactionnel avec interface Web, décisionnel, publication, SI en interaction (préciser lesquels), autres ?)*	

3. Acteurs du projet

Audience	Question	Réponse
🟢🔵	**Chef de projet interne** *(préciser le nom)*	
🟢🔵	**Qui seront les usagers du service ?** *(interne DSI ou équipe sécurité, métiers, partenaires externes, clients)*	
🔵	**Y a-t-il des correspondants pour chacun des groupes d'usager ?**	

🟢🔵	**Y a-t-il une maîtrise d'œuvre externalisée ?**	
🟢🔵	**L'hébergement et la maîtrise d'œuvre sont-ils gérés par le même prestataire ?**	
🟢🔵	**Si non, préciser les missions des prestataires**	

4. Historique du périmètre projet

Audience	Question	Réponse
🟢🔵	**S'agit-il d'une application existante ?** *(Si oui, préciser s'il s'agit d'une évolution majeure et si une évaluation des besoins de sécurité a déjà été conduite)*	
🔵	**Une prestation sécurité des systèmes d'information spécialisée a-t-elle déjà été conduite ?** *(Analyse de risques, audit, audit de code, tests d'intrusion…)* Si oui, préciser les dates de réalisation et les références.	
🟢🔵	**Hébergeur précédent**	

5. Hébergement

Audience	Question	Réponse
🔵	**Quel est le modèle de déploiement cloud envisagé ?** *(Cloud privé déployé en interne, cloud public, cloud privé déployé en externe ou cloud hybride)*	
🔵	**Quel est le type d'offre cloud envisagé ? (IaaS, PaaS, SaaS, etc.)**	
🟢🔵	**Nom de l'hébergeur pressenti** *(si applicable)*	
🔵	**Est-ce que le prestataire fait partie du Registre « CSA Star » ?** *(https://cloudsecurityalliance.org/star/registry)*	
🟢🔵	**Le prestataire propose-t-il d'héberger les données en France ?**	

🟢🔵	**Si les données ne sont pas hébergées en France, le seront-elles au sein de l'Union européenne ?**	
🟢🔵	**Si les équipes du prestataire sont amenées à traiter les données (administration, surveillance des traces, etc), ces dernières seront-elles situées au sein de l'Union européenne ?**	
🟢🔵	**L'hébergeur possède-t-il une ou plusieurs certifications internationales ?** *ISO 27001, SOC 1 (SSAE18, ISAE 3402), SOC 2 (ISAE 3000, AT Section 101), SOC 3…*	
🔵	**Les datacenters offrent-ils des garanties de sécurité suffisantes ?** *TIER III, IV…*	
🟢🔵	**Faut-il mettre en place une interconnexion réseau spécifique ? Si oui, quelles sont les solutions proposées ? Les capacités actuelles (côté client) sont-elles adaptées ?**	
🔵	**Quelles solutions de chiffrement sont prévues par le prestataire pour le transit et le stockage des données ?**	
🔵	**Dans le cas d'un cloud public, quelles solutions sont prévues pour garantir l'isolement des données entre les clients ?**	
🟢🔵	**Est-ce que l'offre d'hébergement inclut un service de télémaintenance ou infogérance ?**	
🟢🔵	**Quel sont le processus d'archivage et le temps de rétention ?**	
🔵	**La télémaintenance/infogérance est-elle opérée par un prestataire tiers ?**	
🔵	**Le prestataire a-t-il recours à un SOC (Security Operations Center) ?**	

6. Contrat

Audience	Question	Réponse
🔵	**Existe-t-il un contrat ou une proposition de contrat à l'échelle du Groupe ou de l'une des sociétés du Groupe ?**	

🟢🔵	**S'agit-il d'un avenant à un contrat en cours ?**	
🔵	**Quelles clauses juridiques, conditions générales d'utilisation ou quel contrat sont étudiés avec le service juridique ?**	
🔵	**Est-ce que les rôles et responsabilités de chacune des parties sont clairement définis dans le contrat ou dans une matrice RACI référencée dans ce dernier ?**	
🟢🔵	**Est-ce que le contrat est soumis au droit européen ou à une autre réglementation ?**	
🟢🔵	**Quelle est la durée du contrat et de la reconduction tacite ?**	
🟢🔵	**Quelles sont les possibilités de résiliation en cours de contrat ?**	
🟢🔵	**Les services proposés sont-ils couverts par l'assurance professionnelle de l'hébergeur en cas de défaillance ?**	
🟢🔵	**Les conditions d'évolution de la solution cloud sont-elles clairement définies ?** **(Évolutions tarifaires, évolutions techniques des interfaces externes, compatibilité ascendante, etc.)**	
🔵	**Quelles sont les possibilités d'audit ?** *(Fournisseur, hébergeur, infrastructures…)*	
🟢🔵	**Quelles sont les garanties de niveau de service ?** *(SLA, etc.)*	
🔵	**Existe-t-il des pénalités si le service attendu n'est pas délivré ?**	
🟢🔵	**Quels sont les engagements de communication sur les incidents de sécurité ?** *(Fuite de données, intrusion, sabotage, etc.)*	
🔵	**Existe-t-il des engagements sur la fourniture des journaux d'événements/sécurité dans le cadre de démarches forensic ?**	
🟢🔵	**Quels sont les moyens mis en œuvre dans le cadre de la protection des données personnelles ?** *(Politique, durée de rétention, effacement, chiffrement, etc.)*	

🟢🔵	**Existe-t-il une procédure de réversibilité ?** *(Récupération des données et des fonctions métiers dans un format exploitable)*	
🔵	**Existe-t-il une procédure d'effacement ?** *(Destruction des données actives et des sauvegardes en cas d'abandon de la solution) ?*	

7. Sécurité des données et des accès

Audience	Question	Réponse
🟢🔵	**Les données hébergées sont-elles soumises au RGPD ?**	
🟢🔵	**Le prestataire présente-t-il une gouvernance de conformité au RGPD ?**	
🟢🔵	**Est-ce que les données fournies seront utilisées par le prestataire dans le cadre de traitement massif de données ?**	
🟢🔵	**Y a-t-il des procédures de sauvegarde et de restauration des données ?**	
🔵	**Le prestataire est-il en mesure de supprimer de manière définitive des données sur demande ?** *(Y compris les données effacées)*	
🔵	**À la fin du contrat, comment le prestataire sera-t-il en mesure d'effacer les données de manière définitive ?**	
🟢🔵	**Est-ce que le service cloud utilisé implique le transfert de données vers un pays hors UE ?** *(Pour des raisons de support notamment)*	
🟢🔵	**L'accès au service demande-t-il des prérequis techniques ?** *(Navigation, accès Internet)* **Si oui est-ce compatible avec nos postes de travail et notre infrastructure ?**	
🔵	**Est-ce que des solutions de chiffrement des échanges sensibles sont proposées ?**	
🔵	**Y a-t-il un filtrage des accès par IP source ?** *(Accès uniquement depuis le réseau de notre société)*	

🔵	**Le niveau de confidentialité est-il adapté à la sensibilité des données ?** *(Chiffrement, authentification forte, etc.)*	
🔵	**Est-il possible de mettre en place un interfaçage (API) avec des solutions de sécurité ?** *(Supervision, Gestion des identités)*	
🟢🔵	**SaaS – Est-ce que l'application s'appuie sur un CMS *(Content Management System)* ?** *(Wordpress, Joomla, Drupal, Magento, Prestashop, etc.)*	
🟢🔵	**SaaS – L'application utilise-t-elle des bibliothèques ou composants tiers ?** *(jQuery, Angular/React.js, Symfony, Spring, etc.)*	
🔵	**SaaS – L'application est-elle accessible sous forme d'interface de programmation (API) externe ? Si oui, quelles sont les mesures de sécurité proposées ?**	

3 Évaluation des besoins de sécurité

Bien que non spécifique au cloud, l'évaluation des besoins de sécurité est d'autant plus critique dans ce contexte car les données sont plus exposées, alliée au partage des responsabilités notamment en matière de sécurité cela rend la maîtrise de ces données plus complexe.

La sensibilité d'un SI est établie après avoir déterminé les missions et les objectifs auxquels le système contribue, et après avoir évalué l'importance de cette contribution ainsi que les conséquences de la non-atteinte des objectifs qui pourraient lui être imputables.

Plus concrètement, les besoins de sécurité d'un SI doivent idéalement être estimés selon quatre critères de sécurité : disponibilité, intégrité, confidentialité et traçabilité/preuve (DICT/P).

- **Disponibilité** : propriété d'accessibilité au moment voulu des biens essentiels par des personnes autorisées
  - La disponibilité est donc l'ensemble des mécanismes rendant les systèmes ou les données accessibles tel qu'attendu (résilience) : redondance matérielle et logicielle, Plan de reprise d'activité…
  - Ce critère protège contre la dégradation ou l'arrêt d'un service souscrit.
- **Intégrité** : propriété de protection de l'exactitude et de la complétude d'un actif
  - L'intégrité adresse l'écriture ou la modification de la donnée.
  - Le prestataire doit mettre en œuvre des moyens de protection adéquats contre l'altération des données ; avoir la capacité de restaurer en cas de problème, et garantir des données exactes et complètes.
  - Il y a deux types d'intégrité : l'intégrité de la donnée et l'intégrité du système.
    - L'intégrité de la donnée protège des modifications non autorisées : CRC, *Message Digest,* signature numérique…
    - L'intégrité système protège les systèmes d'exploitation : antimalware, par exemple.
- **Confidentialité** : propriété d'un élément essentiel connu et accessible uniquement pour des personnes explicitement autorisées
  - La confidentialité est le fait d'éviter une lecture non autorisée de données (l'information n'est pas divulguée à des personnes, des entités ou des processus non autorisés).
  - Le prestataire assure que les données demeurent protégées contre la divulgation non autorisée.
  - On peut appliquer la confidentialité dans les trois états de la donnée :
    - au repos : les données stockées sur disque (chiffrement AES, par exemple) ;
    - en transit : les données sont envoyées sur le réseau (chiffrement avec TLS par exemple, ;
    - en traitement : les données sont affichées, imprimées ou en cours d'utilisation par le CPU.
- **Traçabilité** (ou preuve) : propriété désignant la conservation des traces de l'état et des mouvements de l'information (qui fait quoi et quand) dans le but d'avoir la capacité de prouver l'occurrence d'un événement ou d'une action donnée ainsi que les entités qui en

sont à l'origine (mise à disposition des traces et des enregistrements en cas de litige). Sans cela, il est impossible d'avoir l'assurance que les trois autres critères sont respectés.

Plus concrètement, les besoins de sécurité d'un SI doivent idéalement être estimés à l'aide d'une échelle multiniveaux (par exemple de 1 à 4) en précisant les raisons. Les besoins sont exprimés par rapport aux fonctions assurées, indépendamment des mesures de sécurité éventuellement déjà mises en place (procédure dégradée manuelle, architecture technique redondée, etc.).

Le formulaire d'évaluation suivant doit être rempli par grand domaine fonctionnel ou par processus métier :

Disponibilité (Impact sur l'activité de la structure)	Définition	La disponibilité est l'aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévues.
	Score 1	N'est pas considéré comme gênant si l'indisponibilité dépasse 48 h.
	Score 2	Perturbe l'activité si l'indisponibilité est comprise entre 4 h et 48 h.
	Score 3	Nuit à l'activité si l'indisponibilité est comprise entre 2 h et 4 h.
	Score 4	Nuit gravement à l'activité si l'indisponibilité est supérieure à 2 h.
Intégrité (Altération par modification d'un traitement ou d'une donnée non autorisée)	Définition	L'intégrité est la propriété assurant qu'une information ou un traitement n'ont pas été modifiés ou détruits de façon non autorisée.
	Score 1	Données altérables, ne gêne pas l'activité.
	Score 2	Perturbe l'activité : détection automatique des altérations.
	Score 3	Nuit à l'activité : altérations détectées et soumises à correction.
	Score 4	Nuit gravement à l'activité : aucune altération n'est acceptée.
Confidentialité (Accès limité aux seules personnes ayant le droit d'en connaître)	Définition	La confidentialité est la propriété permettant de s'assurer que seuls les utilisateurs ayant à en connaître et habilités dans les conditions normales prévues ont accès aux informations.
	Score 1	Ne gêne pas l'activité, les données sont publiques.
	Score 2	Perturbe l'activité, les données sont internes, réservées à l'organisation.

	Score 3	Nuit à l'activité, les données sont sensibles, la connaissance doit être limitée.
	Score 4	Nuit gravement à l'activité, données classifiées ou données connues d'un nombre très restreint de personnes.
Traçabilité (Garantie de la conservation des opérations fonctionnelles et/ou techniques)	Définition	La traçabilité est la propriété qui garantit la conservation des enchaînements d'opérations fonctionnelles et/ou techniques (par exemple, la création d'un document, les responsables d'une prise de décision, etc.).
	Score 1	N'est pas nécessaire : l'identification des acteurs n'est pas requise.
	Score 2	Doit être effective sur les fonctions majeures du SI.
	Score 3	Doit être assurée : imputabilité des actions.
	Score 4	Impérative : aucune contestation possible (preuve opposable en justice).

Si le DICT/P est décliné sur plusieurs domaines fonctionnels, indiquez ci-dessous les niveaux maximums retenus :

Tableau récapitulatif DICT/P	**Niveau retenu**
Disponibilité	
Intégrité	
Confidentialité	
Traçabilité/Preuve	

4 Introduction à l'identification des actifs et leur évaluation

4.1 Préambule

L'identification et l'évaluation des actifs sont l'une des premières étapes à effectuer dans le cadre d'une analyse de la gestion de risques. Chaque méthode possède une approche qui lui est propre ; par exemple, la norme ISO 27005 propose dans son annexe B de distinguer les actifs en deux catégories : les actifs primordiaux (processus et activités métiers, informations) et les actifs en support (matériel, logiciel, réseau, personnel, site, etc.).

4.2 Identification des actifs

Dans le cadre d'un projet cloud, ce sont *a priori* les données à traiter qui seront les actifs primordiaux au centre des préoccupations et sous la responsabilité directe du client tandis que les actifs support seront très certainement en grande partie sous la responsabilité du prestataire retenu (selon le type d'offre cloud choisi).

Voici quelques exemples d'actifs qui semblent être pertinents à utiliser dans le cadre d'un projet cloud (liste non exhaustive à adapter au contexte) :

Catégories	**Exemples d'actifs**
Actifs immatériels	• Réputation de la société • Confiance des clients • Loyauté des employés (capacité à se protéger de la malveillance interne) • Propriété intellectuelle
Informations	• Données personnelles sensibles • Données personnelles • Données de santé • Données techniques/Savoir-faire
Applications	• Application XYZ • Utilisateurs de l'application XYZ • Contrôle d'accès à l'application XYZ • Interface de gestion de l'application XYZ • Interface de gestion API de l'application XYZ • Code source de l'application XYZ • Journaux d'événements opérationnels de l'application XYZ • Journaux d'événements de sécurité de l'application XYZ
Personnel (de l'entreprise)	• Personnel/Décideurs • Personnel/Utilisateurs • Personnel d'exploitation et de maintenance • Personnel/Développeurs

Actifs matériels	• Sauvegarde • Réseau • Matériel • Bâtiment

Il convient ensuite de désigner pour chaque actif un propriétaire qui en est responsable. Sans pour autant forcément jouir du droit de propriété de l'actif concerné, le propriétaire est responsable de sa production, de son développement, de sa maintenance, de son utilisation et de sa protection (selon le cas).

4.3 Évaluation des actifs

Afin d'évaluer les différents actifs, il convient préalablement d'avoir choisi une échelle de mesure et les critères associés. Chaque méthode de gestion des risques propose des approches qui se veulent très différentes, il appartiendra alors à la personne responsable de la gestion des risques de choisir la plus adaptée au contexte.

L'échelle d'évaluation peut aussi bien être basée sur un seul critère comme la valeur perçue de l'actif sur trois (haute, moyenne, basse) ou quatre niveaux (très haute, haute, basse, très basse), ou encore faire appel à des formules plus complexes multicritères fondées sur la valorisation des besoins en sécurité (disponibilité, intégrité et confidentialité), noté chacun sur une échelle de 1 à 4 par exemple.

Pour aller plus loin :

- ISO/IEC 27005:2018 : Chapitres Identification des actifs, Valorisation des actifs et Annexe B (Identification et évaluation des actifs et appréciation des impacts).
- ENISA – Cloud Computing Security Risk Assessment : Chapitre 5, Assets

5 Checklist des clauses contractuelles

5.1 Recommandations de la CNIL

Le contenu de ce chapitre est un résumé de l'annexe du document « Recommandations pour les entreprises qui envisagent de souscrire à des services de cloud computing », publié par la CNIL en juin 2012 qui reste néanmoins une très bonne synthèse adaptée au contexte des clauses contractuelles pouvant être judicieusement complétées par les définitions du RGPD.

1. Informations relatives aux traitements
    a. Respect des principes européens en matière de protection des données personnelles
    b. Existence d'un système de remontée des plaintes et des failles de sécurité
    c. Moyens de traitement
    (Description des moyens mis en œuvre pour le traitement)
    d. Sous-traitance
    (Officialisation de l'existence de sous-traitants et rôles de ces derniers)
    e. Existence de procédures simples permettant de respecter les droits des personnes concernées vis-à-vis de leurs données

2. Garanties mises en œuvre par le prestataire
    a. Durée de conservation des données limitée et raisonnable au regard des finalités pour lesquelles les données ont été collectées
    b. Destruction et/ou restitution des données
    c. Devoir de coopération avec les autorités de protection des données compétentes
    d. Audits
    (Droit d'audit direct ou par un tiers de confiance)

3. Localisation et transferts
    a. Destinataires
    (Engagement du prestataire sur la communication d'informations relatives aux destinataires des données)
    b. Indication claire et exhaustive des pays hébergeant les serveurs du prestataire
    c. Assurance d'une protection adéquate à l'étranger (notamment grâce à des clauses contractuelles types ou à des règles contraignantes d'entreprise « BCR »)
    d. Possibilité de limiter les transferts de données uniquement vers des pays tiers assurant un niveau de protection adéquat
    e. Information du client en cas de requête provenant d'une autorité administrative ou judiciaire étrangère
    (Exemple : validité du « EU-US Privacy Shield » mis en place en 2016 et invalidé en 2020)

4. Sécurité et confidentialité
    a. 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

b. Politique de sécurité et mesures de sécurité
(Échange mutuel de documents relatifs aux mesures mises en place pour assurer la sécurité des données)
c. Certification
(Formalisation de la possession d'une ou plusieurs certifications, description du périmètre associé et engagement formel de respect)
d. Réversibilité/portabilité des données
(Formalisation du processus de réversibilité)
e. Traçabilité
(Formalisation de la mise à disposition par le prestataire des traces au client)
f. Continuité de service, sauvegardes et intégrité
(Formalisation des mesures mises en place pour assurer la continuité de service ainsi que la sauvegarde et l'intégrité des données avec engagement de résultat)
g. Engagements de niveau de service
h. Cycle de vie de la donnée
(Garantie d'effacement des données de l'ensemble des supports)

À noter : Le point relatif aux obligations de déclaration auprès de la CNIL (rendu en partie obsolète par le RGPD) n'a pas été repris.

5.2 Pour aller plus loin

Les organismes ayant de fortes contraintes en matière de protection de l'information sont invités à compléter cette liste par les exigences définies au sein du document *Prestataires de service d'informatique en nuage (SecNumCloud),* dont la version 3.1 a été publiée par l'ANSSI en juin 2018. L'ensemble des exigences sont détaillées du chapitre 5 au chapitre 19.

Bien que les exigences décrites dans le document ne soient pas toutes forcément nécessaires dans un contexte n'exigeant pas la conformité à ce référentiel, elles permettent de balayer de manière quasi exhaustive les points de vigilance qui peuvent être spécifiés contractuellement.

6 Matrice RACI d'un SOC

	Services SOC		Responsable SOC	Analyste SOC niveau 1	Analyste SOC niveau 2	Analyste SOC niveau 3	RSSI	Point de contact	Equipes opérationnels
	ROLES		Services de détection				Equipes sécurité Soumissionaire		Soumissionaire
	Collecte de journaux								
	Administrer et exploiter le SIEM interne de Soumissionaire						I	R	
	Récupérer, centraliser et stocker les journaux au sein de l'outil de gestion des logs, en respectant les règles de sécurité définies par Soumissionaire		I	R			C		
	Administrer et exploiter le SIEM du soumissionnaire		I	R			C		
	Définir les journaux et évènements de sécurité devant être collectés et stockés au sein du SIEM et par les outils de détection		I	R			C	C	
	Définir la criticité des actifs surveillés		C				R	C	R
	Détection des incidents de sécurité								
	Corréler les évènements de sécurité SI remontés au sein de Soumissionaire		I		R				
	Définir les impacts, conséquences et criticité des incidents redoutés		I	C			R	R	
	Premier filtrage sur les alertes de sécurité remontées			R					
	Exploitation des tickets d'alertes			R					
	Vérifier et exclure les faux positifs				R				
	Fournir des propositions visant à optimiser le service de détection des incidents de sécurité		C	R			C	C	
	Analyser et qualifier les alertes de sécurité contextualisées avec le SI de Soumissionaire			R					
	Définir le format des règles de détection				R	R	I	I	
	Réponse aux incidents								
	Accompagner les équipes sécurité de Soumissionaire lors de la gestion de l'incident de sécurité		A	R			C	C	I
	Clôturer l'incident et rédiger un rapport retraçant les étapes de l'incident		C				I		R
	Définir et approuver un plan de remédiation		C				R/A	R	C
	Reporting et tableaux de bord								
	Définir les indicateurs de suivi du service de détection		C				A	R	I
	Construire et maintenir à jour les indicateurs de suivi du service de détection		A	R			I	C	
	Fournir des rapports mensuels établissant le nombre d'alertes remontées par seuil de criticité, de faux positifs		C	R			I	I	

Acronyme		
R	Responsable	Responsable de l'action
A	Accountable	Approuve l'action et responsable de l'avancement
C	Consulté	Un consultant, un intervenant ou un expert en la matière qui est consulté avant une décision ou une action.
I	Informé	Doit être informé après une décision ou une action.

7 Exemples d'implémentation d'un projet cloud

7.1 Préambule

Ce chapitre a pour vocation d'illustrer des cas d'usage d'applications cloud au travers d'un guide pas à pas d'implémentation technique, ils n'ont pas pour objet de faire la promotion de services spécifiques à un éditeur et/ou un fournisseur.

De manière générale, les sujets techniques à anticiper lors de la mise en service d'un service IT sur le cloud peuvent être regroupés en cinq catégories :

- Architecture :
  - Capitalisation d'un service existant (ex. : si le service SaaS Office 365 est déjà en fonction, l'identité Azure AD peut être capitalisée en IaaS ou PaaS sur Azure)
  - Organisation des ressources
  - Évolutivité des besoins (afin de faire des choix d'architecture pérennes)
- Identité :
  - Gestion des identités et des permissions des utilisateurs
  - Gestion des identités et des permissions des administrateurs
- Réseau :
  - Mise en fonction de l'interconnexion avec le SI
  - Publication des services
- Sécurité :
  - Réduction maximale de la surface d'attaque
- Exploitation :
  - Maintien en condition opérationnelle
  - Surveillance et monitoring

7.2 Cas concret : Implémentation d'une infrastructure IaaS/PaaS sur Azure

L'objectif de cette implémentation est la mise en place d'un socle d'infrastructure dans le cloud afin d'y héberger des services.

1. Architecture et cadrage :

   Comme pour tout projet informatique, la première étape consiste en la définition de l'architecture cible souhaitée afin de répondre au mieux aux différentes contraintes :

- Couverture des besoins métiers :
  - Détermination des exigences utilisateurs,
  - Définition du cahier des charges à respecter ;
- Sécurité globale de la solution :

    - Choix de l'outil de sécurisation réseau,
    - Définition des permissions d'administration ;
- Projection de coût :
    - Choix des niveaux de service souhaités,
    - Utilisation de la calculatrice proposée par l'éditeur ;
- Intégration au SI existant :
    - Définition des sous-réseaux utilisés,
    - Choix de la solution VPN ;
- Communication :
    - Information des différents acteurs du projet.

2. Mise en place de l'abonnement

Afin de pouvoir créer des ressources, une souscription Azure est créée directement auprès de l'éditeur[10], c'est au sein de celle-ci que l'ensemble des ressources seront créées.

3. Gestion des identités et des accès

Les premières ressources pouvant être créées, il est temps de positionner les permissions d'accès et de configurer l'authentification Azure AD (activation du MFA…).

Les groupes d'accès suivants sont créés :

Rôle	Permissions
Admin. général	Accès à toutes les ressources
Admin. réseau	Gestion de l'ensemble des briques réseau Azure
Exploitation	Gestion des VMs, Supervision, Sauvegardes…
Resp. Application	Accès aux ressources dédiées à une application
Admin. Utilisateur	Gestion des comptes sur Azure AD (MFA, réinitialisation mot de passe…)

Le MFA a également été activé sur l'ensemble des comptes administrateurs ayant accès aux ressources Azure.

Après ces premières étapes, le projet est prêt à démarrer et l'ensemble des acteurs au sein du SI sont informés. Les premières actions techniques peuvent commencer et les intervenants peuvent accéder à la plateforme.

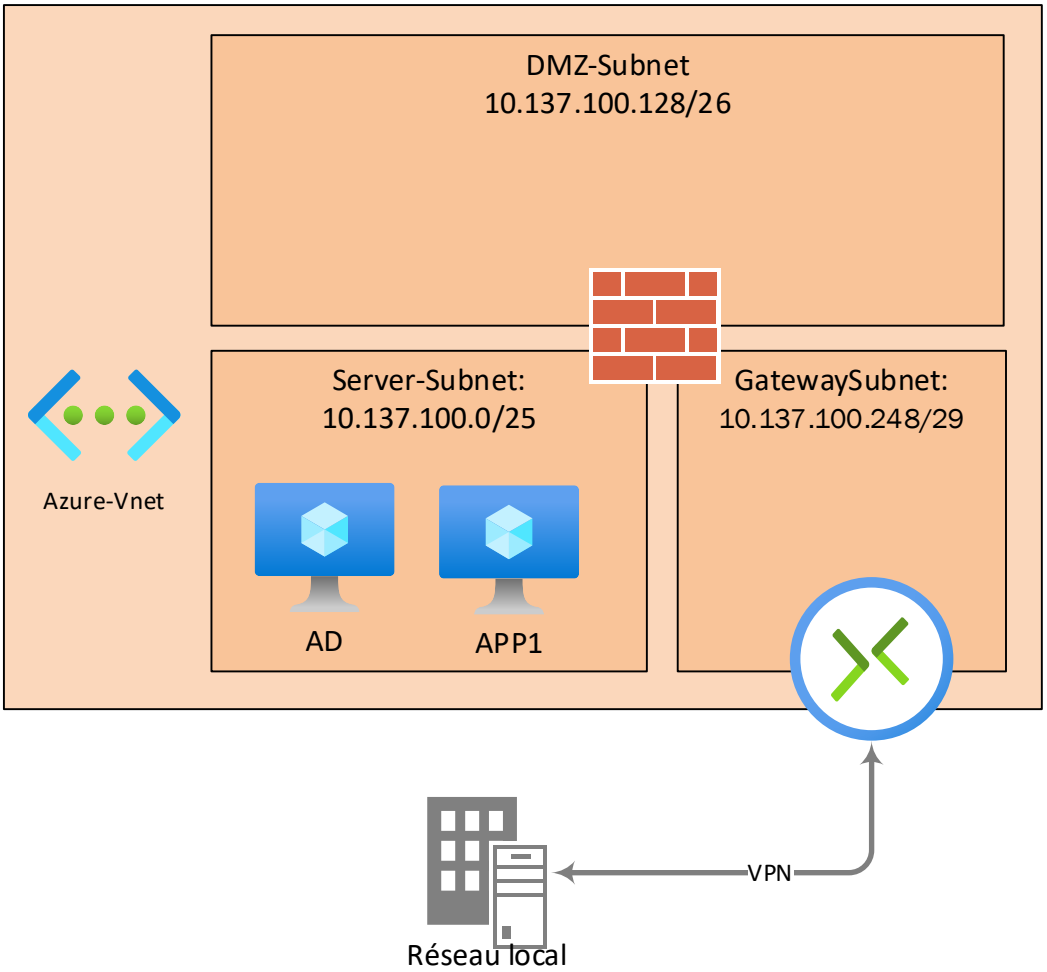
4. Implémentation de l'interconnexion réseau

L'infrastructure réseau définie lors de la phase d'architecture est implémentée avec les équipes réseau :

- Création du réseau virtuel (VNet) ;
- Configuration du VPN permettant les échanges avec le SI ;
- Mise en place du firewall cloud et implémentation des règles de sécurité ;
- Génération d'une DMZ.

Le schéma ci-après résume la configuration implémentée.

[10] Il existe différents types de souscription impliquant des méthodes de facturation et d'implémentation différentes.



Cas concret : Architecture réseau Azure

5. Déploiement des services

Une fois le réseau implémenté, il est possible de déposer les premières ressources de production.

Les deux premières VM sont créées : un serveur AD et un serveur applicatif sont déployés au sein du réseau LAN Azure comme présenté dans le schéma ci-dessus.

6. Mise en place du *monitoring*

Avant de basculer l'environnement Azure en production, les deux VMs implémentées sont ajoutées à la solution de supervision utilisée pour les VMs situées au sein de l'infrastructure locale. L'implémentation d'une infrastructure de supervision sur Azure sera à envisager dans un second temps.

7. Mise en place du suivi des consommations (FinOps)

L'infrastructure étant amenée à évoluer et héberger progressivement de nouvelles applications, une personne est définie comme responsable de la supervision des coûts de l'environnement. Cette personne a implémenté une alerte sur la supervision des coûts afin d'éviter l'augmentation irrationnelle de la facture.

Le socle de cloud public Azure est désormais implémenté, l'environnement peut désormais être utilisé pour l'implémentation de nouveaux services tout en respectant le modèle déterminé.

7.3 Cas concret : Authentification unique sur Docusign *via* Okta

L'objectif de cette implémentation est de permettre aux utilisateurs une connexion automatique au service de signature électronique DocuSign *via* la solution d'identité Okta.

Cette implémentation est réalisée en deux étapes :

1. **Provisionnement des comptes sur Docusign**

La première étape pour l'implémentation du SSO consiste à synchroniser les utilisateurs depuis l'annuaire d'entreprise vers la base Docusign. Cette synchronisation a plusieurs objectifs :

- L'application dispose d'un compte par collaborateur ayant besoin d'y accéder ;
- Dans le cas du départ d'un salarié, le compte n'est pas conservé ce qui évite la surconsommation de licences ;
- Tout collaborateur ayant quitté la société ne pourra plus se connecter à ses applications de manière automatique.
- Les options suivantes sont définies pour la synchronisation :
- Création et suppression automatique des comptes dans DocuSign en fonction de l'appartenance à un groupe dans l'annuaire d'entreprise : « Utilisateurs DocuSign » ;
- Définition de la liste des attributs à synchroniser dans l'application et correspondance des champs d'annuaire avec les champs de l'application :
  - nom,
  - prénom,
  - adresse email,
  - Téléphone,
  - …

2. **Implémentation du SSO**

Une fois les comptes connus et provisionnés au sein de l'application, il est possible de passer à la configuration de l'authentification unique. Celle-ci se base ici sur le protocole SAML.

- Dans le portail d'administration Docusign :
  - Création d'un nouveau fournisseur d'identité SAML « Okta »,
  - Saisie des différentes informations SAML (issuer, login URL, méthodes…),
  - Correspondance des claims (attributs) avec les comptes synchronisés :
    - Indication des claims à récupérer dans le jeton utilisateur (NameID…),
    - Correspondance avec les champs de l'application (identifiant…),
  - Import du certificat,
  - Copie des informations de l'application ;
- Dans le portail Okta, configuration de l'application Docusign :
  - Saisie des informations récupérées (URLs et identifiants de fédération),
  - Choix des attributs à fournir dans le jeton utilisateur *(claims)* :
    - Choix des attributs utilisateurs dans l'annuaire (mail, identifiant…),
    - Définition de "Claims" qui hébergeront ces informations (NameID…) ;
- Test et recette.

Sources : https://saml-doc.okta.com/Provisioning_Docs/Docusign_Provisioning.html

https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-in-DocuSign.html

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr