<table>
<tr><td colspan="2">Domaine : Systèmes d'Information et télécommunication
Entité émettrice : CCOS-DSIT-EM
Nature du document : Note de Politique (NP)</td><td>Id. Rte :
RTE_2025_0133346_0
Id. métier :</td></tr>
<tr><td>Version
0.1
Statut
Brouillon
Accessibilité
Interne RTE</td><td colspan="2">Doctrine Cloud RTE</td><td>Date d’approbation

<u>Prescriptif</u>
Date d’applicabilité :
Date de fin de validité :
[Date de fin de validité]
Revue d’exigence :
[simplifiée ou détaillée]</td></tr>
<tr><td colspan="2">Destinataire(s) pour Action
DSIT/DPOSE, DSIT/DPCM, DSIT/DPOI, DSIT/DPCO, DSIT/DESIGN, DSIT/DDL, Direction Achats

Destinataires pour Information
PISSIN</td><td>Rédacteur(s)
BENJAMIN BAA-PUYOULET, FABIEN CAPODICASA

Vérificateur(s)
ROMUALD BOURGOIN, PIERRE BRUNEL, LAURENT POTIER, JEAN-PHILIPPE GRAS, DAPHNE ZANATTA, PASCAL SEGURA, LAURENT PERINET, THIBAULT FERTEY

Approbateur(s)
VALERIE VAGAGGINI, SEBASTIEN HENRY</td></tr>
<tr><td colspan="3">Document(s) de référence
Schéma directeur Cloud pour le SI de RTE - Etat des lieux et décisions
Plan stratégique SI v2 - Feuille de route technologique PSSI - Feuille de route technologique vf.docx - Nuxeo Platform
Benchmark sur la gestion du chiffrement et les usages Cloud – RTE Synthèse exécutive</td></tr>
</table>

Dans le cadre de la modernisation du SI et de la recherche d’une plus grande efficacité pour répondre aux différents enjeux stratégiques des métiers, RTE a décidé, dans le cadre du plan stratégique SI v2, d’hybrider ses plateformes avec un usage plus régulier des clouds commerciaux.

Ce document vient définir le périmètre des cas d’usage devant être hébergés par défaut sur le cloud (« Cloud First ») et préciser les conditions d’application.

Rte - Réseau de Transport d’Électricité
Immeuble WINDOW
7C, place du Dôme
92073 PARIS LA DEFENSE CEDEX

1 Contexte

Les opportunités relatives au cloud dans le cadre d'une hybridation des plateformes RTE ont été décrites dans la feuille de route technologique du Plan Stratégique SI v2. Elle identifie le cloud comme l'un des chantiers prioritaires de la modernisation du SI. Elle encourage la DSIT à s'emparer du cloud et à s'appuyer sur son potentiel pour répondre aux besoins stratégiques des métiers et aux projets d'innovation portés par la R&D tout en garantissant un niveau de cybersécurité homogène et conforme aux règles et bonnes pratiques en vigueur à RTE.

Les enjeux sous-jacents à l'hybridation de nos plateformes sont les suivants :

- Enjeu de modernisation pour RTE, en ce que le cloud en est un facilitateur. L'adoption du cloud doit s'accompagner de celle des pratiques à l'état de l'art dans la production de services numériques (scalabilité/élasticité, robustesse, automatisation).

- Enjeu d'efficacité : l'adoption du cloud permet de bénéficier de services managés avec de la supervision et sécurité intégrées (base de données, dataplatform, IA/Chaine MLOps) ; en effet, la construction de tels services dans nos datacenters sur base de brique open source serait bien trop coûteuse à industrialiser.

Le terme générique de cloud recouvre habituellement trois niveaux de services différents : l'hébergement distant « Infrastructure as a Service » (IaaS), l'appui sur des composants techniques mutualisés pour simplifier la fabrication d'applications « Platform as a Service » (PaaS), et l'accès en mode locatif à des logiciels « Sofware as a Service » (SaaS).

Nous distinguerons dans la suite deux finalités :
- Le « cloud pour les équipes SI », qui recouvre le niveau **PaaS**[1];
- Le « cloud pour les utilisateurs », qui recouvre les services logiciels accédés par les salariés et les partenaires de RTE en **Saas**.

Suite au benchmark des usages cloud 2024 sur d'autres OIV françaises, il a été confirmé que les clouds publics français et les premiers clouds de confiance ne proposent pas un catalogue suffisant pour couvrir tous les besoins RTE en termes de services managés et de solutions de sécurité. Pour tirer profit au maximum des services clouds, les hyperscalers[2] sont à date les seuls à proposer un catalogue complet sous forme de solution PaaS. Suite à l'analyse menée par la DSIT (« Schéma directeur Cloud pour le SI de RTE - Etat des lieux et décisions »), il a été identifié que l'usage du cloud Azure offrait le meilleur compromis pour RTE sur le PaaS, du fait notamment de l'existant construit pour le projet S4us, de la montée en compétence initiée par quelques équipes projet (S4us, Gridsuite, Kiwi, Gridcapa, OperatorFabric…). Par ailleurs, à date l'hébergement Azure France ne permettant pas de couvrir tous les besoins des projets RTE (i.e. le service managé HPC pour le calcul intensif est basé sur Azure Europe du Nord), il est donc préconisé de positionner les projets RTE sur des services Azure Europe.

[1] Le terme PaaS recouvre les services managés tels que des bases de données, des outils d'orchestration de containers ou de clusters HPC, etc.
[2] Le terme "hyperscalers" désigne les entreprises qui possèdent et exploitent une infrastructure informatique à très grande échelle, leur permettant de fournir des services cloud (comme le stockage, la puissance de calcul, ou l'hébergement d'applications) à des millions d'utilisateurs dans le monde entier.

2 Données critiques RTE

Criticité des données

La méthode de classification de confidentialité des données de RTE a été définie dans un contexte où les offres des clouds commerciaux étaient peu matures technologiquement et n'amenaient pas un niveau de sécurité suffisant.
Du fait des mécanismes de sécurité disponibles sur le cloud, le niveau de confidentialité des données doit être traitée via une gestion des habilitations adéquate mais ne sera pas déterminante pour le choix d'hébergement.

Toutefois, afin d'assurer la résilience de ses activités, RTE doit évaluer la criticité d'une donnée qu'elle pourrait positionner sur le cloud.
Une donnée dans un processus métier spécifique est considérée, sous un angle opérationnel, comme critique, si elle répond aux conditions suivantes :

- Sa divulgation non maitrisée donnerait un avantage évident à un acteur industriel extra-européen sur le marché européen
- Son indisponibilité ou l'altération de son intégrité mettrait en risque un processus critique temps réel ou proche temps réel

Par souci de clarté, une donnée peut être considérée comme critique dans un processus temps réel mais in fine, ne plus l'être si elle est utilisée dans le cadre d'étude statistique ou de démarche d'innovation. Il est donc important d'analyser de manière conjointe la donnée et le processus visé (cf. « 3. Analyse de risques sur les processus et les données »).
A titre d'exemple, l'entrainement d'un modèle de prévision de consommation n'a pas d'impact direct sur la prévision de consommation proche temps réel – l'entrainement ne relève donc pas d'un processus critique et est ainsi éligible au cloud, il sera toutefois nécessaire de valider l'intégrité et la fiabilité du modèle entrainé sur un datacenter interne avant de le déployer en production.

En première analyse, les données relatives à des contentieux vis-à-vis d'un acteur industriel américain, ou les réponses aux appels d'offres sur un marché pour lequel l'un des candidats serait américain, doivent être considérées comme critiques.

Les données personnelles sensibles telles que définies par l'article 9, RGPD recouvrent les données suivantes :

- l'origine raciale ou ethnique,
- les opinions politiques,
- les convictions religieuses ou philosophiques ou l'appartenance syndicale,
- ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique,
- des données concernant la santé,
- des données concernant la vie sexuelle, l'orientation sexuelle d'une personne physique.

Ces données personnelles sensibles sont également considérées comme des données critiques RTE.

Données à caractère hautement personnel

Les données hautement personnelles incluent notamment des informations telles que (liste non exhaustive) :

- Le numéro de sécurité sociale,
- Les données relatives aux condamnations pénales ou aux infractions,
- Les données de localisation,
- Les données financières et bancaires,
- Les communications électroniques.

Cette catégorie de données personnelles, dont la liste n'est pas connue de façon exhaustive, est décrite dans les lignes directrices [3] spécifiques du G29 [4] sur les AIPD permettant de déterminer si des traitements sont susceptibles d'engendrer un risque élevé pour les personnes concernées.
Ainsi, si un projet traite des données à caractère hautement personnel, le projet devra mener une AIPD [5]. Toutefois ce type de données ne relèvent pas des données critiques RTE. La doctrine ne vient donc pas modifier le traitement actuel propre aux données à caractère hautement personnel ainsi ces données peuvent être hébergées sur le cloud à la condition de mettre en œuvre les recommandations faites par l'AIPD.

3 Analyse de risques sur les processus et les données

Une analyse du caractère critique de la donnée dans un processus métier spécifique doit être menée par le projet au plus tard en phase de faisabilité avec l'appui des experts cybersécurité de DSIT/DESIGN/CCoE et de la mission DPO. Cette analyse doit notamment identifier les données à caractère personnel qui doivent être traitées par l'écosystème informatique du projet pour caractériser si elles relèvent des données personnelles sensibles. Cette analyse doit être pilotée et validée par le référent confidentialité de la Direction métier concernée. Dans le cas où le projet souhaite utiliser des données issues de plusieurs domaines métiers, l'analyse doit être pilotée et validée par le/la responsable de la gouvernance de la donnée. Une saisine de la Direction Juridique demeure en tout état de cause toujours possible si besoin.

Si l'une des données utilisées par le projet relève des données critiques RTE, alors cette donnée devra être hébergée et transiter uniquement sur des datacenters internes RTE ou cloud souverain européen[6]. Cela signifiera également que cette donnée critique ne devrait pas être hébergée ou transférée via des outils clouds américains (M365, SharePoint online, Teams, WhatsApp, iPhone…).

[3] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679Cf. wp248 rev.01_fr (page 11 §4)
[4] Groupe de travail rassemblant les représentants de chaque autorité européenne de protection des données
[5] AIPD désigne une Analyse d'Impact relatif à la Protection des Données personnelles
[6] Cloud souverain européen désigne un fournisseur de cloud dont le siège social est basé en Europe, dont les datacenters sont localisés en Europe et qui est exempt de toute législation extraterritoriale tel que le Cloud Act et FISA

4 Concernant le cloud pour les équipes SI (PaaS)

Ce chapitre concerne les applications/outils développés en spécifique par RTE.

4.1 Mécanismes de sécurité préconisés

Les mécanismes de sécurité (i.e. authentification, chiffrement…) existants ne permettent pas de garantir totalement la sécurité[7] d'une donnée critique face aux moyens des fournisseurs de clouds américains.
Les solutions de chiffrement existantes (cf. liste ci-dessous) assurent la protection des données au repos mais elles ne permettent pas de garantir la protection des données lorsqu'elles sont manipulées durant leur traitement :

- le chiffrement natif (clé gérée par l'hébergeur avec son générateur de clés)
- le chiffrement BYOK[8] (clé gérée par RTE avec le générateur de clés de l'hébergeur)
- le chiffrement HYOK[9] (clé gérée par RTE avec le générateur de clés d'un tiers)

A date, les technologies de chiffrement des données pendant le traitement ne sont pas assez matures dans le contexte cloud, ainsi la seule solution préconisée pour l'hébergement d'une donnée critique RTE sera un hébergement dans les datacenters internes de RTE.

Suite à l'analyse par le projet, si aucune donnée ne relève ni des données critiques ni des données personnelles sensibles, par défaut, les mécanismes de sécurité suivants devront être mis en œuvre par le projet :

- chiffrement natif offert par le cloud Azure des données au repos et chiffrement en transit (ainsi les données sont protégées d'une atteinte externe hors fournisseur cloud)
- désactivation des points de terminaison publics (ainsi l'accès à l'environnement du projet n'est pas directement exposé sur internet, il est uniquement accessible que depuis le SI RTE)

L'application de ces mécanismes fera l'objet de contrôles par le CCoE.
Toute application hébergée dans le cloud Azure devra appliquer dès sa conception les politiques de sécurité cloud en vigueur telles que définies par le CCoE et devra s'insérer dans les infrastructures sécurisées[10] par le CCoE (« LandingZone »[11]).

[7] Le terme sécurité ici recouvre la disponibilité, l'intégrité, la confidentialité et la traçabilité de la donnée
[8] Le BYOK ne permet pas de s'assurer techniquement que le fournisseur cloud ne dispose pas des clés de chiffrement au repos car elles sont générées par son générateur de clés – de plus, le coût de ce service n'est pas négligeable : facturation par transaction auquel il faut ajouter les coûts d'administration
[9] A noter que les technologies HYOK (i.e CipherTrust Thales) ne sont pas compatibles avec les services PaaS Azure et bien qu'elles existent sur AWS (XKS), certains services PaaS AWS qui seraient nécessaires pour RTE (Parallel Cluster multi-région, Databricks) ne sont pas compatibles avec XKS.
[10] D'autres systèmes de sécurité viennent s'ajouter à ceux préconisés pour les applications mais sont de la responsabilité du CCoE (i.e détection d'attaques ou d'intrusion via une supervision centralisée de la landing zone, contrôle et gestion des droits, scan de contrôle de la bonne application des politiques de sécurité).
[11] La landing zone est un espace privé et sécurisé dédié à RTE au sein du cloud opéré par Microsoft Azure.

4.2 Nature des applications devant être hébergées sur le cloud

Les applications développées en spécifique respectant l'ensemble des critères suivants devront par défaut s'appuyer sur les services Azure hébergés en Europe en faisant appel au CCoE[12] :

- Nécessitent des services managés s'appuyant sur des infrastructures HPC (CPU/GPU) avec une élasticité[13] dans la consommation de ressources
- La plage d'intervention en cas d'incident est du Lundi-Vendredi 5j/7, 9h-18h
- N'utilisent aucune donnée critique RTE
- Ne nécessitent pas de flux bidirectionnel Datacenter RTE <-> Cloud (*voir annexe d*)

Dans le cas où l'équipe projet responsable d'une application respectant tous ces critères ne prévoit pas de s'appuyer sur le cloud, elle devra faire valider sa demande de dérogation au COSIT[14].

Pour les applications ne respectant pas tous ces critères, ces dernières peuvent également s'appuyer sur le cloud selon l'arbre de décision décrit en annexe B. Si leur positionnement sur le cloud est permis selon cet arbre de décision, ils devront par défaut s'appuyer sur Azure via le CCoE.

Les « proof of concept » (en phase d'opportunité ou phase de faisabilité) ne nécessitant pas de tester une intégration dans le SI hébergé sur les datacenters internes RTE, devront également par défaut s'appuyer sur Azure via le CCoE (*voir annexe C*).

4.3 Appui à la consommation des offres cloud

RTE contractualise avec Azure via la centrale d'achat public UGAP. Chaque application disposera de son propre abonnement Azure pour suivre ses coûts Azure et le CCoE aura également accès à la totalité des abonnements. La refacturation des coûts Azure de l'abonnement concerné sera faite à chaque projet (en opex). Chaque projet devra définir un seuil de dépense mensuel, conforme à son estimation des coûts de sa consommation à la création de sa souscription. Une alerte sera reçue en cas d'approche de ce seuil et permettra de limiter les dépassements. Le CCoE, ainsi que les responsables du projet, seront destinataires de cette alerte.

4.4 Compétences

Les prestataires externes et les membres internes des équipes projet allant sur le cloud devront avoir des compétences cloud Azure pour être suffisamment autonomes. Le cas échéant, les plans de formation des membres internes des projets allant sur le cloud devront comporter un volet cloud Azure coconstruit avec le CCoE. Il en va de même pour ceux des Architectes techniques concernés.

[12] CCoE (Cloud Center of Excellence) désigne l'équipe DSIT/DESIGN en charge de l'offre de service cloud pour administrer la landing zone RTE sur Azure et accompagner les projets qui s'appuient sur cette dernière.
[13] Le terme élasticité signifie ici que les calculs ne sont pas exécutés en continu sur du 24/7 (peu ou pas de calcul hors heures ouvrés)
[14] COSIT (Comité de Sécurisation IT) désigne le comité SI en charge des revues techniques des projets en amont de la décision d'investissement.

4.5 Portabilité

La portabilité multi-clouds voire si possible sur les datacenters internes RTE doit être recherchée à chaque projet. A cette fin, les équipes informatiques s'assureront avec l'appui du CCoE que les adhérences techniques et fonctionnelles à Azure sont identifiées et justifiées par des gains opérationnels évidents lorsqu'elles sont engageantes de manière durable. Le cas échéant, une telle dépendance doit rester l'exception.

5 Concernant le « cloud pour les utilisateurs » (SaaS)

Les éditeurs de logiciels offrent pour la grande majorité des solutions Saas et incitent leurs clients à y souscrire. Cette tendance est particulièrement marquée pour les logiciels Corporate (RH, Finance, bureautique, Achats…) pour lesquels l'offre fonctionnelle est plus riche et évolutive en mode SaaS qu'en achat classique (qui parfois n'est d'ailleurs plus possible).

La DSIT doit accompagner les métiers pour faciliter l'identification des offres logicielles SaaS qui répondront le mieux aux enjeux simultanés d'ergonomie, de richesse fonctionnelle, de sécurité, de protection des données et de facilité d'utilisation.
Cet accompagnement doit également être l'occasion d'identifier les opportunités de mutualisation pour réaliser des économies d'échelle ou des gains opérationnels.

Un clausier sécurité viendra préciser les exigences contractuelles devant être respectées par les éditeurs de solution SaaS et se réfèrera aux conditions décrites dans la Doctrine Cloud en vigueur.
Le chiffrement des données (en transit et au repos) sera exigé et mis en œuvre par l'éditeur[15].

A titre d'illustration, les solutions SaaS retenues devront répondre à des exigences de :

- Sécurité renforcée comme la surveillance continue des environnements par le Titulaire et la notification de RTE en situation d'incident, yc incident d'origine Cybersécurité ;
- Gestion des identités et des accès pour garantir que seuls les utilisateurs autorisés peuvent accéder aux données à caractère hautement personnel ;
- Conformité réglementaire vis-à-vis du RIA[16] et du RGPD avec mise en œuvre de l'AIPD si des données hautement personnelles sont traitées ;
- Performances, résilience et fiabilité au regard du besoin exprimé ;
- Gestion des données pour assurer leur portabilité, ainsi qu'une stratégie de sauvegardes régulières pour se prémunir contre les pertes accidentelles ou malveillantes.

[15] Pour un SaaS, le chiffrement par RTE n'est pas possible ainsi il est exigé contractuellement pour être mis en œuvre par l'éditeur

[16] RIA (AI Act) : Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (Règlement - UE - 2024/1689 - EN - EUR-Lex)

5.1 Nature des applications devant être en SaaS par défaut

Tous les projets relevant du SI Corporate doivent privilégier les offres SaaS pour leur recherche de solution. Cette étude sera réalisée conjointement entre le métier concerné, le responsable DSIT/DPCO et la MOA SI.

En l'absence de solutions SaaS adaptées sur le marché, elles peuvent engager un développement sur mesure limité au périmètre spécifique en question.

Afin de maitriser la stratégie achat de services numériques, la diversité des fournisseurs doit être recherchée à l'échelle de RTE sur chaque segment des services aux utilisateurs, pour éviter la création de marchés captifs. Les chefs de projet doivent, chaque fois que possible, évaluer plusieurs offres couvrant leurs besoins.
La solution doit être conforme aux exigences de sécurité définies par la DSIT, assurer un hébergement de bout en bout[17] en Europe[18] et offrir contractuellement des dispositifs de supervision (incluant des rapports sur le niveau de service) à destination de RTE pour s'assurer de la qualité de service.
Le choix d'un SaaS est également engageant pour le métier, aucun développement fonctionnel spécifique interne au SaaS ne sera demandé et implémenté (hors configuration). Ainsi les directions métiers devront intégrer cette limite et, le cas échéant, adapter leurs processus opérationnels aux standards du marché lorsque les outils choisis sont basés sur des SaaS.

5.2 Exceptions pour les données critiques RTE

Pour les applications devant traiter des données critiques RTE telles que décrites au chapitre 2, les lois extraterritoriales américaines (FISA 702 (1) et Cloud Act (2)) ne permettent pas de garantir à date que les données hébergées chez un acteur américain ne seront jamais transférées aux Etats-Unis dans le cadre d'une instruction judiciaire. Aussi, il est obligatoire d'héberger ces données sur les datacenters internes RTE ou sur un cloud souverain européen dans ce cas.

Pour rappel :

(1) FISA 702 : Permet aux agences américaines (comme la National Security Agency « NSA ») de collecter des données auprès de fournisseurs électroniques (comme AWS, Microsoft (Azure), Google) même si les données sont hébergées hors des États-Unis, tant que l'entreprise est soumise à la juridiction américaine. La collecte peut se faire sans notification ni consentement du citoyen concerné (même si européen).

(2) Cloud Act : Autorise les autorités américaines à accéder aux données stockées à l'étranger par une entreprise américaine, via mandat ou assignation. Cela oblige les fournisseurs de services cloud américains à remettre les données même si elles sont stockées dans des datacenters hors des USA.

[17] Cette prescription sur l'hébergement vise toutes les sauvegardes
[18] Au titre de la conformité avec le RGPD

6 Synthèse de la doctrine

En résumé des conditions décrites précédemment, la mise en œuvre de la doctrine sur des applications SI pour les différentes catégories du SI aboutit à la matrice suivante :

Catégorie du SI (SIIV, Industriel, Corporate, Bureautique)	Hébergement(s) préconisé(s)
Application SIIV	Datacenter interne uniquement
Application SI Industriel relevant d'un processus critique TR ou proche TR	Datacenter interne uniquement
Application SI Industriel hors processus critique TR ou proche TR	Datacenter interne ou Cloud en PaaS (sauf si elle manipule des données critiques)
Application SI Corporate/Bureautique avec donnée critique	SaaS sur cloud souverain par défaut ou datacenter interne si pas d'offre SaaS disponible
Application SI Corporate/Bureautique sans donnée critique	SaaS en Europe par défaut ou datacenter interne si pas d'offre SaaS disponible
Outil non industriel/démonstrateur/POC	Cloud en PaaS par défaut ou datacenter interne s'il manipule des données critiques

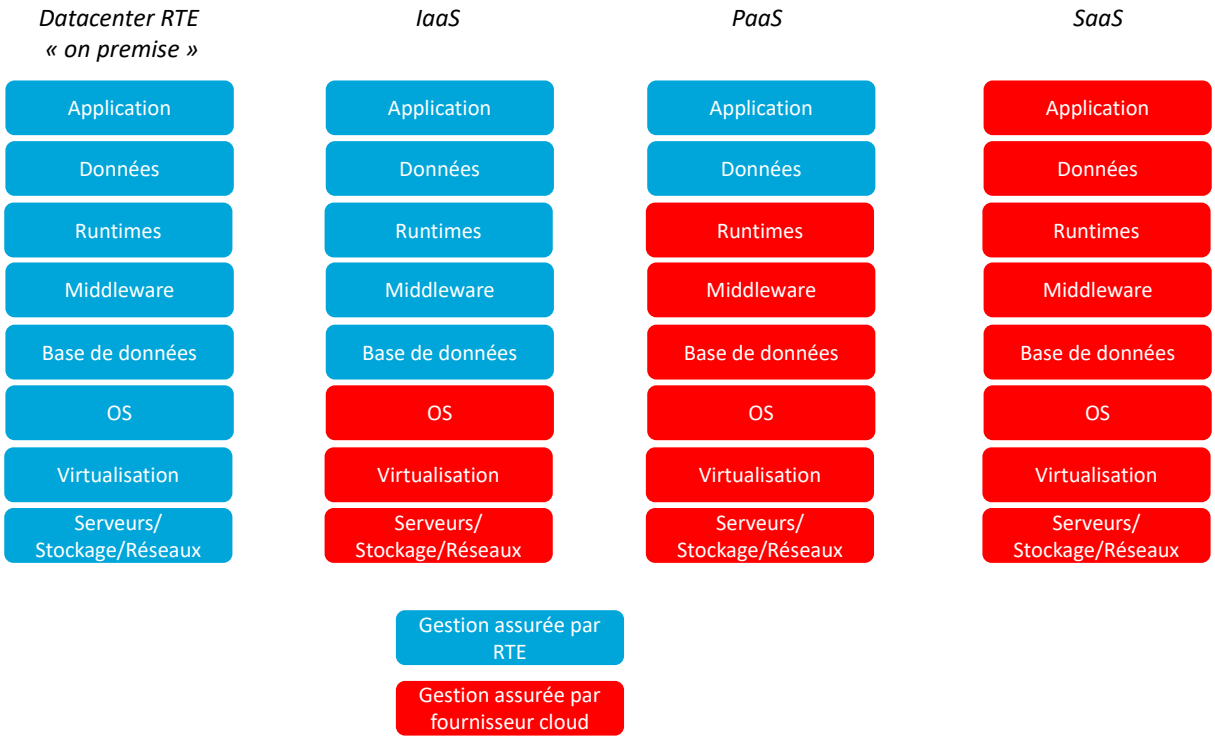
7 Mise à jour de la doctrine

Cette doctrine aura vocation à évoluer avec l'enrichissement de l'offre de service proposée par le CCoE et de l'évolution de la réglementation internationale et de l'état de l'art techniques. Elle devra faire l'objet d'un premier retour d'expérience au second trimestre 2026. De plus, comme prévu par la feuille de route technologique, une nouvelle évaluation du catalogue des services proposés par les clouds souverains européens devra être menée en 2027. Les conclusions de cette nouvelle évaluation pourraient également aboutir à devoir amender la doctrine en conséquence, en vue d'une probable migration sur un cloud souverain européen au cours de la période tarifaire TURPE 8.

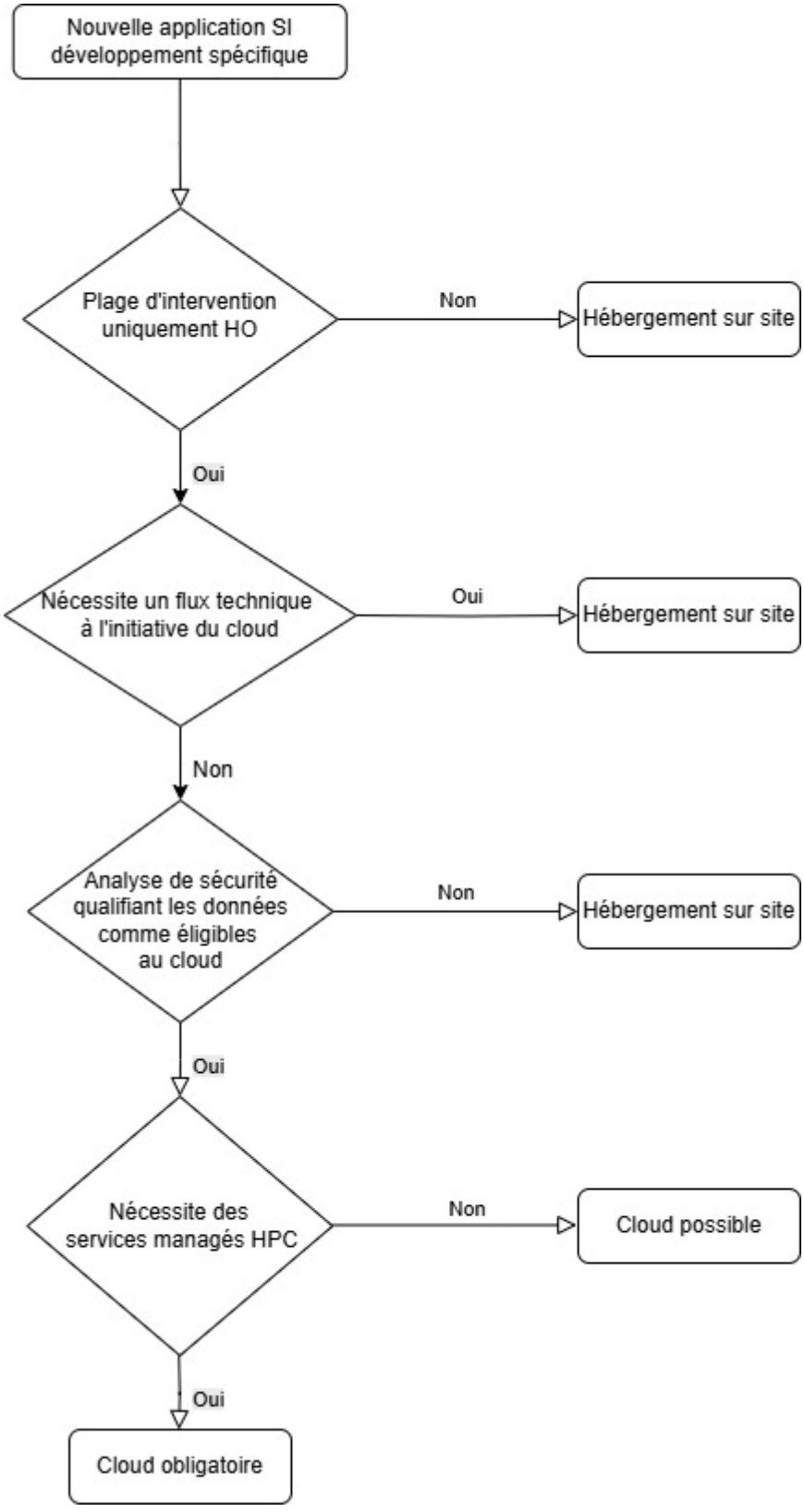
Signataires (Titre / Nom)

Annexes

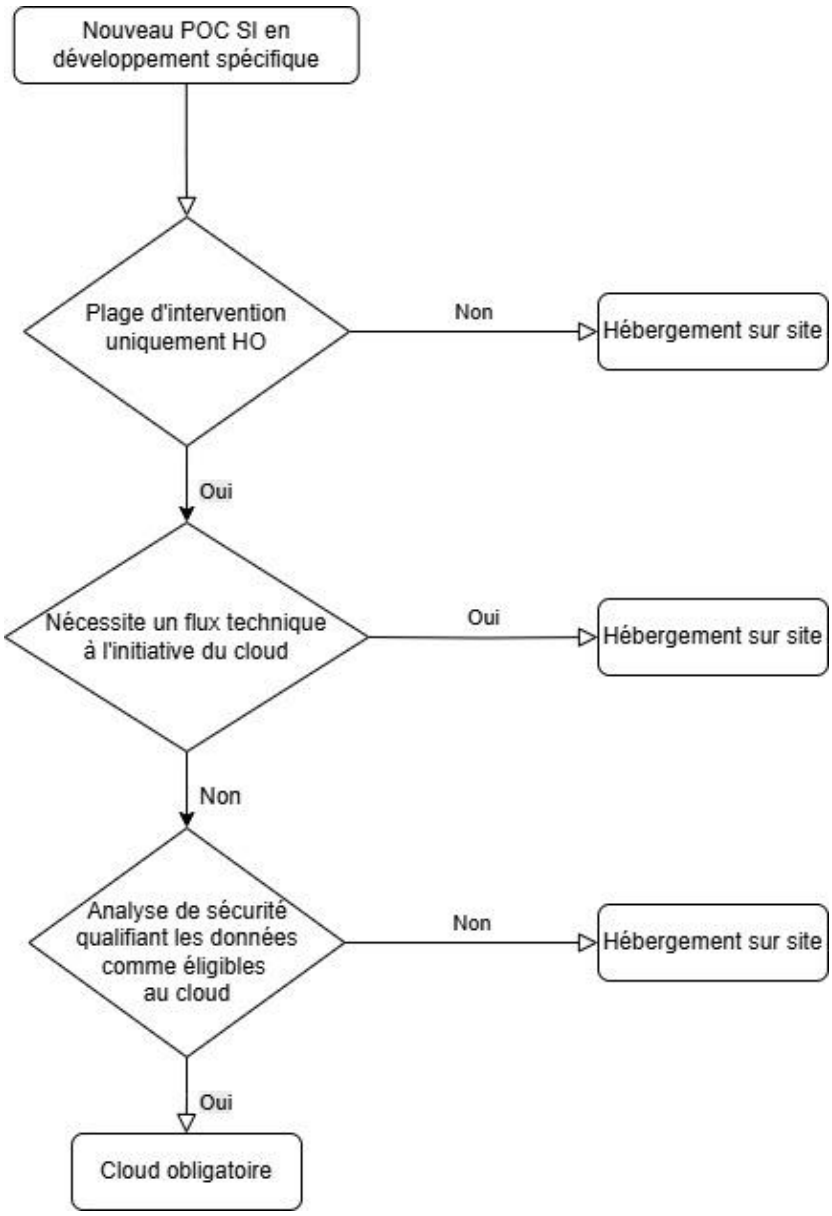
a. Description des services gérés par RTE et le fournisseur cloud selon les environnements retenus



b. Arbre de décision pour le positionnement d'une application SI développée en spécifique

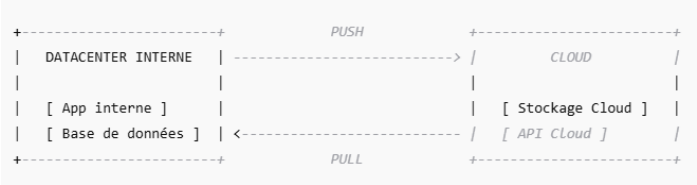


c. Arbre de décision pour le positionnement d'un POC SI développée en spécifique



d. Description des flux autorisés entre les datacenters RTE et la landing zone Azure RTE

A l'exception des flux spécifiques entre Gaia (solution d'authentification RTE) et Azure, seuls des flux techniques à l'initiative du datacenter interne RTE via une connexion réseau privé dédiée (« express route Azure ») tels que décrits ci-dessous sont autorisés à date.



e. Classification des applications par type d'hébergement (non exhaustif)

Catégorie du SI	Exemples d'applications	Hébergement préconisé	Justification de l'hébergement
SIIV (i.e Stanway, NAZA)	Stanway, NAZA, etc.	Datacenter interne	Leur altération ou indisponibilité affecte directement un processus TR
SI Industriel relevant d'un processus critique TR ou proche TR	**Conduite du réseau :** GridHorus, OperatorFabric, Gridsuite (pour le métier exploitation), Consol, SEA, Stabsys, chaine d'inférence IPES-N et SCONSO, Assistflux **Chaine EOD TR et proche TR** : Titien (limité aux données chaudes), Topniveau, Topase, Gipse, Daisy, Spa, Smash, Trio, Totem, Racoon, Cia, Rmc, Tao, Ocappi, Scorpion, Cristal, Ouistiti **Chaine de supervision et de gestion TR des incidents CORSN** : SIEM SNP & DCH, Centreon, Plasma	Datacenter interne	Leur altération affecte directement des processus TR ou proche TR
SI Industriel hors processus critique TR ou proche TR	**Chaine EOD back office :** Bob, Boss, Coreal, Fenix, CDP Prod, Kiwi, Coyote **Chaine d'analyse ex-post/REX** (outillage AESIS) **Chaine de publication des données** : TACITE **Bases patrimoniales et gestion de portefeuille GI (PAPT, PFM1)**	Datacenter interne ou Cloud en PaaS possible	Leur altération ou indisponibilité n'affecte pas directement des processus TR ou proche TR (à date, aucune application de cette catégorie ne manipule de donnée critique – aucun acteur industriel américain n'intervient sur le marché de l'électricité à date – si ce cas se présente, alors l'hébergement devra obligatoirement être sur un datacenter interne)
	Chaine d'entrainement des prévisions ENR, Consommation, Assistflux	Cloud en PaaS par défaut	Leur altération ou indisponibilité n'affecte pas directement des processus TR ou proche TR. Nécessitant du calcul intensif (GPU/CPU) de

	Etudes prospectives ou décisionnelles : Antares, Imagrid, RFS		manière variable, ils doivent par défaut être positionnés sur le cloud
SI Corporate/Bureautique avec donnée critique	Portail fournisseur Aida Artesis Simed Asterisq	SaaS sur cloud souverain par défaut ou datacenter interne si pas d'offre SaaS disponible	Manipule des données critiques (i.e réponse à des appels d'offre dont des sociétés américaines, données de santé, orientation sexuelle, appartenance syndicale)
SI Corporate/Bureautique sans donnée critique	Office365 Propulse	SaaS en Europe par défaut ou datacenter interne si pas d'offre SaaS disponible	Ne manipule pas de donnée critique