Stratégie Cloud du Secteur Public Français – Adaptation du Cadre Canadien (GGCL) au Contexte de la France

Contexte Général (France vs. Canada). La France a adopté en 2021 une doctrine nationale ambitieuse – **« Cloud au Centre »** – visant à généraliser l'usage du cloud dans l'administration **sous réserve de garanties de souveraineté strictes**. À l'inverse, le Canada applique depuis 2018 une approche « **Cloud First** » plus pragmatique, autorisant largement le recours aux grands clouds publics internationaux pour ses données sensibles (*niveau Protégé B*) avec des mesures d'atténuation des risques[1] [2]. **En d'autres termes, la France privilégie d'emblée un "cloud de confiance" souverain, tandis que le Canada a d'abord misé sur le cloud commercial avec des garde-fous, avant d'évoluer récemment vers davantage de souveraineté.** Le tableau ci-dessous résume d'un coup d'œil ces différences de doctrine :

Doctrine « Cloud au Centre » en France : Cloud de Confiance et Souveraineté d'État

En juillet 2021, le gouvernement français a émis une circulaire fixant une nouvelle doctrine cloud pour le secteur public, résumée ainsi : **« le Cloud au centre de la transformation numérique de l'État, mais aux conditions du Cloud de Confiance »**[3]. Cela signifie que **les ministères et administrations doivent d'abord envisager des solutions cloud** (plutôt que de nouveaux serveurs locaux) pour tout projet informatique, *à condition* que ces solutions respectent la **doctrine de confiance de l'État**. Les grands principes de cette doctrine sont :

- **Souveraineté & Localisation des données :** Les services cloud utilisés doivent garantir que **les données restent sur le sol européen et protégées du droit étranger**[4]. Concrètement, cela impose de recourir à des offres opérées par des entités de droit européen, sans lien de subordination juridique avec un pays tiers (en

[1] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[2] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[3] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[4] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

particulier les États-Unis et leur *Cloud Act*)[5]. *Exemple :* héberger les données d'un ministère sur une plateforme gérée par une société française/européenne, plutôt que directement chez un hyperscaler américain non contrôlé en Europe.

- **Certification de sécurité ANSSI obligatoire (SecNumCloud)** : Pour être qualifié de **"cloud de confiance"**, un fournisseur doit obtenir la **qualification SecNumCloud 3.2** délivrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[6]. Ce label exige de hauts standards de sécurité (accréditation ISO 27001, cloisonnement, chiffrement, etc.) *et* des garanties juridiques de souveraineté. **À partir de 2021, l'État français réserve l'hébergement de ses données sensibles aux seuls clouds disposant de cette qualification**[7]. Au moment de l'annonce, cela excluait de fait les offres des Big Tech américaines (aucune n'était qualifiée SecNumCloud) – seuls des fournisseurs 100% français l'avaient obtenue (OVHcloud, 3DS Outscale, Oodrive)[8] [9].
- **Hiérarchisation selon la sensibilité :** La doctrine distingue les cas d'usage :
    - Pour les **données les plus critiques** (défense, intérieur…), il est préconisé d'utiliser les infrastructures **souveraines de l'État** ou des clouds nationaux déjà qualifiés (solution interne type Ministère des Armées ou clouds privés de l'État appelés "Nuages ministériels")[10].
    - Pour les **données sensibles ou personnelles courantes** (niveau équivalent Protégé B), l'administration **peut recourir au cloud public** *uniquement si* le prestataire est certifié SecNumCloud (*ex:* un ministère peut externaliser sa

[5] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[6] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[7] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[8] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[9] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[10] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

messagerie sur une solution SecNumCloud, mais pas sur Microsoft 365 tant que celui-ci n'est pas certifié via un partenaire en France)[11] [12].

- Pour des **données peu sensibles ou des besoins non-prodal**, la doctrine est un peu plus souple : les acteurs publics peuvent éventuellement utiliser des clouds non certifiés pour ces cas limités, *sur dérogation expresse et transitoire*. En pratique, cela a permis par exemple de tolérer temporairement l'usage de certains outils collaboratifs non qualifiés pendant que l'offre de confiance se mettait en place (cas du Health Data Hub sur Azure en 2020-21, qui a déclenché cette doctrine)[13].

En résumé, **la France a ancré dans sa doctrine l'idée que la transformation cloud doit se faire sans compromis sur la maîtrise des données**. Ce resserrement a été motivé par des épisodes comme l'invalidation du Privacy Shield UE-USA en 2020 et la polémique de 2021 sur l'hébergement des données de santé françaises chez Microsoft : ces événements ont convaincu l'État d'éviter de dépendre d'opérateurs soumis à des lois extraterritoriales[14] [15]. La stratégie Cloud au Centre vise donc un double objectif : **accélérer la modernisation numérique** (en tirant profit de l'élasticité et de l'agilité du cloud) tout en **préservant la souveraineté** (juridique et opérationnelle) sur les infrastructures critiques.

Comparaison canadienne : Au Canada, la politique équivalente (les **"Guidelines for Government Cloud Use"** ou stratégie d'adoption du cloud) a initialement adopté une posture presque inverse : *tout ce qui n'est pas expressément interdit peut aller dans le cloud.* Le gouvernement canadien a classé ses données par niveaux (Protégé A = public, Protégé B = sensible moyen, Protégé C = très sensible) et autorisé dès 2018 le stockage des données Protégé B sur des clouds publics commerciaux, y compris opérés par des sociétés

---

[11] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[12] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[13] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[14] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

[15] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

étrangères, **à condition que les données restent hébergées physiquement au Canada**[16] [17]. Des contrats-cadres via Services Partagés Canada imposent cette résidence locale et des mesures comme le chiffrement des données et la gestion interne des clés de cryptographie[18]. Ainsi, la stratégie canadienne a d'abord mis l'accent sur la rapidité et l'efficacité du **"Cloud d'abord"**, estimant pouvoir gérer les risques de souveraineté via des *"contrôles de sécurité"* (basés sur l'ITSG-33 et des principes Zero-Trust) plutôt que par une interdiction pure et simple[19]. Cette approche plus ouverte a permis au Canada de migrer rapidement de nombreuses applications vers Microsoft Azure ou Amazon Web Services (au point que plus de **90 organismes publics canadiens** utilisent aujourd'hui du cloud public, Azure étant le plus utilisé)[20]. **Cependant**, le Canada a commencé à infléchir sa position depuis 2022-2023 vers davantage de souveraineté, conscient comme l'Europe des enjeux stratégiques : la mise à jour 2023 de sa stratégie mentionne le besoin de répondre aux exigences de **« résidence des données et souveraineté »** dans le cloud[21], et le gouvernement a lancé en 2024 un programme de **« Sovereign AI Cloud »** doté de 2 milliards $CAN pour stimuler des infrastructures cloud/IA nationales[22] [23]. *(Voir plus loin : Initiatives récentes.)*

---

[16] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[17] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[18] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[19] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[20] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/Documents/Microsoft%20Copilot%20Chat%20Files/P118-34-2024-eng.pdf?web=1

[21] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[22] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[23] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

Sécurité et Conformité : Certification SecNumCloud vs. Approche Contractuelle

SecNumCloud et « Cloud de confiance » français. Le **label SecNumCloud** est le pilier technique du cloud de confiance à la française. Établi dès 2016 par l'ANSSI, ce référentiel de sécurité est devenu en 2021 un passage obligé pour les prestataires souhaitant héberger des données d'organismes publics. La version 3.2 (mars 2022) de SecNumCloud a renforcé les critères de **souveraineté juridique** en plus des mesures de cybersécurité :

- Le fournisseur doit être une **entreprise de droit de l'UE ou de l'Espace économique européen**, avec son siège en Europe[24] [25].
- **Aucun actionnaire ou entité extra-européen** ne doit pouvoir exercer de contrôle ou accès privilégié aux données ou infrastructures. En pratique, l'ANSSI impose une gouvernance à majorité européenne : par exemple, si une technologie américaine est utilisée sous licence, l'opérateur du service cloud doit être une société contrôlée par des intérêts français/UE (d'où la création de joint-ventures pour "européaniser" Azure et Google Cloud, voir section suivante)[26] [27].
- Les **données et traitements doivent s'effectuer uniquement sur le territoire de l'UE** (centres de données en France ou pays UE).
- Sur le plan sécurité technique : la plateforme doit répondre à ~40 exigences couvrant le **chiffrement des données** (y compris clés détenues par l'opérateur ou le client, selon les cas), la **compartimentation** entre clients, la **supervision 24/7**, la **gestion des vulnérabilités**, etc. Il s'aligne sur des normes de type ISO 27001/27017/27018, avec des contrôles supplémentaires de niveau *ANSSI* (par ex. tests d'intrusion, configurations durcies).
- L'opérateur qualifié doit accepter des **audits réguliers** et contrôles de l'ANSSI. La qualification est à renouveler périodiquement (tous les 3 ans généralement).

[24] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[25] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[26] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[27] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

Actuellement (fin 2023), **quatre fournisseurs français** ont la qualification SecNumCloud : **OVHcloud**, **3DS Outscale** (Dassault Systèmes), **Oodrive** et **Scaleway** (groupe Iliad)[28]. Ils offrent principalement des solutions **IaaS/PaaS** (infrastructure virtuelle, stockage, parfois containerisation). Par exemple, Outscale (filiale de Dassault) a été le premier dès 2019 à être qualifié pour son IaaS souverain[29]. D'autres acteurs français, comme **NumSpot** (nouvelle coopérative entre Docaposte, Bouygues Télécom, la Caisse des Dépôts et Dassault-Outscale), sont en cours de démarche pour des offres PaaS souveraines en s'appuyant sur ces infrastructures existantes (NumSpot vise une qualification en 2024)[30] [31].

> **Critères principaux de la qualification SecNumCloud 3.2 (France)**[32] [33]
>
> - **Localisation UE** de l'hébergement des données et de l'administration de la plateforme (datacenters situés en France ou en Europe).
> - **Immunité juridique** vis-à-vis des lois extra-européennes : contrôle capitalistique majoritaire par des entités européennes, aucun droit d'accès privilégié pour une maison-mère non-UE.
> - **Support et exploitation localisés en UE** (équipes ingénierie/opération basées en France ou en Europe uniquement).
> - **Chiffrement des données sensibles** en stockage et en transit + gestion saine des clés (pas d'accès en clair non justifié).
> - **Sécurité opérationnelle** de haut niveau : supervision continue, gestion des patchs en <30 jours, segmentation réseau forte, authentification multi-facteurs, etc.
> - **Haute disponibilité** : redondance multi-sites en France/UE, plan de reprise, localisation de secours intra-UE.
>
> *(Source : référentiel SecNumCloud v3.2, 2022)*

---

[28] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[29] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[30] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[31] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[32] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[33] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

En contrepartie de ces exigences strictes, une offre SecNumCloud est considérée par l'État comme **"apte à recevoir des données sensibles confidentielles"**. Ainsi, **le stockage de données de santé, de données fiscales, d'enquêtes judiciaires, etc., doit être confié à un prestataire SecNumCloud (ou équivalent)**. La circulaire 2021 précise que les DSI ministérielles doivent s'assurer de la conformité SecNumCloud de leurs fournisseurs cloud avant de leur confier des charges de travail sensibles[34].

Pour l'instant, **aucun géant étranger n'a obtenu SecNumCloud**, ce qui reflète l'ambition française de soutenir ses propres acteurs. Toutefois, l'État a aussi encouragé des modèles hybrides innovants pour combler l'écart technologique avec les hyperscalers – c'est l'objet des partenariats présentés plus loin (Bleu, S3NS), où les technologies de Microsoft et Google seront exploitées en *confiance* via des sociétés de droit français qualifiables SecNumCloud[35] [36].

Approche canadienne : Le Canada, de son côté, n'a pas de label de sécurité dédié au cloud souverain. Il s'appuie sur des **normes globales (ISO, SOC 2) et sur les certifications des fournisseurs (ex: FedRAMP américain)** pour évaluer le niveau de sécurité des clouds publics, combinés à ses propres exigences (contrôles Cloud du Centre pour la cybersécurité). Plutôt que de certifier les fournisseurs, le Canada choisit les *"Services cloud certifiés par ailleurs"* et **ajoute des conditions dans ses appels d'offres** : par exemple, les contrats conclus via Services Partagés Canada avec AWS, Azure ou Google Cloud imposent la **résidence des données au Canada**, la **notification en cas de demande légale étrangère**, et la possibilité de **chiffrer les données avec clés gérées par le gouvernement**[37]. En pratique, le gouvernement canadien utilise des régions cloud situées sur le sol canadien (p. ex. usager d'Azure Canada Centre ou AWS Montréal) pour stocker ses données, réduisant l'exposition aux lois extraterritoriales.

Jusqu'en 2023, aucun incident notable n'a remis en cause ce modèle, mais il existe une **incertitude juridique** : en 2021, devant le Sénat français, Microsoft a admis qu'il ne pouvait garantir qu'un gouvernement étranger n'accède pas aux données de ses clients européens

---

[34] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[35] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[36] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[37] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

en vertu de lois comme le Cloud Act[38]. Ce genre de déclarations a eu un écho au Canada également, où la **question de la souveraineté des données est devenue un sujet politique en 2023-2024**[39] [40]. Désormais, la stratégie canadienne affiche dans ses principes qu'il faut tenir compte de la **souveraineté numérique** (Principe "Cloud Security" – répondre aux besoins de « data residency and sovereignty »)[41]. Fin 2024, le Canada a lancé un **"Sovereign AI Compute Strategy"** avec 2 milliards $CAN pour financer des centres de données et supercalculateurs *nationaux*[42] [43]. Cela inclut la volonté de développer un **cloud canadien** qui réduise la dépendance aux fournisseurs américains et assure une maîtrise locale des infrastructures critiques (notamment pour l'IA et le quantique)[44] [45]. En somme, *le Canada est en train de rattraper son retard en matière de souveraineté*, en passant d'une approche contractuelle **« confiance pragmatique »** à une approche plus normative inspirée de l'Europe. On notera d'ailleurs que dans un **Mémorandum Canada–R.-U. de 2023**, les deux

[38] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[39] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[40] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[41] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[42] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[43] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[44] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[45] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

pays s'engagent à coopérer pour développer des capacités de calcul/stockage souveraines tout en continuant à utiliser prudemment les clouds globaux actuels[46] [47].

Acteurs et Solutions « Cloud Souverain » : Bleu, S3NS, NumSpot, etc.

Pour mettre en œuvre sa stratégie, la France a encouragé la création de **partenariats public-privé innovants** et le développement de nouveaux services cloud conformes à SecNumCloud, afin de disposer d'alternatives compétitives aux géants existants :

- **Projet Bleu (Orange + Capgemini + Microsoft)** : Annoncée en mai 2021, **Bleu** est une co-entreprise détenue majoritairement par les français Orange et Capgemini, destinée à opérer les technologies **Microsoft Azure et 365** en France dans un environnement SecNumCloud[48] [49]. L'idée est de **fournir aux administrations le riche catalogue d'Azure/Office** (puissance de calcul, outils collaboratifs) **mais via une entité française souveraine** (Microsoft n'ayant aucun accès privilégié aux données ou au CA de Bleu)[50] [51]. La Commission européenne a validé ce montage en 2022 (conformité antitrust) et Bleu a démarré ses activités commerciales en janvier 2024[52]

---

[46] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B68C1E4B1-5F93-4BE9-99CC-09DA87960592%7D&file=Document%2033.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[47] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B68C1E4B1-5F93-4BE9-99CC-09DA87960592%7D&file=Document%2033.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[48] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[49] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[50] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[51] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[52] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[53]. **Calendrier :** Bleu a commencé à travailler avec des clients pilotes publics fin 2024, et vise la qualification SecNumCloud d'ici mi-2025[54] [55]. À terme (2025+), un ministère pourra donc utiliser Microsoft 365 ou déployer des applicatifs Azure sur la plateforme Bleu en bénéficiant de l'**écosystème Microsoft complet et** du niveau de confiance requis par l'État. C'est considéré comme un projet stratégique – Orange lui-même s'est engagé à migrer **70% de ses propres applications IT vers Bleu d'ici fin 2025**, ce qui crédibilise la solution.

- **Projet S3NS (Thales + Google)** : Lancée en juin 2022, **S3NS** (prononcer *"sens"*) est la co-entreprise entre le groupe français Thales (majoritaire) et Google Cloud[56]. Objectif : offrir les services **Google Cloud Platform (GCP) et Google Workspace** via une entité de confiance française répondant aux critères SecNumCloud[57]. En juillet 2024, S3NS a déposé son dossier auprès de l'ANSSI et vise la qualification d'ici l'**été 2025**[58]. **Dès fin 2024**, S3NS a commencé à faire migrer une trentaine de clients pilotes sur son infrastructure test (parmi eux, des entreprises privées et probablement quelques administrations innovantes)[59]. Comme Bleu, S3NS prévoit un réseau de centres de données sur le territoire français et un **contrôle intégral par Thales** (Google n'a aucun droit de vote au conseil d'administration)[60] [61]. Si S3NS

---

[53] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[54] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[55] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[56] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[57] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[58] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[59] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[60] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[61] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

obtient le label en 2025, l'État pourra exploiter des solutions comme Google Docs, Google AI Platform ou BigQuery dans un cloud souverain.

- **Initiative Numspot (Dassault/Outscale + Docaposte + Bouygues + Banque Postale)** : Lancée fin 2022, **Numspot** est une alliance d'acteurs 100% français pour proposer un **PaaS/IaaS souverain mutualisé**. Elle s'appuie sur les infrastructures qualifiées SecNumCloud d'Outscale (Dassault)[62] et vise à fournir des services cloud intermédiaires (containers, OpenShift, bases de données, etc.) à un niveau de confiance élevé. Numspot a entamé sa propre démarche de qualification début 2024[63]. C'est une offre davantage orientée vers les entreprises et administrations qui cherchent une alternative française *clé en main*. Sa particularité : impliquer La Poste (via Docaposte) et la Banque Postale, qui apportent leur caution d'opérateurs de confiance publics.
- **Fournisseurs français historiques :** Parallèlement à ces nouveautés, les acteurs traditionnels comme **OVHcloud** et **Outscale** continuent d'étoffer leur catalogue souverain. OVHcloud propose par exemple son offre « SecNumCloud » de cloud public (VM, stockage objet, Kubernetes) déjà utilisée par certains ministères et récemment choisie par le Ministère de l'Éducation pour héberger la messagerie de 5 millions d'élèves[64]. De plus, des opérateurs sectoriels émergent : ainsi la DINUM (direction du numérique de l'État) a mis en place un **« Cloud Interne de l'État »** (appelé *Andromède*), qui est une plateforme privée pour certaines applications sensibles ne pouvant aller ni sur SecNumCloud (par manque de fonctionnalité) ni sur le legacy – par exemple pour développer des services communs interministériels.

Bilan et déploiement. Fin 2023, les solutions SecNumCloud "natives" (OVH, Outscale, etc.) sont utilisées sur quelques projets structurants, mais la plupart des grands chantiers (migration massive des messageries, des applications RH, etc.) sont en attente des plateformes Bleu et S3NS, dont la pleine disponibilité est prévue courant **2024-2025**[65] [66]. On assiste donc à une période transitoire où l'État prolonge certains contrats existants (par ex.

---

[62] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[63] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[64] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[65] https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[66] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

utilisation limitée d'Office 365 sur Azure France avec dérogation) en attendant de basculer vers Bleu une fois SecNumCloud obtenu. **À partir de 2025**, on anticipe un **essor rapide du cloud de confiance** : de nombreux ministères ont préparé des plannings de migration conditionnels (le Ministère de la Justice, par exemple, qui n'a pas déployé O365 attend Bleu pour le faire en conformité). Orange Business Services annonce de son côté migrer 70% de ses propres applications vers Bleu en 2025, ce qui servira de vitrine test. S3NS compte déjà des adopteurs pilotes (Matmut, Club Med, Thales lui-même) qui auront amorcé leur migration dès fin 2024 sur l'infrastructure pré-qualifée[67].

Comparaison canadienne : Le Canada n'a pas créé de joint-ventures spécifiques avec les Big Tech pour l'instant. Il continue d'utiliser les data centers canadiens d'Azure, AWS et GCP via les accords-cadres existants. Cependant, l'idée d'un **cloud souverain canadien** gagne du terrain. Fin 2022, le Conseil canadien des innovateurs (CCI) a recommandé de **« prioriser les infrastructures cloud souveraines »** dans le plan budgétaire fédéral[68]. En 2024, le gouvernement a annoncé un investissement de **2 milliards $CAN** pour augmenter la capacité nationale en calcul et en stockage – officiellement pour l'IA, mais qui comprend la construction de centres de données au Canada[69] [70]. En parallèle, des opérateurs privés canadiens se mobilisent : les télécoms **Bell** et **TELUS** ont investi dans de nouveaux data centers "souverains" en 2023[71], et le français **OVHcloud** a ouvert plusieurs sites au Canada en se positionnant comme fournisseur de cloud souverain au service du gouvernement (OVHcloud est d'ailleurs le seul non-nord-américain référencé sur le marché public canadien, et souligne stocker les données au Canada sous contrôle local)[72].

Il y a donc une **convergence France-Canada sur le constat** de dépendance aux géants étrangers, et une volonté commune (depuis 2024-2025) de renforcer les offres nationales/alternatives. Là où la France a créé des entités dédiées (Bleu, S3NS) et un label

---

[67] https://www.zdnet.fr/actualites/thales-et-google-visent-secnumcloud-pour-s3ns-a-lete-2025-394750.htm

[68] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[69] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[70] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[71] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[72] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

contraignant (SecNumCloud), le Canada pourrait plutôt s'appuyer sur ses champions nationaux (opérateurs télécoms, hébergeurs locaux) et sur des **partenariats internationaux**. Par exemple, en septembre 2023, le Royaume-Uni et le Canada ont signé un accord pour collaborer sur l'**accroissement de leur capacité de calcul souveraine** (IA compute), reconnaissant la nécessité d'unir leurs forces face aux hyperscalers[73] [74].

Initiatives Futures : France 2030, EUCS et Vision à Long Terme

Investissements France 2030. La France ne s'est pas arrêtée à la doctrine et aux partenariats. Dans le cadre du plan **France 2030**, une enveloppe spécifique est consacrée au cloud souverain et à l'**accélération du cloud**. En mars 2024, le gouvernement a ainsi lancé un **appel à projets « Renforcement de l'offre de services cloud »** doté de « plusieurs dizaines de millions d'euros » pour soutenir les solutions françaises et européennes innovantes en matière de cloud (par exemple de nouveaux services PaaS souverains, du cloud pour l'IA, etc.)[75] [76]. L'objectif affiché par la Secrétaire d'État au Numérique, Clara Chappaz, est de *« bâtir une offre de cloud européenne attractive, performante, compétitive »* et de consolider le secteur numérique européen face à la domination des acteurs étrangers[77]. Ce même jour (15 avril 2025), elle a annoncé la création d'un **Observatoire de la Souveraineté Numérique** chargé de mesurer la dépendance

---

[73] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B68C1E4B1-5F93-4BE9-99CC-09DA87960592%7D&file=Document%2033.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[74] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B68C1E4B1-5F93-4BE9-99CC-09DA87960592%7D&file=Document%2033.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[75] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

[76] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

[77] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

technologique de la France (cloud, composants, etc.) et de guider les politiques publiques pour la réduire[78].

Ces initiatives montrent que la France inscrit sa stratégie cloud dans un cadre plus large de **souveraineté numérique**, en lien avec d'autres sujets comme les composants (GPU), les services IA souverains (ex: LLM français comme Mistral AI)[79], etc. Le cloud est vu comme une brique d'infrastructure critique au même titre que l'énergie ou les transports. Sur ce point, la France rejoint la vision canadienne émergente en 2025 : le nouveau discours politique au Canada place le **« nuage souverain » parmi les projets nationaux stratégiques**, aux côtés des pipelines ou des ports[80]. Mark Carney, pressenti pour un rôle majeur au Canada, a même déclaré en 2025 que *"la souveraineté numérique et le cloud font partie de la construction de la nation, pour avoir le contrôle indépendant de notre puissance de calcul"*[81] [82]. Ottawa a ainsi lancé une **Stratégie pour l'infonuagique et l'IA souveraines** en 2024 avec 2 G$ pour financer des infrastructures de calcul sur le sol canadien[83]. On voit donc un alignement transatlantique sur l'importance cruciale du cloud souverain pour l'**avenir (IA, quantique, etc.)**.

Cadre européen (EUCS). Au niveau de l'Union européenne, la France milite pour généraliser sa démarche à l'échelle du continent. Un **schéma européen de certification cloud (EUCS)** est en cours d'élaboration par l'ENISA : la France, soutenue par l'Allemagne, défend l'intégration dans EUCS d'un **niveau « High / Souveraineté »** incluant des critères proches

[78] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

[79] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

[80] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[81] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[82] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[83] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

de SecNumCloud (localisation UE, pas de contrôle extra-UE)[84]. Ce débat a été vif car certains États membres et entreprises y voyaient un risque d'exclusion des hyperscalers non-européens. Fin 2022, un compromis semblait se dessiner pour qu'EUCS offre plusieurs niveaux d'assurance, dont un niveau maximal avec exigence de **capitaux et traitement 100% européens** – laissant aux États la possibilité d'exiger ce niveau pour leurs marchés publics sensibles[85]. **En 2024-2025, l'EUCS devrait être finalisé** et deviendra vraisemblablement la référence commune ; la France aura alors réussi à "européaniser" son label de confiance. Cela facilitera aussi les coopérations entre pays de l'UE : par exemple, l'Allemagne a un projet similaire (**Gaia-X**, cloud fédéré) et discute avec la France pour rendre interopérables et mutuellement reconnues leurs solutions. On peut imaginer à terme un écosystème européen où un service SecNumCloud français pourrait servir des clients publics allemands et vice versa, grâce à EUCS – répondant du même coup aux besoins d'échelle et de compétitivité.

Évolution à long terme. En France, un enjeu sera de **s'assurer que les offres de cloud de confiance soient attractives (en coût, en fonctionnalités)** face aux offres globales classiques. Les partenariats avec Microsoft et Google visent précisément à éviter un déclassement technologique : si Bleu et S3NS réussissent leur pari (certification + adoption), alors la France aura trouvé un modèle conciliant souveraineté et innovation internationale. Dans le cas contraire (si par ex. ces offres peinent à obtenir la certification ou à séduire des clients au-delà du secteur public), il pourrait y avoir des ajustements de stratégie. Néanmoins, la tendance est clairement lancée vers davantage de souveraineté. Le **marché européen du cloud souverain** est estimé en forte croissance, soutenu par les investissements publics (France 2030, programme Digital Europe de l'UE, etc.). D'ici 2027, on peut s'attendre à ce que la plupart des données sensibles des États européens soient hébergées sur des infrastructures labellisées **EUCS "High"** (donc souveraines), avec en parallèle l'utilisation de services cross-cloud pour des besoins moins critiques ou transfrontaliers.

Du côté du Canada, l'horizon 2025-2026 sera marqué par la concrétisation ou non de son **projet de "Cloud national"**. Si l'initiative reçoit un soutien politique fort (comme les propos

[84] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

[85] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

attribués à M. Carney le laissent penser)[86] [87], on pourrait voir émerger une **alliance canadienne** impliquant les grands fournisseurs nationaux (les télécoms Bell et Telus, peut-être des partenariats avec des européens comme OVHcloud ou des américains consentants comme IBM) pour bâtir un cloud fédéral certifié au Canada. Le Canada collaborera sans doute avec des pays alliés (Royaume-Uni, Union européenne) via des *Memorandums of Understanding* déjà signés sur l'IA compute[88] [89].

En définitive, **la France et le Canada étaient partis de positions différentes, mais convergent sur l'importance stratégique du cloud souverain**. La France, pionnière en la matière en Europe, a établi un cadre très contraignant mais qui commence à porter ses fruits (solutions en cours de déploiement en 2024-25). Le Canada, après une phase d'ouverture totale, ajuste son curseur pour mieux protéger sa souveraineté dès 2024 tout en conservant les atouts du cloud public (d'où le terme *"Cloud Smart"* désormais employé plutôt que *Cloud First*[90] [91]). Les deux pays devront continuer d'équilibrer **innovation, souveraineté et sécurité**. À court terme, la France aura son « cloud de confiance » opérationnel et le Canada s'appuiera probablement sur une approche mixte (**« souveraineté équilibrée »**) : utilisation de clouds étrangers sous conditions + montée en puissance de clouds nationaux.

---

[86] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[87] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/

[88] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B68C1E4B1-5F93-4BE9-99CC-09DA87960592%7D&file=Document%2033.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[89] https://floodready1-my.sharepoint.com/personal/jamie_floodready_ca/_layouts/15/Doc.aspx?sourcedoc=%7B68C1E4B1-5F93-4BE9-99CC-09DA87960592%7D&file=Document%2033.docx&action=default&mobileredirect=true&DefaultItemOpen=1

[90] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

[91] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html

Pour conclure, **le modèle français du GGCL (Guidelines for Government Cloud Use) adapté au contexte hexagonal se caractérise par une intransigeance sur la maîtrise des données et une intervention volontariste de l'État pour façonner le marché cloud**. Il s'inscrit dans une dynamique européenne plus large de **reconquête de la souveraineté numérique**, à laquelle le Canada prête de plus en plus attention. Cette approche combinant **régulation (SecNumCloud/EUCS)** et **coopération industrielle (Bleu, S3NS)** fait de la France un cas d'étude suivi de près par d'autres gouvernements cherchant à concilier cloud computing et autonomie stratégique. Les prochaines années diront dans quelle mesure ce pari est réussi, en France comme au Canada, face à l'évolution ultra-rapide des technologies et des risques numériques. [92] [93]

[92] https://www.solutions-numeriques.com/cloud-letat-lance-un-appel-a-projets-de-plusieurs-dizaines-de-millions-deuros-et-cree-un-observatoire-de-la-souverainete-numerique/

[93] https://thequantuminsider.com/2025/09/12/carney-pushes-for-sovereign-cloud-as-canada-navigates-quantum-future/