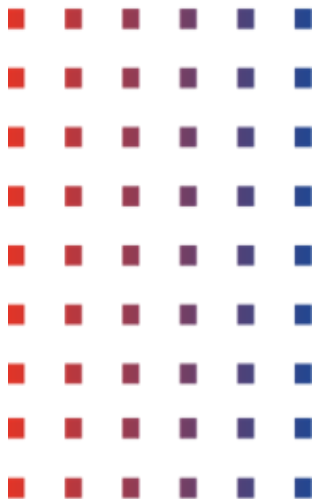




Direction Interministérielle du Numérique



Note de synthèse Audit Article 5

Sécurisation de la fin de migration du
projet GEOPORTAIL

VERSION V1.0 – 25/03/2020

1 Préambule

1.1 Rappel de l'ambition initiale de la migration du GEOPORTAIL et de la mission de sécurisation

Avec la fin du contrat d'hébergement et d'infogérance de l'application GEOPORTAIL¹ courant 2016, l'IGN a été confronté à l'impératif de changer son infrastructure², de préférence vers un environnement apportant des garanties de sécurité et de souplesse nécessaire pour faire face aux pics de sollicitation.

Pour cela, l'IGN, en coopération avec ses tutelles³, a fait le choix fin 2015 de l'offre de service d'hébergement de l'État OSHIMAE couplé au réseau optique à haut débit du RIE⁴. La société THALES Service ayant remporté l'accord cadre de développement, la TMA associée et l'infogérance du Géoportail en juillet 2017, elle est engagée sur un projet de migration sur ce nouvel environnement.

A l'issue de cette migration, l'objet était pour l'application GEOPORTAIL de bénéficier de :

- **l'élasticité de l'infrastructure d'un Cloud** et donc de la **capacité** à mieux **faire face** à la fois aux **pics de consommation et aux besoins croissants de l'application**,
- la **connexion sécurisée au Réseau interministériel de l'État (RIE)** pour servir les besoins des ministères et acteurs publics sans les risques liés aux usages de l'internet public.

En raison de difficultés rencontrées pendant la phase de construction du système et à l'issue de la migration, le Ministère de la Transition Ecologique et Solidaire et le Ministère de l'Agriculture, en accord avec l'IGN, ont saisi solidairement la DINUM pour mener un audit spécifique.

Les objectifs de cette mission de sécurisation ont été principalement :

- **d'analyser** les éventuelles causes structurelles des **difficultés rencontrées** pour tenir le niveau d'**engagement de service**,
- **d'apprécier la cohérence globale du système**, les capacités d'exploitation du système dans son ensemble tant en réponse à des incidents que dans le cadre d'opérations de maintenance programmées,
- **d'évaluer l'adéquation de l'hébergement OSHIMAE** avec le GEOPORTAIL d'aujourd'hui et avec le projet de GEOPLATEFORME⁵ de demain.

1.2 Le déroulement de la mission de sécurisation GEOPORTAIL

La mission de sécurisation du projet GEOPORTAIL s'est déroulée en trois phases :

Phase 1 – Cadrage visant à confirmer le périmètre de l'audit, affiner la compréhension des difficultés à analyser et à investiguer au travers d'entretiens stratégiques pour confirmer les axes d'analyse et les points de difficultés à creuser.

Phase 2 – Diagnostic ou « Revue 360° » permettant de couvrir les différentes dimensions du programme et notamment les points clés mentionnés dans la lettre de saisine⁶ et en se fondant sur :

- des entretiens complémentaires avec les acteurs majeurs du programme,
- l'analyse de l'importante documentation produite dans le cadre du projet.

¹ <https://www.geoportail.gouv.fr/> Le portail national de la connaissance du territoire

² Infrastructure propriétaire gérée par la société Worldline

³ Ministère de la Transition écologique et solidaire ; Ministère de l'Agriculture et de l'Alimentation

⁴ Réseau interministériel de l'Etat

⁵ Futur espace public de l'information géographique qui vise à optimiser la production et la diffusion des géodatas au service de la décision publique

⁶ Saisine commune MAA/MTES du 26 novembre 2019

Phase 3 –Recommandations de sécurisation visant à proposer un plan d’actions de sécurisation sur les **axes prioritaires identifiés** et à évaluer l’**adéquation** de l’offre d’hébergement **OSHIMAE** avec le projet **GEOPLATEFORME**.

2 Constats

Le premier constat d’ordre général montre un fort investissement de toutes les parties pour pouvoir opérer à ce jour le Geoportail migré dans l’offre OSHIMAE-RIE.

Pour autant, l’application GEOPORTAIL rencontre encore de nombreux problèmes d’exploitation qui nécessite :

- la sécurisation de l’exploitation réalisée par la société Thalès,
- la stabilisation de l’offre OSHIMAE/RIE portée par le MAA.

A décembre 2019, la finalisation de la migration passe, en particulier, par l’implémentation d’une solution de sauvegarde, la mise à niveau des différents environnements d’homologation, la livraison de la documentation technique et des services de sécurité.

La phase de diagnostic 360° a permis de dégager un ensemble de constats autour de 3 grandes thématiques :

1. La sécurisation de la fin de migration et l’exploitation GEOPORTAIL (IGN & Thalès)
2. L’adéquation de l’offre OSHIMAE/RIE pour les besoins GEOPORTAIL
3. Le cadrage de la future GEOPLATEFORME

Synthèse des constats par thématique:

1. La sécurisation de la fin de migration et l’exploitation GEOPORTAIL (IGN & Thalès)

L’étude de la documentation et les entretiens menés ont révélé une gouvernance IGN qui peine à jouer pleinement son rôle d’ensembliser entre OSHIMAE/RIE et Thalès dans un environnement complexe et multi-parties. A ce titre, l’organisation du projet sans pilotage centralisé et incarné n’est pas clairement définie avec une dilution des responsabilités. Ce projet vu comme un projet de migration technique n’embarque pas de MOA⁷ et les impacts utilisateurs sont donc subis. Enfin, les attentes notamment en termes de moyens sont insuffisamment décrites pour pouvoir piloter la relation contractuelle avec Thalès. Thalès, qui pour rappel, n’est pas seulement attributaire d’un subséquent pour la migration mais plus largement d’un marché cadre pour la maintenance et le développement ce qui influe la gestion du contrat de migration.

Concernant la planification, le reste à faire Thalès est à finaliser et les actions OSHIMAE à planifier.

Du point de vue technique, l’architecture GEOPORTAIL s’avère perfectible et pas assez « Cloud Ready⁸ ». Le niveau d’adhérence reste important entre l’ancienne infrastructure (opérée par Worldline) et la nouvelle infrastructure OSHIMAE (OpenStack).

L’infogérance ne répond toujours pas aux exigences de disponibilité et de performance attendues. Une rotation importante des équipes Thalès est observée ce qui ne favorise pas un niveau de capitalisation suffisant sur les problèmes rencontrés. De plus, le niveau de séniorité et la dispersion géographique des équipes en sont des facteurs aggravants.

2. L’adéquation de l’offre OSHIMAE/RIE pour les besoins GEOPORTAIL

L’offre OSHIMAE/RIE a été un choix collégial porté par toutes les parties (même si ce Cloud était en

⁷ La maîtrise d’ouvrage (MOA), aussi dénommée maître d’ouvrage est la personne pour qui est réalisé le projet

⁸ Une application native pour le cloud se compose de services plus petits, indépendants et faiblement couplés

cours de conception à ce moment). A l'origine, cette offre devait être co-portée entre le MAA et le MTES avec la mise en place d'une équipe commune et la mise à disposition d'une offre unifiée MAA/MTES répartie entre le site de Toulouse et celui de La Défense. Des divergences de vues ont finalement amené le MAA à porter opérationnellement cette offre durant les 18 derniers mois. Lors des premiers entretiens, le MTES a souhaité reconsolider ce partenariat s'appuyant sur un nouveau PIA⁹.

Aujourd'hui, OSHIMAE/RIE en tant que Cloud de l'Etat répond à des contraintes de ressources qui ne permettent pas de satisfaire pleinement aux exigences opérationnelles et professionnelles du GEOPORTAIL. En effet, des moyens humains internes capés conjugués à une expertise OpenStack, rare sur le marché, limitent les capacités d'OSHIMAE à répondre aux besoins croissants de GEOPORTAIL. Ajoutons que l'utilisation du RIE pour GEOPORTAIL est dévoyée puisque l'usage est essentiellement professionnel ou grand public. GEOPORTAIL représente 25 à 30% de la bande passante du RIE.

OSHIMAE reste une offre dont le niveau d'industrialisation reste à parfaire pour surmonter les difficultés opérationnelles persistantes et pour laquelle la pérennité des choix techniques est à questionner. En effet, OSHIMAE se base sur la distribution OpenStack HPE (que l'éditeur a annoncé début octobre ne plus maintenir) et dans une version 4 obsolète.

3. Le cadrage de la future GEOPLATEFORME

Le projet GEOPLATEFORME est structurant pour le projet d'établissement de l'IGN. A date, il est au stade conceptuel et mérite d'être approfondi techniquement pour mesurer l'adéquation entre OSHIMAE/RIE et les services Thalès afin d'accueillir la GEOPLATEFORME.

Le développement de l'Entrepôt V2 (modernisation de GEOPORTAIL) est un prérequis de la GEOPLATEFORME. A ce stade (mars 2020) le développement de cette brique est toujours suspendu en attendant une offre d'hébergement adaptée.

3 RECOMMANDATIONS

A la suite des différents ateliers de sécurisation, la DINUM formule une dizaine de recommandations regroupées en 4 catégories : prioritaire, majeure, essentielle et importante.

1. Prioritaires

1. Le pilote du projet GEOPORTAIL

L'IGN doit **recruter/sélectionner un directeur de projet ayant une expérience dans les projets complexes et les relations multipartites**. Sa tâche sera importante afin de fédérer les actions au sein des équipes de développement. Il instaurera une relation coordonnée avec le « métier » pour lequel il sera légitime.

Le directeur de projet est rattaché à la direction des sciences et technologies de l'information de l'IGN.

Actions associées :

- ▶ Redéfinir l'organisation GEOPORTAIL avec les rôles et les responsabilités de chacun.
- ▶ Mettre en place à minima un comité régulier de partage interne IGN.
- ▶ Partager les résultats lors des différents comités.
- ▶ Préparer les différents comités (Supports/CR).
- ▶ Valider le contenu des supports en amont des réunions dans le cas où leurs rédactions ont été déléguées au MAA ou à Thalès.

⁹ Programme d'Investissement d'Avenir

2. Une recherche d'infrastructure adaptée

L'IGN doit **s'assurer que les services d'hébergement et les services d'infogérance correspondent aux enjeux des utilisateurs du Géoportail et clients des géoservices.**

Même si le service d'hébergement OSHIMAE s'est amélioré depuis quelques mois, il reste « fragile » au regard de la maîtrise (notamment fonctionnelle) de la société Thalès. La **question d'un hébergement adapté se pose** aussi bien pour les besoins croissants du GEOPORTAIL que pour la future GEOPLATEFORME.

Les **besoins en termes de services, d'espaces de stockage** et de **puissance de calcul** sont considérables et devraient encore augmenter et les infrastructures de l'état **ne répondent pas à ce jour à ces besoins.**

Faute d'un accroissement notable des moyens et des ressources dans les prochains mois pour gérer les services du Cloud OSHIMAE, la mission préconise de ne pas développer les futurs modules de la GEOPLATEFORME sur cette cible.

Au regard des différentes options possibles, la **solution technique la plus raisonnable** serait de s'appuyer sur une infrastructure privée qui apporterait le niveau de service compatible avec les services professionnels et grand public de l'IGN.

Actions associées :

- ▶ Etablir une roadmap claire avec un planning et des actions précises de la montée de version Helion 5.
- ▶ Etudier les potentiels impacts d'une montée de version Openstack 4 à 5 avec Thalès et le MAA.
- ▶ Renforcer l'équipe d'exploitation OSHIMAE avec au minimum 2 profils Openstack.
- ▶ Mettre en place une connexion réseau internet additionnelle et s'assurer que les fournisseurs proposent un niveau de services ainsi que de sécurité au moins équivalent à celui du RIE, notamment en ce qui concerne les attaques DDOS (discussion en cours avec Orange).
- ▶ Faire de la résilience un sujet prioritaire en identifiant les moyens à mettre en œuvre à court terme (utilisation des 2 salles, mise en place de la résilience au niveau applicatif, LBS supplémentaires au niveau des bases de données...).
- ▶ Evaluer les limites de montée en charge de l'infrastructure OSHIMAE hébergeant l'application GEOPORTAIL, notamment à travers la réalisation de stress tests sur cette dernière.

▶ Majeures

3. Un soutien pour améliorer la vie du projet

Une **mission de soutien est préconisée** dès le mois de janvier 2020 pour 3 mois afin de **soutenir les équipes IGN** dans la mise en œuvre des actions découlant des recommandations afin de coordonner les acteurs et gérer les risques.

Actions associées :

- ▶ Renforcer les échanges avec les équipes OSHIMAE ;
- ▶ Aider les chefs de projets (TMA, Exploitation, nouveaux développement) pour obtenir de la société Thalès une prestation performante et conforme à ses engagements contractuels ;
- ▶ Sécuriser le reste à faire ;
- ▶ Conforter le planning ;
- ▶ Ajuster la proposition Entrepôt V2 ;

- ▶ Soutenir la direction des sciences et technologies de l'information et aider la direction générale lors des arbitrages.

4. Les décisions au bon niveau

Le **management de l'IGN** impliqué dans la mise en œuvre opérationnelle du projet doit retrouver **son niveau de responsabilité**. Le comité de niveau direction générale doit être réservé comme instance d'arbitrage pour les litiges majeurs.

5. Le nécessaire alignement de l'IGN avec le MAA

Dans une logique partenariale, l'IGN et le MAA doivent **s'aligner sur des positions communes** en amont des points avec la société Thalès.

Actions associées :

- ▶ Concevoir et partager les classes de services ainsi que leurs SLA de performance dans la convention OSHIMAE.
- ▶ Mettre en place un point hebdomadaire entre l'IGN (acteurs techniques) et le responsable produit MAA.
- ▶ Déclencher une première instance tripartite selon ce format pour traiter entre l'IGN, le MAA et la société Thalès les points de blocages liés à la sauvegarde (objet et fichier).

▶ Essentielles

6. La sécurisation du fonctionnement avec Thalès

Les points de **désaccord sur les écarts contractuels et la sécurisation de l'exploitation** avec la société Thalès **doivent être traités en priorité** pour **revenir à une situation** plus sereine avant d'enclencher la suite des travaux tels que l'Entrepôt V2 marche pied de la GEOPLATEFORME.

Actions associées :

- ▶ Partir du marché subséquent de migration et des livrables attendus pour définir la liste du reste à faire.
- ▶ Définir les contours d'une supervision fonctionnelle avec la société Thalès et élaborer le plan d'actions relatif à sa mise en place.
- ▶ Faire un inventaire complet de l'état actuel de la supervision technique afin d'identifier les manques impactant la remontée d'alertes et l'anticipation du traitement des incidents.
- ▶ S'aligner sur le périmètre contractuel de la supervision technique.

7. La gestion des écarts

Le pilotage de l'infogérance, la TMA et les futurs développements doivent être mieux challengés. Un **dispositif de gestion des écarts doit être mis en place**.

Les **propositions et engagements** de la société Thalès **doivent être mesurés** et suivis toutes les semaines avec la direction de projet Thalès (en collaboration avec la mission de soutien). Ce travail est consommateur mais devrait donner des résultats dès la fin du premier trimestre 2020.

8. Un système de sauvegarde performant

Le GEOPORTAIL et **ses données doivent être sauvegardés grâce à un dispositif adapté**. Cette action doit être menée dès janvier 2020. En cas de corruption, le système ne peut redémarrer dans un délai compatible avec une activité professionnelle.

Actions associées :

- ▶ Organiser des ateliers tripartites dédiés à la sauvegarde objet et la sauvegarde fichier.
- ▶ Elaborer la feuille de route des sauvegardes objet et fichier à la suite des ateliers.

9. Le futur projet Entrepôt V2

La **proposition Entrepôt V2 doit être revue** sous plusieurs angles afin de sécuriser le projet : détenir le planning, valider les prérequis, modifier la démarche, revoir les responsabilités et les engagements de recette applicative conditionnant la réception du développement.

Ce développement doit être adapté à sa future cible d'hébergement afin de ne pas multiplier les coûts d'investissement.

Actions associées :

- ▶ Organiser un point avec le MAA pour vérifier qu'il puisse répondre aux besoins techniques de l'IGN (si OSHIMAE retenu comme cible d'hébergement pour la Géoplateforme).
- ▶ Clarifier la phase de tests (périmètre, planning, types de tests, responsables) et estimer la charge induite ;
- ▶ Incorporer les documents mentionnés dans l'offre Thalès pour qu'elle soit autoporteuse ;
- ▶ Spécifier les réponses aux exigences.

10. La GEOPLATEFORME

La **GEOPLATEFORME est en phase de cadrage**. Elle doit fournir aux partenaires la possibilité de charger, co-produire et diffuser des données géographiques. Elle doit permettre également de fournir des services métiers sous forme d'API.

L'équipe interne affectée à ce projet n'est pas dimensionnée pour faire face aux futurs enjeux et le calendrier est incertain. La valeur délivrée est liée à des cas d'usage et ce projet doit être priorisé au sein de l'IGN comme stratégique.

Le **MAA devra se positionner sur sa capacité à répondre aux prérequis** de l'IGN pour lancer ce projet (en particulier l'allocation de nouvelles capacités).

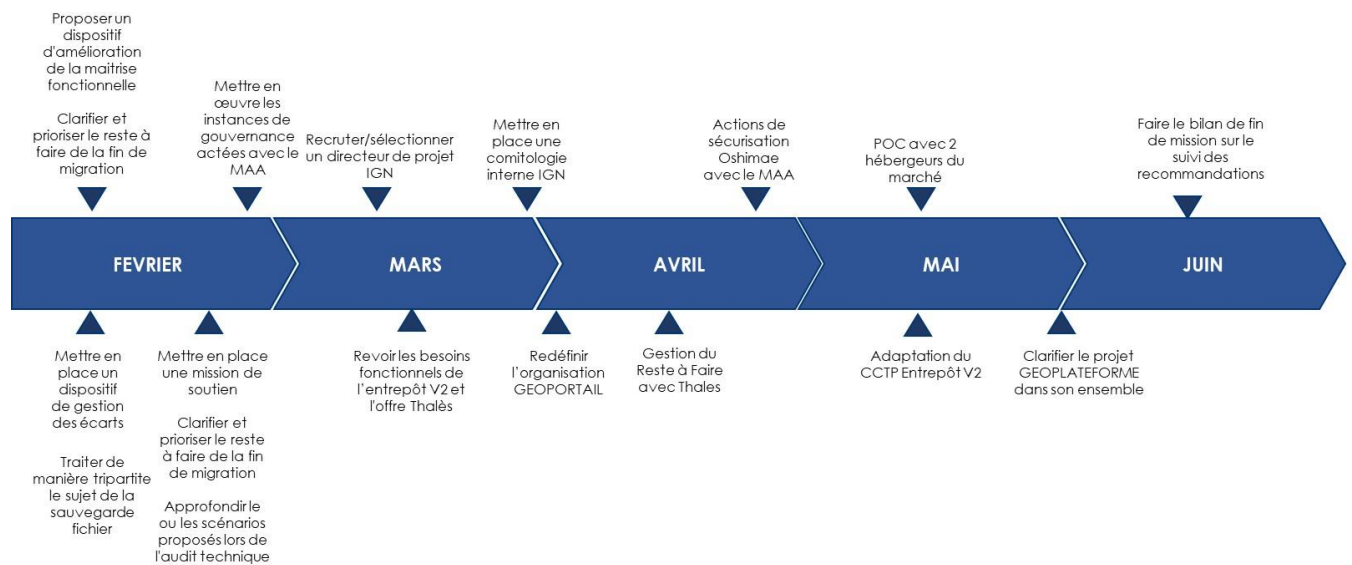
Le projet doit être encore travaillé avant d'être présenté dans le cadre d'un Article 3¹⁰.

Actions associées :

- Clarifier le projet GEOPLATEFORME dans son ensemble.
- Renforcer les ressources sur le projet GEOPLATEFORME.

¹⁰ Décret n°2019-1088 du 25 octobre 2019

4 Feuille de route



5 FOCUS SUR L'HEBERGEMENT

La mission a rencontré les acteurs majeurs de l'Etat et du secteur privé proposant des solutions d'hébergement. Sur la base de ces différentes rencontres, 4 scénarii ont été retenus pour être étudiés:

- **Scénario 1** : Le maintien du GEOPORTAIL / GEOPORTEFORME au sein du Cloud OSHIMAE :
 - Le maintien du GEOPORTAIL / GEOPORTEFORME au sein du Cloud OSHIMAE passe par 2 phases d'optimisation :
 - La prise en compte de 7 recommandations techniques prioritaires estimées entre 590 K€ HT et 720 K€
 - La mise en place d'un plan d'industrialisation / automatisation pour un budget prévisionnel estimé entre 1,24 M€ et 1,51M€ HT
 - Ces phases d'optimisation doivent être adossées à l'affectation de ressources (ETP) complémentaires au nombre de 4 minimum (profil : Openstack, exploitation, réseau)
 - Enfin, avec une infrastructure OSHIMAE sur une distribution OpenStack HP Helion qui ne sera plus maintenue à terme, il faut envisager un changement de socle technique (migration vers une autre distribution OpenStack ou une autre technologie (type VMWare). Ce changement de socle implique un investissement conséquent d'au-moins 5M€ prenant en compte les phases de test de non régression.
 - L'investissement prévisionnel total de ce scénario est compris entre 7,25 M€ et 7,75 M€ HT pour la période 2020-2021.
 - Une variante à ce scénario consisterait à étudier une convergence technique du socle Openstack vers une solution commune entre le MTES, le MAA (et le MEF).
- **Scénario 2** : Migration vers le Cloud NUBO (MEF)

- Une réunion de travail et d'échange avec le MEF a permis d'apprécier la nature et le niveau de maturité de l'offre. Récemment construite, l'offre demande encore à être consolidée pour accueillir une application de taille conséquente qui exige de hautes performances comme le GEOPORTAIL ou la GEOPLATEFORME
 - Même si cette offre est disponible, une étude préalable à l'hébergement est nécessaire pour identifier les impacts et adaptations nécessaires (étude estimée à 3 mois et 150 K€) aussi bien au niveau du Cloud NUBO qu'au niveau du GEOPORTAIL.
 - La disponibilité de cette offre n'est pas éprouvée à ce jour (peu d'applications en production).
 - Faute de retour d'expériences suffisants sur NUBO à ce stade, ce scénario n'est pas retenu car l'IGN ne peut se permettre d'investir une nouvelle fois dans la mise en œuvre et mise au point du GEOPORTAIL et de la GEOPLATEFORME dans un Cloud « neuf ».
 - Ce scénario n'est pas valorisé.
- **Scénario 3 : Offre Cercle 2**
- La disponibilité, la flexibilité et la richesse de l'offre sont supposées bonnes puisqu'elles devraient reposer sur un industriel spécialisé dans l'hébergement.
 - La date de mise à disposition prévisionnelle est courant 2021 (ou 2022).
 - Le positionnement Cercle 2 est envisageable pour la GEOPLATEFORME mais le délai de mise à disposition de cette offre n'est pas compatible avec les enjeux de planning actuels.
 - Ce scénario n'est pas valorisé.
- **Scénario 4 : Offre Cercle 3**
- La disponibilité, la flexibilité et la richesse de l'offre sont supposées bonnes puisqu'elles reposent sur un industriel spécialisé dans l'hébergement.
 - Cette offre est garantie sur 4 ans puisqu'elle se base sur le marché UGAP dont la notification est prévue en avril 2020 (offre disponible avant l'été 2020).
 - Le positionnement est envisageable pour la GEOPLATEFORME qui nécessitera de mettre en place une liaison RIE.
 - Sous réserve d'un accord sur les modalités de financement du scénario, pour vérifier la faisabilité technique et affiner les coûts de migration et de RUN, l'IGN lancera des Proof of Concept avec 2 fournisseurs (OVH et AWS) en collaboration avec un cabinet d'experts et son infogérant (à noter : opportunité de partir sur le fournisseur OVH pour se rapprocher à terme du Cloud Cercle 2 (si le POC mené par le MinArm est confirmé).
 - L'investissement prévisionnel total de ce scénario est compris entre 5,6 M€ et 6,1 M€ HT pour la période 2020-2021.

6 ADEQUATION ET ASPECTS FINANCIERS

Le tableau suivant affiche l'adéquation de l'offre pour la Géoplateforme suivant 4 critères (Disponibilité, Pérennité, Flexibilité, Richesse de l'offre d'hébergement cible)

	S1 : maintien au sein d'OSHIMAE		S2 : NUBO	S3 : Cercle 2	S4 : Cercle 3	
Disponibilité	++		++	++	++	
Pérennité	-		++	++	++	
Flexibilité	-		+	++	++	
Richesse	-		+	++	++	
Date de mise à disposition	Opérationnel		Janvier 2021	2021/2022	Juin 2020	
Budget 2020-2022 en M€ HT	OSHIMAE 5,7 à 6,2	IGN 1,55	Dates incompatibles		OSHIMAE 0,7 à 1,2	IGN 4,9
ETP par an (OSHIMAE) ou durant la phase projet (IGN)	4	5 à 7			4	5 à 7

7 CONCLUSIONS

Si l'hébergement OSHIMAE répond actuellement aux besoins d'exploitation du GEOPORTAIL, les travaux préliminaires de la GEOPATEFORME ont mis en exergue des exigences fortes en termes de disponibilité et de flexibilité qui ont demandé de réétudier l'adéquation du futur hébergement.

L'IGN doit recentrer son activité vers des travaux d'évolutions fonctionnels pour **répondre aux attentes de ses partenaires et maintenir son niveau de compétitivité** sur le marché de la donnée géographique. Les travaux techniques ne doivent plus être une « préoccupation ».

Au regard des besoins et des niveaux de maturité des offres étatiques ou publiques, les **offres industrielles du marché** sont à privilégier pour la GEOPATEFORME au travers du marché UGAP (actuellement, seule l'offre Cercle 3 sera disponible en juin 2020). L'investissement prévisionnel total du **scénario migration vers un « Cloud Public » est compris entre 5,6 M€ et 6,1 M€ HT** pour la période 2020-2021. Un renfort en ETP est nécessaire pour d'une part, migrer les services GEOPORTAIL et amorcer la dynamique GEOPATEFORME et, d'autre part, exploiter OSHIMAE.

Dans l'hypothèse où le **scénario « maintien sur OSHIMAE »** serait retenu, l'investissement prévisionnel total **est compris entre 7,25 M€ et 7,75 M€ HT** pour la période 2020-2021. Un renfort en ETP sera également nécessaire pour d'une part, migrer les services GEOPORTAIL sur le nouveau socle OSHIMAE et amorcer la dynamique GEOPATEFORME et, d'autre part, exploiter OSHIMAE.