MINISTERE
DES GRANDS TRAVAUX,
DE L'EQUIPEMENT,
en charge des transports aériens,
terrestres et maritimes

DIRECTION POLYNESIENNE
DES AFFAIRES MARITIMES

DIRECTION POLYNESIENNE
DES AFFAIRES MARITIMES

MARCHE PUBLIC

CAHIER DES CHARGES TECHNIQUES

CONSULTATION TELESERVICE n° 2023-01-MGT-DPAM

Analyse des risques du téléservice et audit technique REVATUA

SOMMAIRE

INFORMATIONS GENERALES

1.1 CATEGORIE A LAQUELLE APPARTIENT L'ACHETEUR PUBLIC

La Polynésie française.

1.2 MAITRISE D'OUVRAGE

Le maître d'ouvrage est la Direction Polynésienne des Affaires Maritimes, représentée par sa Directrice, Madame Catherine ROCHETEAU.

1.3 CATEGORIE DE MARCHE

Marché public de prestation de services.

1.4 LIEU D'EXECUTION.

Papeete, Tahiti, Polynésie française

1.5 PROCEDURE DE PASSATION.

Le présent marché est un marché dispensé de procédure de publicité et de mise en concurrence, conformément à l'article LP. 223-3 -1° du Code polynésien des marchés publics.

1.6 ÉLEMENTS D'INFORMATION UTILES CONCERNANT LES PROJETS DU MARCHE

L'objectif du Pays est de pouvoir dématérialiser à moyen terme 70% des démarches de ses usagers. La DPAM s'est inscrite pleinement dans cet objectif en lançant dès 2019 le téléservice « REVATUA » de gestion des connaissements maritimes et des documents obligatoires dans le cadre du transport maritime intérieur.
Depuis novembre 2018, tout téléservice mis en production doit faire l'objet d'une homologation préalable conformément à la Loi du Pays n° 2017-30 du 2 novembre 2017 et à son arrêté d'application n° 2043 CM du 18 octobre 2018.
Les prestations faisant l'objet du marché consistent donc à accompagner la DPAM dans la démarche d'homologation de sécurité de la suite du développement de REVATUA, notamment son module avec la Direction Générale des Affaires Economiques (DGAE) tels que décrit au chapitre suivant.

1.6.1 REVATUA

Le transport maritime intérieur est une activité importante et essentielle pour la population et l'économie polynésiennes. En effet, les 76 îles habitées sont approvisionnées par une desserte maritime. L'essentiel du flux se fait de l'international vers Tahiti, puis les marchandises sont redistribuées de Tahiti vers les autres îles.

Les importations représentant l'essentiel de l'approvisionnement de la Polynésie française, les importateurs et les commerçants envoient ensuite les marchandises dans les îles. C'est aussi le cas des activités de production ou de transformation.

Les populations ont aussi besoin de transport intérieur, pour des échanges familiaux, déménagements, approvisionnements.

Le transport de marchandises repose sur un contrat, passé entre l'armateur (celui qui transporte la marchandise) et le chargeur (celui qui veut faire transporter sa marchandise). Ce contrat est matérialisé par un connaissement.

Il est établi en plusieurs exemplaires, jusqu'à 7 en fonction des besoins. Le volume annuel est d'environ 1 000 000 de connaissements, sous format papier. 80% du nombre de connaissements est produit par des particuliers et représente 20% du volume des marchandises transportées.

A contrario, 20% du nombre de connaissements est produit par des professionnels et ils représentent 80% du volume des marchandises transportées.

Le gouvernement de la Polynésie française prend en charge les coûts de transport pour certaines marchandises et mène aussi des politiques publiques d'aides au transport pour les échanges entres îles afin de favoriser par exemple l'agriculture locale.

En 2020, la DPAM a mis en service « REVATUA », le téléservice de dématérialisation des plannings des navires, complété par la dématérialisation des connaissements en janvier 2021. Le téléservice REVATUA a déjà été homologué 2 fois.

1.6.1.1 FINALITES ET MISSIONS

1.6.1.1.1 LES OBJECTIFS DU TELESERVICE

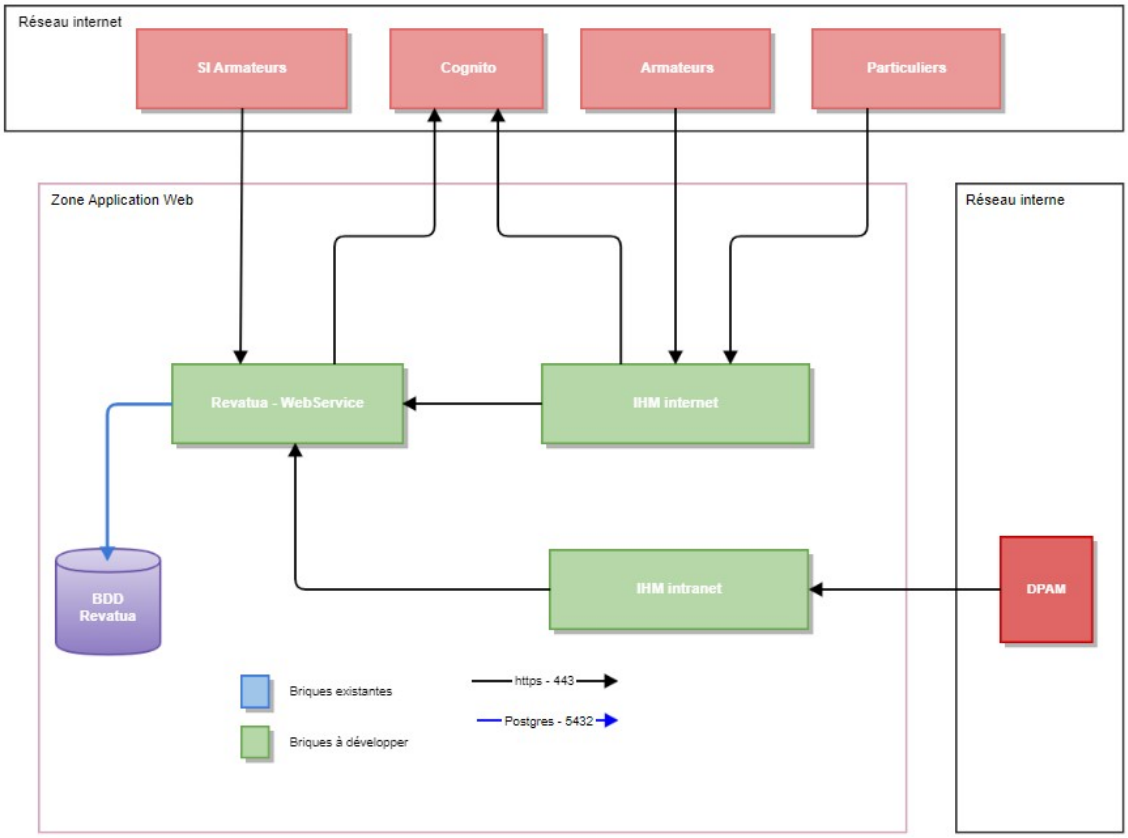
L'objectif principal est de permettre la mise en œuvre de la dématérialisation dans le cadre du transport maritime intérieur, Polynésie française du téléservice « REVATUA » :

- Qui s'adressera à une population cible élargie (particuliers ou professionnels souhaitant envoyer un colis et établir un connaissement) ;
- Qui apportera plusieurs fonctionnalités :
    - Planning des voyages des navires ;
    - Saisie de formulaires dématérialisés pour :
        - La création de voyages ;
        - La saisie de connaissements ;
        - La saisie des états de passages ;
    - Statistiques avec Power BI ;
    - Signature électronique des connaissements / manifestes ;
    - Téléversement des listes d'équipages et des mouvements de navires et des documents de la DGAE ;
    - Voire l'état des remboursements réalisés par la DGAE.
- Qui améliorera et digitalisera l'existant tant pour les utilisateurs externes qu'internes (ergonomie, fonctionnalités) ;

- Qui améliorera la sécurité du territoire grâce à une meilleure connaissance des voyages et des produits.

1.6.1.2 MODULES ET FONCTIONNALITES

1.6.1.2.1 MODULES



1.6.1.2.2 PARTIES PRENANTES ET FONCTIONNALITES

Parties prenantes REVATUA	**Rôles REVATUA**
DPAM	Maîtrise d'ouvrage
DSI	Développement, hébergement
IDT	Développement
Agent DPAM	Utilisation du Back-Office pour : Contrôler les voyages Contrôler les manifestes Contrôler les inscriptions Contrôler les documents téléversés Administrer
Agent DGAE	Traiter les remboursements des connaissements éligibles

	Administrer les tarifs de remboursements Suivre l'historique des remboursements
Utilisateurs externes	Armateur : Saisir les voyages Créer et gérer des connaissements Gérer les demandes de connaissements chargeur Voir les états de remboursement DGAE Gérer la société et les membres Créer et gérer les états de passages Chargeur professionnel : Créer et suivre les connaissements Gérer la société et les membres Chargeur particulier : Créer et suivre les connaissements

1.6.1.2.3 TECHNOLOGIES

Sujet	**Choix**
Service API REST (Serveur HTTP)	ASP.net
Application IHM Téléservice	Angular14 / JAVA8
Base de données	PostgreSQL
Application DPAM / DGAE	JAVA8 / ANGULAR10
Envoi du courriel	DSI
Hébergement	DSI
Authentification	Keycloack et Cognito

1.6.1.2.4 DESCRIPTION DES NOUVELLES API ET DU NOUVEAU MODULE DGAE A HOMOLOGUER

Objectif de mise à disposition des API GET pour les armateurs :

- Liste des remboursements : en attente / accepte / refusé / en attente de document complémentaire
- Téléversement des documents complémentaires

Agent DGAE :

- Se connecter au BACKOFFICE DPAM via son LDAP
- Traiter les remboursements des connaissements éligibles
    - Rembourse et génère un document pour la DBF
    - Rejet et génère un document pour l'armateur
    - Demande et traite des documents complémentaires
- Administrer les tarifs de remboursements
- Suivre l'historique des remboursements

2. DESCRIPTION DES PRESTATIONS DEMANDEES

Le marché comporte une tranche ferme et une tranche conditionnelle qui ne peuvent être attribuées qu'au même prestataire.

La tranche ferme est composée de 2 phases distinctes :

Phase 1 : L'analyse des risques

Phase 2 : Les tests d'intrusion

La tranche conditionnelle est composée d'une phase :

Phase 3 : Le contre-audit

Si le test d'intrusion révèle des vulnérabilités, des corrections devront être réalisées. Leur implémentation devra être vérifiée lors d'un contre-audit qui rejouera uniquement les scenarii de tests à l'origine de ces vulnérabilités.

2.1 AU TITRE DE LA TRANCHE FERME

2.1.1 L'ANALYSE DE RISQUES

La mission consiste à étudier les risques du téléservice REVATUA sur le nouveau module DGAE. Conformément au guide d'homologation en neuf étapes (Guide homologation), il est recommandé d'homologuer séparément la plateforme technique, en étudiant les risques qui lui sont propres et qui impactent potentiellement tous les services applicatifs qu'elle héberge.
Dans le contexte de ces deux téléservices, la démarche d'étude consiste donc à découper le périmètre d'étude comme suit :

A. Risques du téléservice REVATUA en propre sur le module DGAE

A ce titre il est attendu :

1. La réalisation d'analyses des risques en suivant la réglementation * ;
2. La documentation d'un dossier d'homologation ;
3. Une synthèse des travaux d'homologation dans un livrable final qui sera présenté à la commission d'homologation pour avis

**Ces analyses devront se conformer à la Loi de Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices et son arrêté d'application n°2043 CM du 18 octobre 2018. en complément elles pourront s'appuyer sur les guides, outils et recommandations de l'ANSSI en matière d'homologation de sécurité.*

Activités à réaliser au titre d'une analyse des risques

- L'animation de la réunion de cadrage en présence du RSSI
    - Documents attendus, planning prévisionnel
    - Identifier les parties prenantes
    - Définir le périmètre à homologuer en cohérence avec la vision du RSSI

- La définition avec le métier des objectifs de sécurité en termes de :
    - La disponibilité
    - L'intégrité
    - La confidentialité
    - La traçabilité
    - Auxquels s'ajoute l'authentification (tel que défini dans le RGS)

- Un travail de capitalisation sur :
  - Les documents fournis par la DPAM (techniques, fonctionnels, organisationnels)
  - Les risques et principales menaces du domaine
  - Les analyses de risques déjà menées par la DPAM

- L'identification des risques en suivant la réglementation métier et la loi de pays 2017-30 :
  - Conduite d'entretiens avec les parties prenantes (préparés au préalable avec envoi d'un questionnaire et planification de l'atelier plusieurs jours à l'avance)
  - Propositions d'événements redoutés, biens supports, sources de menace, niveau d'exposition et état de la menace cyber du domaine.
  - Production du plan de traitement proposé, soumis à validation du client et de la RSSI

- L'évaluation finale des risques tenant compte des résultats des audits d'intrusion menés

- La rédaction, tout au long de la prestation, du dossier d'homologation associé (format type Word)

- La rédaction en fin de prestation d'une présentation synthétique des conclusions de l'analyse (format type Power Point)

- La présentation des conclusions à la commission d'homologation en tant qu'expert en sécurité des systèmes d'information

La méthode d'analyse des risques est liée aux enjeux de sécurité. Elle est relative à la profondeur de la démarche qui est précisée en Annexe - Profondeur de la démarche d'analyse des risques de sécurité

Les référentiels :

L'approche « par conformité » :

L'approche par conformité vérifiera le niveau de risques vis-à-vis de la conformité aux référentiels de sécurité suivants :

- Le Référentiel Général de sécurité
- Guide d'hygiène informatique (ANSSI)
- La charte informatique
- La PSSI

Le Référentiel Général de Sécurité de Polynésie rendu opposable par l'arrêté d'application 2043 CM de la Loi de pays 2017-30 est le référentiel de conformité promulgué au titre de l'homologation (RGS).

La PSSI du Pays est en cours d'élaboration, à sa sortie elle devra être prise en compte comme référentiel de conformité pour les mesures existantes et les recommandations de sécurité.

Référentiels de mesures auxquels La Direction du système d'information de la Polynésie française (DSI) se réfère :

- Recommandations de l'OWASP Project
- Guides de l'ANSSI
- Guides de durcissement type CIS benchmark
- Annexe A ISO 27002
- ISO 20 000

Lorsque les mesures de sécurité sont issues de l'un de ces référentiels, le prestataire devra citer leur référence.

Référentiels de risques :

- Risques ou scenarii stratégiques construits à partir des sources de risques et objectifs visés de la méthode (EBIOS, ...)
- Et risques typiques d'un service web : Top Ten OWASP

2.1.2 AUDIT TECHNIQUE : TEST D'INTRUSION

Le téléservice REVATUA sera exposé sur Internet à destination des usagers.
Afin de tester sa résilience vis-à-vis des cyberattaques et évaluer la qualité de son implémentation (code et plateforme d'hébégerment), il doit faire l'objet d'un test d'intrusion externe.

Les deux tests d'intrusion souhaités seront conduits en mode :
- Boite noire (sans accès, source de menace externe),
- Boite grise (tests authentifiés, source de menace interne ou utilisateur, vérification du cloisonnement)

Ils suivront les recommandations suivantes :
- Ils sont conduits sur un environnement de pré-production, sans données de production
- En contournant le dispositif de filtrage applicatif en amont du téléservice afin de tester la résilience des développements,

Néanmoins certains scenarii pourront être joués sans le WAF puis avec, pour évaluer l'apport de ces dispositifs et mesurer le niveau de sécurité « brut » et « net ». Cela concerne les scenarii pour lesquels les vulnérabilités identifiées pourraient être bloquées par le WAF (signature d'attaque connue, ex : Injection SQL). Le WAF étant un composant mutualisé chaque scenario d'attaque transitant par ce dernier devra être explicitaement validé par la RSSI.

- Scenarii de test : rechercher en priorité les vulnérabilités du Top 10 de l'OWASP
- Les évènements redoutés issus de l'analyse des risques guident la rédaction des scénarii stratégiques de test :

Les évènements redoutés de l'analyse des risques REVATUA alimenteront le pentest REVATUA.

- Recommandations sur les corrections : PSSI, OWASP testing Guide, Guide Hygiène ANSSI, Référentiel Général de Sécurité, ISO 27 002
- Le Client valide les scenarii et comptes faisant l'objet des tests par signature d'une fiche d'autorisation d'audit

La documentation de référence attendue à minima est la suivante:

- Méthodologie de test : rechercher en priorité les vulnérabiltiés du Top 10 de l'OWASP et se focaliser sur les évènements redoutés issus de l'analyse des risques
- Recommandations sur les correction : OWASP testing Guide, Guide Hygiène ANSSI, Référentiel Général de Sécurité (et dans une moindre mesure RGI, RGAA).

Données fournies par la DPAM et la DSI lors de la réunion de lancement:

- Plages horaires des tests
- Matrice des rôles
- Contact technique en cas de problème sur l'application,
- Contact du RSSI de la DSI

La réunion de lancement permettra d'identifier les profils pertinents pour réaliser les tests authentifiés (boite grise).
Dans sa réponse, le prestataire estimera le nombre de comptes et de profils de tests inclus, sa méthodologie pour évaluer les vulnérabilités déctectées et sa documentation de référence.

S'agissant d'un audit d'intrusion, il n'y a pas à proprement dit d'obligation de certification PASSI (ANSSI) mais si les pentesteurs sont certifiés PASSI, c'est un plus. Dans le cas contraire, le prestataire doit fournir les références et l'expérience des auditeurs pressentis.

2.2 AU TITRE DE LA TRANCHE CONDITIONNELLE : LE CONTRE-AUDIT

Si le test d'intrusion révèle des vulnérabilités, des corrections devront être réalisées. Leur implémentation devra être vérifiée lors d'un contre-audit qui rejouera uniquemement les scenarii de tests à l'origine de ces vulnérabilités.

3. METHODOLOGIE

La Direction du système d'information (DSI) fournira à minima les documents suivants au prestataire :
- Dossier d'architecture technique
- Dossier de spécifications fonctionnelles, story maps, user story ou abuser story
- La liste des risques du projet
- L'ensemble des documents contractuels spécifiques au projet.

3.1 DEROULEMENT

- Les entretiens avec les parties prenantes ne doivent pas dépasser 1h30
- Ils doivent être réalisés en présentiel dans les locaux de la DPAM ou de la DSI afin de faciliter la participation des agents. Une visioconférence peut être proposée en cas de contact à risque ou autre cas spécifique validé par le référent métier.
- Les livrables intermédiaires doivent être simplifiés au maximum pour se concentrer sur l'essentiel

3.2 PROFONDEUR DE LA DEMARCHE D'ANALYSE

REVATUA est développé en méthode agile. Néanmoins les risques n'ont pas fait l'objet de formalisation d'abuser story. La méthode d'analyse de risque sera traditionnelle comme pour un projet en cycle en V.

La profondeur de la démarche a été qualifiée au travers d'une grille fournie en ANNEXE Profondeur de la démarche. La démarche sera d'un niveau avancé sans nécessité de recourir à un prestataire certifié.

Le prestataire s'organisera pour mutualiser les ateliers techniques relatifs aux bien supports et mesures existantes afin d'optimiser la prestation. Il pourra compter sur le chef de projet DSI, ressource dédiée à ces deux projets, pour organiser la prestation en lien avec les équipes de la DPAM et fournir la documentation.

3.3 PLANNING

La cible d'ouverture du nouveau module du téléservice REVATUA est janvier 2024.
Dans le cadre de la Tranche ferme :

Phase 1 : L'analyse des risques
Idéalement la prestation doit se dérouler de manière à permettre une mise en service du volet DGAE début janvier 2024, aussi les prestations devront être exécutées entre mi-septembre et fin décembre 2023.

Phase 2 : Les tests d'intrusion
L'analyse des risques débutera avant les tests d'intrusion. En effet, les phases d'élaboration du contexte, de la collecte des enjeux, des besoins de sécurité, des biens essentiels et des évènements redoutés permettront d'orienter les tests d'intrusion en imaginant des scenarii d'attaques correspondants aux principaux évènement redoutés du métier.

3.4 PREREQUIS DE LA PRESTATION

Compétences humaines attendues :

- Pédagogie, capacité en sensibiliser les parties prenantes et à susciter l'adhésion de tous à la démarche
- Capacité d'adaptation à l'auditoire et capacité à parler de la sécurité en termes simples et évocateurs (éviter les acronymes et les termes informatiques complexes, se rapprocher d'exemples métiers concrets).
- Capacité à créer un lien fort avec le métier :

- Réaliser les réunions en présentiel (sauf cas à risque au niveau du Covid19)
- Maintenir des échanges réguliers complémentaires par téléphone pour appréhender les freins et les obstacles indicibles.
- S'assurer que la direction métier est au fait de la démarche en l'intégrant dans les transmissions de livrables (à minima).

3.5 COMPETENCES PROFESSIONNELLES ATTENDUES

La DSI fournira :

Au titre de l'analyse des risques :

- Les échelles de gestion des risques (impact, vraisemblance, besoins de sécurité)
- Précédents travaux équivalents d'identification des risques
- La liste des risques du projet
- L'outil à utiliser pour réaliser l'analyse des risques
- La PSSI de l'administration, le cas échéant les règles à respecter
- La charte informatique

Au titre du projet :

- Dossier de spécifications fonctionnelles
- Dossier d'architecture technique complet
- Les rôles de chaque partie prenante et les contacts projet

Les compétences professionnelles attendues sont :

- Capacité de synthèse pour simplifier le travail des parties prenantes lors des ateliers.
- Connaissance des enjeux de l'administration et du domaine métier en particulier
- Bonne connaissance de l'actualité de l'écosystème cybersécurité en général et de l'actualité des menaces pesant sur les collectivités territoriales et les administrations.
- La méthode d'analyse des risques est liée aux les enjeux de sécurité. Elle est relative à la profondeur de la démarche qui est précisée en ANNEXE Profondeur de la démarche

3.6 LIVRABLES

Les livrables attendus au titre de la prestation sont liés aux les enjeux de sécurité. Ils sont relatifs à la profondeur de la démarche qui est précisée en Annexe 2 – Profondeur de la démarche.

Les livrables attendus sont :

- Comptes rendus des ateliers
- Rapports intermédiaires d'analyse dont la définition des objectifs de sécurité du projet
- Dossier d'homologation (à fournir 7 jours avant la réunion de commission d'homologation)
- Présentation de synthèse des travaux devant la commission d'homologation incluant les résultats du ou des audits d'intrusion menés

- Un état de la conformité au Règlement Général de Sécurité : pour les 4 fonctions de sécurité ciblés dans le RGS (authentification, signature électronique, confidentialité, et horodatage) le prestataire détaillera l'implémentation de la fonction de sécurité en fonction des besoins de sécurité.

- Liste synthétique du plan d'action recommandé

Les outils à utiliser sont les suivants :

- Confluence pour la consultation de la documentation existante
- Livrables déposés sur un canal/sharepoint microsoft
- Teams pour la visio conférence

3.7 **OFFRE**

Le candidat doit émettre une proposition avant le Lundi 19/06/2023 à 11h (heure de Tahiti) contenant :

- Une offre technique et financière pour la tranche ferme et pour la tranche conditionnelle.

Cette proposition devra comprendre :

- L'organisation de la prestation et le planning envisagé ;
- Le CV des intervenants et expérience dans des prestations similaires ;
- Les éventuelles certifications de sécurité des intervenants (EBIOS, ISO 27005…) ;
- Le plan de charge des intervenants sur les 6 prochains mois ;
- Description de la méthodologie envisagée pour l'analyse des risques.

L'offre financière devra préciser le prix hors taxe détaillé pour chacune des 3 phases de prestations.

Pour toute question sur l'aspect sécurité, merci de se rapprocher de Emmanuel BOUNIOT : emmanuel.bouniot@administration.gov.pf ; pour les questions sur la consultation: orama.lehartel@administration.gov.pf

ANNEXE 1 – EVALUATION DES ENJEUX

Thème	1	2	3	4	Notes	Max
Gravité des conséquences potentielles	**Question n° 1 :** Votre système est-il important pour remplir vos missions ?				3	3
	Non, le système est accessoire à l'accomplissement des missions	Oui, les missions seraient fortement perturbées par un dysfonctionnement du SI.	Oui, les missions dépendent totalement du SI	Je ne sais pas		
	Question n° 2 : Si un sinistre atteint votre SI, causant un dysfonctionnement ou une perte de données, les conséquences en interne (pour vos services) seraient-elles graves ? *Exemple : une panne électrique ne permet pas d'utiliser le système, le contenu d'une base de données a été supprimé, etc.*				3	
	Non, les conséquences internes d'un sinistre seraient négligeables	Oui, les conséquences internes d'un sinistre seraient significatives	Oui, les conséquences internes d'un sinistre seraient graves, voire fatales	Je ne sais pas		
	Question n° 3 : Si un sinistre touche la sécurité de votre système (il ne fonctionne plus ou pas bien, vol d'informations…), les conséquences pour l'extérieur (pour vos usagers, administrés…) seraient-elles graves ?				3	
	Non, les conséquences d'un sinistre pour l'extérieur seraient négligeables	Oui, les conséquences d'un sinistre pour l'extérieur seraient significatives	Oui, les conséquences d'un sinistre pour l'extérieur seraient graves, voire fatales	Je ne sais pas		
Thème	**1**	**2**	**3**	**4**	**Note**	**Max.**
Sensibilité des données du système	**Question n° 4** : Le fait que les données de votre système soient inaccessibles est-il grave ? Exemple : vous ne pouvez pas accéder aux données en raison d'une panne matérielle.				2	3
	Non, le fait qu'il ne soit pas accessible ne gêne quasiment pas l'activité	Oui, le fait qu'il ne soit pas accessible perturbera l'activité de manière significative	Oui, le fait qu'il ne soit pas accessible peut être fatal pour l'activité	Je ne sais pas		
	Question n° 5 : Le fait que les données de votre système soient altérées est-il grave ? Exemple : un virus a modifié des valeurs dans une base de données, les remettant toutes à 0.				3	
	Non, le fait que les données soient altérées ne gêne quasiment pas l'activité	Oui, le fait que les données soient altérées perturbera l'activité de manière significative	Oui, le fait que les données soient altérées peut être fatal pour l'activité	Je ne sais pas		
	Question n° 6 : Le fait que les données de votre système ne soient pas ou plus confidentielles est-il grave ? Exemple : la liste des bénéficiaires du service social est dévoilée.				3	

	Non, le défaut de confidentialité ne gêne quasiment pas l'activité	Oui, le défaut de confidentialité perturbera l'activité de manière significative	Oui, le défaut de confidentialité peut être fatal pour l'activité	Je ne sais pas		

Thème	1	2	3	4	Note	Max
Base d'estimation des potentiels d'attaques cyber	**Question n° 7** : Quel est le niveau de compétence maximal présumé de l'attaquant ou du groupe d'attaquants susceptibles de porter atteinte au système ?					3
	Individu isolé de niveau de compétence élémentaire	Individu isolé de niveau de compétence avancé	Groupe d'individus organisés, de niveaux individuels de compétence faibles à moyens, ou individu isolé aux compétences expertes	Groupe d'individus experts, organisés, aux moyens quasi illimités	3	
	Question n° 8 : Quelle est la précision des attaques potentielles envers le SI ?					
	Attaques « au hasard » sur le cyberespace	Attaques orientées vers le la Polynésie française	Attaques ciblant un groupe de victimes présentant des caractéristiques communes	Attaques visant précisément le système	3	
	Question n° 9 : Quel est le niveau de sophistication des attaques potentielles contre le SI ?					
	Outils d'attaque triviaux (logiciel de scan de ports, virus connus, etc.)	Outils élaborés génériques prêts à l'emploi (réseaux de botnet loués, faille connue, etc.)	Outils sophistiqués, adaptés pour le SI (zéro-Day, etc.)	Boîte à outils très hautement sophistiquée.	2	
	Question n° 10 : Quelle est la visibilité des attaques potentielles contre le SI ?					
	Attaque annoncée (revendications « d'hacktivistes », rançon, etc.)	Attaque constatée immédiatement par ses effets sur le SI	Attaque discrète, qui laisse des traces dans les journaux d'événements, mais ne perturbe pas le fonctionnement du SI	Attaque invisible, réalisée en laissant le minimum de traces	2	
	Question n° 11 : Quelles sont la fréquence et la persistance des attaques potentielles contre le SI ?					

	Unique : l'attaque ne se produit sur la cible qu'une seule fois	Ponctuelle : l'attaque survient plusieurs fois sans régularité dans sa fréquence (elle peut être liée à l'actualité).	Récurrente : Attaques par vagues successives importantes	Permanente	2	
Thème	**1**	**2**	**3**	**4**	**Note**	**Max**
Exposition et vulnérabilités	**Question n° 12** : Quel est le niveau d'hétérogénéité du système ? Exemple : plusieurs logiciels, matériels ou réseaux différents pour un même système.				2	3
	Le système est jugé comme homogène	Le système est jugé comme faiblement hétérogène	Le système est jugé comme fortement hétérogène	Je ne sais pas		
	Question n° 13 : Quel est le degré d'ouverture/interconnexion du système ? *Exemple : Internet, un autre système interne ou externe (celui d'un prestataire, d'une autre autorité administrative…) …*				3	
	Le SI n'est pas ouvert	Le SI n'est ouvert qu'à des systèmes internes maîtrisés	Le système est ouvert à des systèmes internes non maîtrisés ou externes (Internet)	Je ne sais pas		
	Question n° 14 : Le contexte dans lequel se trouve le SI et ses composants (matériels, logiciels, réseaux) évolue-t-il régulièrement ?				1	
	Le SI et son contexte sont jugés stables	Le SI et son contexte changent souvent	Le SI et son contexte évoluent en permanence	Je ne sais pas		
	Question n° 15 : Les composants du SI sont-ils mis régulièrement à jour ?				3	
	Les composants du SI sont tous tenus à jour en permanence	Une partie des composants du SI est régulièrement mise à jour	Les mises à jour sont effectuées de manière irrégulière	Je ne sais pas		
					Total des quatre valeurs maximales	**12**

ANNEXE 2 – PROFONDEUR DE LA DEMARCHE D'ANALYSE

Avec les résultats du questionnaire ci-dessus, on estime le besoin de sécurité du Service et la profondeur de la démarche à "Avancée".

Somme des quatre valeurs de la colonne Max.	Autre critère	Besoin de sécurité du système	Démarche d'analyse de risques
De 4 à 6	-	1 – Faible	Simple
De 7 à 16	-	2 – Moyen	**Avancée**
	Si vous avez répondu 3 à au moins 2 questions du Thème Sensibilité des données du système	3 – Fort	Approfondie

- **Avancée :** démarche autonome, que l'autorité d'homologation peut mener **avec une assistance conseil externe,** par l'application des outils et des indications donnés dans le guide d'homologation et ses ressources internes.
    - L'analyse des risques doit être conduite en s'inspirant d'une méthode d'analyse des risques (EBIOS ou ISO 27005) tout en **étant simplifiée et limitée au périmètre vertical du téléservice**.
    - Avec un prestataire disposant d'une certification en gestion des risques OU d'une expérience équivalente en gestion des risques IT.
    - Le dossier d'homologation est un rapport de synthèse comprenant :
        - Une description du système à homologuer (mission, finalités, parties prenantes)
        - Le périmètre retenu pour l'analyse (fonctionnel, technique, organisationnel, géographique) avec un schéma
        - La liste des mesures de sécurité existantes et les porteurs
        - La liste évaluée des risques Bruts et Nets,
        - Le plan de conformité avec les échéances et responsabilités
        - Les risques résiduels à l'issue du plan
        - En annexe : la présentation de restitution des travaux à la commission d'homologation

ANNEXE 3 – ECHELLES D'EVALUATION SSI

Echelle des besoins de sécurité

Critères DIC Niveaux	Disponibilité	Intégrité	Confidentialité	Traçabilité
1 Très faible	Indisponibilité > 1 jr	Aucun besoin en intégrité	Public	**Indication technique** L'élément de preuve n'est pas indispensable
2 Faible	Indisponibilité < 1 jr	Détecter et corriger à terme les altérations	Interne	**Trace fonctionnelle** L'élément de preuve est nécessaire, mais son absence temporaire n'est pas vitale
3 Moyen	Indisponibilité < 4h	Détecter et corriger rapidement les altérations	Diffusion restreinte / projet spécifique	**Preuve** L'élément de preuve est obligatoire (i.e. contrainte légale)
4 Fort	Indisponibilité < 2h	Intégrité en temps réel	Confidentiel	

Echelles d'évaluation des risques
Le niveau d'impact est défini sur le maximum des critères suivants :

Niveaux Critères	1 Mineur	2 Moyen	3 Grave	4 Critique
Organisation	Retards ponctuels dans la réalisation d'activités	Perturbations récurrentes des activités	Exécution dégradée des activités	Impossibilité de remplir les activités
Financier	Inférieur à 100 000 XPF	De 100 000 à 1 million XPF	De 1 millions à 10 millions XPF	Supérieur à 10 millions XPF
Juridique	Plainte déboutée	Indemnités à verser	Condamnation civile	Condamnation pénale
Image	Négligeables	Locales	Locales récurrentes et/ou médiatisation	Métropole et/ou International
Social	Mécontentements ponctuels	Perte de confiance durable	Grève de la part des métiers / Manifestations de la population	Blocage d'activités du pays

Le niveau de vraisemblance est défini selon le tableau suivant :

Vraisemblance		Niveaux
Invraisemblable	Ne se produira vraisemblablement jamais	**1**
Vraisemblable	Peut se produire	**2**
Possible	Devrait se produire un jour	**3**
Certain	Se produira sûrement à court terme	**4**

L'évaluation finale du risque est la résultante des deux critères de vraisemblance et d'impact :

Vraisemblance				
4	Moyen	Moyen	Majeur	Majeur
3	Mineur	Moyen	Moyen	Majeur
2	Mineur	Mineur	Moyen	Majeur
1	Mineur	Mineur	Mineur	Moyen
	1	2	3	4
	Impact			

Objectifs de traitement des risques :

- Les risques mineurs sont acceptables en l'état
- Les risques moyens doivent faire l'objet d'un plan de sécurisation
- Les risques majeurs doivent être traités et réduits au niveau inférieur