POLYNESIE FRANÇAISE

VICE-PRESIDENCE,
MINISTERE DU LOGEMENT,
DE L'AMENAGEMENT,
en charge des transports interinsulaires

DIRECTION POLYNESIENNE
DES AFFAIRES MARITIMES

La Directrice

Affaire suivie par :
Bureau Juridique et des Etudes

N° 4329 **/ VP / DPAM**

Papeete, le 03 OCT. 2022

Objet : Consultation Téléservices n° 2022-01-VP-DPAM - Analyse des risques des téléservices et audit technique « IHITAI » et « ESCALES ».

P. J. : Un formulaire d'engagement ;
Un formulaire DPGF ;
Cahier des clauses administratives générales applicable aux marchés publics de service (CCAG – Code polynésie des marchés publics).

La Direction Polynésienne des Affaires Maritimes (DPAM) procède à une consultation pour la réalisation d'une prestation de service d'analyse des risques et audit technique des téléservices « 'IHITAI » et « ESCALES ».

Pour la présente consultation, les entreprises concernées sont invitées à présenter leur candidature et leur offre par courriel (à l'adresse suivante : robin.cordier@administration.gov.pf)

avant **le lundi 24 octobre 2022 à 11 h 00 (heure de Tahiti)**,

selon les modalités fixées dans la présente lettre de consultation, et comportant les pièces et documents requis qui y sont listés, dont notamment le formulaire d'engagement et le formulaire DPGF dûment remplis, datés et signés.

Dans l'attente de votre réponse, je vous prie d'agréer l'expression de ma considération distinguée.

Pour le Vice-Président, et par délégation

DIRECTION POLYNÉSIENNE DES AFFAIRES MARITIMES DPAM Polynésie française

Catherine ROCHETEAU

B.P. 9005 – 98716 Pirae – TAHITI - Polynésie française
Immeuble SAT NUI, N°12, voie M, Fare Ute, Papeete
Tél. : (689) 40 54 45 00 - Fax. : (689) 40 54 45 04 - Email : accueil.dpam@maritime.gov.pf –
Sites : www.maritime.gov.pf / www.service-public.pf/dpam

SOMMAIRE

1 INFORMATION 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.

2 OBJET ET CARACTERISTIQUES PRINCIPALES

2.1 OBJET DU MARCHE.

La Polynésie française s'est inscrite dans une politique publique de dématérialisation. L'objectif est de pouvoir dématérialiser 70% des démarches des usagers à moyen terme. La Direction Polynésienne des Affaires maritimes (DPAM) s'est inscrite pleinement dans cet objectif en lançant dès 2019 le développement du 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 conforme à la Loi du Pays n° 2017-30 du 02 novembre 2017 et à son arrêté d'application n°2043 CM du 18 octobre 2018.

Les prestations de service faisant l'objet de la présente consultation consistent donc à accompagner la DPAM dans la démarche d'homologation de sécurité de deux nouveaux téléservices « 'IHITAI » et « ESCALES » tel que décrit à l'article 3.

2.2 CATEGORIE DE MARCHE

Marché public de prestation de services.

2.3 LIEU D'EXECUTION.

Papeete, Tahiti, Polynésie française

2.4 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.

3 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 : Les analyse des risques

Idéalement la prestation doit se dérouler pour une mise en service du volet téléservice « ESCALES » entre novembre et décembre 2022 et du volet téléservice « IHITAI » début janvier 2023.

Pour tenir ces délais, la DPAM dédie son Product manager pour être l'interlocuteur principal lors des échanges. L'ensemble des documents nécessaires sont quant à eux prêt.

Attention : il est important de noter que les téléservices sont en cours de refonte, les tests d'intrusion se feront donc en dernier afin de s'assurer que le développement puisse se finir. La priorité est mise sur le téléservice « ESCALES ».

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.

La tranche conditionnelle est composée d'1 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.

3.1 DESCRIPTION DES PRESTATIONS DEMANDEES

3.1.1 AU TITRE DE LA TRANCHE FERME

Les analyses de risques

La mission consiste à étudier les risques pour chaque téléservice : IHITAI et ESCALES.
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 portés par la plateforme technique Odoo DPAM commune à IHITAI et ESCALES
B. Risques du téléservice IHITAI en propre
C. Risques du téléservice ESCALES en propre

A ce titre, il est attendu pour chacun des périmètres ci-dessus :

1. La réalisation d'analyses des risques conformément à 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 2043-CM, 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
    - Livrables 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 le 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

Audit technique : test d'intrusion

Les téléservices IHITAI et ESCALES seront exposés sur Internet à destination des usagers.
Afin de tester leur résilience vis-à-vis des cyberattaques et évaluer la qualité de leur implémentation (code et plateforme d'hébégerment), ils doivent chacun faire l'objet d'un test d'intrusion externe.

Dans le cadre de cette prestation, la plateforme technique Odoo ne fera pas l'objet de test d'intrusion.

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 explicitement 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 'IHITAI alimenteront le pentest 'IHITAI.
Les évènements redoutés de l'analyse des risques ESCALES alimenteront le pentest ESCALES.
Les évènements redoutés de l'analyse des risques de la plateforme technique ODOO seront intégrés dans l'un ou l'autre des pentests ('IHITAI ou ESCALES). Un test d'intrusion sur une réplique de la plateforme Odoo a été réalisée en Avril de cette année.

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

Données fournies par la DPAM et le 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 du DSI
- résultats du test d'intrusion Odoo de mars 2022

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 détectées 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.

3.1.2 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 uniquement les scenarii de tests à l'origine de ces vulnérabilités.

3.2 METHODOLOGIE

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

3.3 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 du 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

3.4 PROFONDEUR DE LA DEMARCHE D'ANALYSE

'IHITAI et ESCALES sont développés 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.

4 LIVRABLES

4.1 LIVRABLES PHASE 1

Les livrables attendus au titre des prestations sont liés aux 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 :

- Compte rendu 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

4.2 LIVRABLES PHASE 2 : TEST D'INTRUSION

Les livrables attendus au titre des tests d'intrusion sont :

- Cahier des charges de l'audit (condition, comptes, profils, scenario opérationnels) justifié par le début des travaux d'analyse des risques
- Rapport d'audit du prestataire ayant réalisé l'audit
- Plan de correction des vulnérabilités

4.3 LIVRABLES PHASE 3 : CONTRE-AUDIT DE VERIFICATION.

Les livrables attendus au titre du contre-audit :

- Mise à jour des livrables du test d'intrusion initial.

Pour tous les livrables, 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

5 DUREE DU MARCHE ET DELAI D'EXECUTION

Les deux téléservices ont fait l'objet d'une première livraison le 5 juillet 2022 pour la fonctionnalité backoffice des deux téléservices. La cible d'ouverture du front office du téléservice « ESCALES » est entre novembre et décembre 2022 et celle pour le téléservice « IHITAI » est janvier 2023.

Le délai de réalisation des prestations (tranche ferme et conditionnelle incluse) est fixé par le candidat dans son offre technique et dans le formulaire d'engagement (*réf. : Formulaire d'engagement – Consultation Téléservices n°2022-01-VP-DPAM).*

Ce délai de réalisation ne peut pas être supérieur à la durée du marché, qui est de 6 mois, selon les modalités suivantes :

- Pour la tranche ferme, le délai d'exécution des prestations est fixé à un maximum de 4 mois sur la durée du marché, à compter de la réunion de lancement qui fera l'objet d'un ordre de service délivré par le maître d'ouvrage prescrivant le commencement des prestations.
- Pour la tranche conditionnelle, le délai d'exécution des prestations est fixé à un maximum de 2 mois sur la durée du marché, à compter de l'ordre de service affermissant cette tranche conditionnelle et prescrivant le commencement de la prestation de cette tranche.

A titre informatif, la notification du marché devrait intervenir fin octobre-début novembre 2022.

6 CONDITIONS DE PAIEMENT

L'opération est financée sur le budget de fonctionnement de la Polynésie française.

Il n'est pas prévu d'avance.

Le règlement du marché est échelonné de la manière suivante :

Pour la tranche ferme :

Règlement de 100 % de la phase 1 à l'issue de la phase 1, après remise du :

- Compte rendu 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

Règlement de 100 % de la phase 2 après remise du :

- Cahier des charges de l'audit (condition, comptes, profils, scenario opérationnels) justifié par le début des travaux d'analyse des risques
- Rapport d'audit du prestataire ayant réalisé l'audit
- Plan de correction des vulnérabilités

En cas d'affermissement de la tranche conditionnelle, règlement de 100 % de la phase 3 à l'issue de la prestation, et après remise du :

- Cahier des charges de l'audit (condition, comptes, profils, scenario opérationnels) justifié par le début des travaux d'analyse des risques
- Rapport d'audit du prestataire ayant réalisé l'audit
- Plan de correction des vulnérabilités

Le délai maximal de mandatement de chaque règlement est de trente (30) jours.

Les prix sont fermes, et actualisables suivants les dispositions du C.C.A.G. applicable aux marchés publics de fournitures courantes et de services.

7 PIECES CONSTITUTIVES DU MARCHE

Les pièces constitutives du marché sont énumérées ci-dessous et prévalent les unes sur les autres, dans leur ordre d'énumération, en cas de contradiction ou de différences entre elles.

7.1 PIECES PARTICULIERES

- La présente lettre de consultation valant également règlement de consultation et cahier des clauses communes :

- Le cadre de décomposition du prix global et forfaitaire (D.P.G.F.) : Formulaire D.P.G.F. dûment complété, daté et signé ;

- L'offre technique du titulaire.

7.2 PIECES GENERALES

- Le Cahier des Clauses Administratives Générales (C.C.A.G.) applicable aux marchés publics de fournitures courantes et de services (Arrêté n° 1455 CM du 24 août 2017 modifié relatif à la partie "Arrêtés" du code polynésien des marchés publics).

7.3 LANGUE

Tous les documents remis par le titulaire doivent être rédigés en langue française ou être accompagnés d'une traduction en langue française. Seuls les documents respectant cette consigne seront étudiés lors des analyses des offres.

8 CONDITIONS DE PARTICIPATION – PIECES A FOURNIR PAR LES CANDIDATS

8.1 PREREQUIS DE LA PRESTATION

8.1.1 COMPETENCES HUMAINES ATTENDUES :Pédagogie, capacité à 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 insurmontables.
    - S'assurer que la direction métier est au fait de la démarche en l'intégrant dans les transmissions de livrables (à minima).

8.1.2 COMPETENCES PROFESSIONNELLES ATTENDUESLes compétences professionnelles attendues du prestataire 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 enjeux de sécurité. Elle est relative à la profondeur de la démarche qui est précisée en ANNEXE Profondeur de la démarche

8.1.3 LES OUTILS A UTILISER SONT LES SUIVANTS :

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

8.2 DOSSIER DE CANDIDATURE

Les pièces à fournir pour justifier des capacités techniques, professionnelles à l'appui de la candidature sont les suivantes :

- Le CV des intervenants sur la prestation de service et leur expérience dans des prestations similaires ;
- Les certifications de sécurité des intervenants (EBIOS, ISO 27005…)

9 DOSSIER D'OFFRE

Le candidat doit présenter :

- Une offre pour la tranche ferme ;
- Une offre pour la tranche conditionnelle.

La proposition devra comprendre :

- L'organisation de la prestation et le planning envisagé
- Le plan de charge des intervenants sur les 6 prochains mois
- La description de la méthodologie envisagée pour l'analyse des risques, les tests d'intrusion et l'éventuel contre-audit.

10 CRITERES DE NOTATION

Le marché sera attribué à l'offre économiquement la plus avantageuse sur la base des critères pondérés suivants, après élimination des offres irrégulières, inacceptables, inappropriées et anormalement basses :

Critères	Barème de notation	Points
Valeur technique	Adaptation de la réponse au contexte de la prestation	25
	Compétences techniques (gestion des risques, sécurité, etc)	10
	Calendrier et organisation de la prestation	25
Prix		40
Total		100

Pour le critère « Valeur technique », il est appliqué le calcul suivant à chaque composante du barème de notation :

Appréciation du barème de notation	% de points retenus
Absent	0 %
Insuffisant	25 %
Correct	50 %
Très Satisfaisant	75 %
Excellent	100 %

Pour le critère « Prix », il est appliqué la formule suivante :

B = [P+bas / Poffre] * Z

- B = le nombre de points obtenus par l'offre examinée
- P+bas = le montant de l'offre régulière la moins disante
- P offre = le montant de l'offre examinée

- Z = le nombre maximum de points attribué pour le critère prix qui sera donc de 40.

La note de 40 est affectée à l'offre la moins disante (P+bas).

11 DELAIS DE REMISE DES CANDIDATURES ET DES OFFRES

Le candidat doit présenter sa candidature et son offre par courriel (à l'adresse suivante : robin.cordier@administration.gov.pf) avant **le 24/10/2022 à 11h (heure de Tahiti)**

Le candidat doit présenter :

- Une offre pour la tranche ferme
- Une offre pour la tranche conditionnelle.

Pour toute question sur l'aspect sécurité, merci de se rapprocher de Anne-sophie Bonnat : anne-sophie.bonnat@administration.gov.pf,

Pour les questions sur la consultation: orama.lehartel@administration.gov.pf

12 INSTANCE CHARGEE DES PROCEDURES DE RECOURS

Tribunal administratif de la Polynésie française, avenue Pouvanaa-a-Oopa, BP 4522, 98713 Papeete.
Tél : (689) 40 50 90 25 ; Fax : (689) 40 45 17 24 ; Courriel : greffe.ta-papeete@juradm.fr ; Site Internet : http://polynesie-française.tribunaladministratif.fr/.

13 REGLES DIVERSES ET DELAI DE VALIDITE DES OFFRES

13.1 PROPRIETE DE L'OFFRE DE SERVICE.

Les offres de service présentées par chaque candidat, ainsi que les documents afférents, demeurent la propriété exclusive du maître d'ouvrage et ne seront pas retournés au candidat, sauf si la consultation ne donne pas lieu à suites.

13.2 DELAI DE VALIDITE DES OFFRES.

Le délai de validité des offres présentées par les candidats est fixé à 190 jours, décompté à compter de la date limite de réception des offres mentionnée à l'article 11 ci-dessus.

14 ÉLEMENTS D'INFORMATION UTILES CONCERNANT LES PROJETS DU MARCHE

14.1 'IHITAI

Ce projet est piloté par la DPAM (Direction Polynésienne des Affaires Maritimes). Il s'inscrit dans la démarche de digitalisation de ses services (tout comme dans le cadre du téléservice « REVATUA »).

Le téléservice projeté est défini comme l'application de gestion "des gens de mer", dénommé « 'IHITAI » ("Le marin").

En effet, La Vice-Présidence, Ministère en charge des transports interinsulaires, a confié à la DPAM une mission de conception et de coordination d'un projet dont l'objectif est d'assurer la gestion de carrière des marins relevant de la compétence de la Polynésie française, en passant par la délivrance des titres professionnels ainsi que le suivi du temps de navigation en mer et la gestion des examens.

Depuis 2014, la DPAM est chargée de délivrer les titres de formation professionnelle maritime requis pour les marins de Polynésie française. Or, le projet demeurait en attente de proposition de solution technique de gestion informatique. Il a mis en évidence un besoin indispensable et obligatoire de régulation, afin de permettre la délivrance sécurisée des titres de formation professionnelle maritime.

Particulièrement exacerbé durant cette période d'attente, l'expression du besoin de gestion opérationnelle de la carrière des marins a été largement relayé depuis 2017 par les inquiétudes des professionnels du secteur auprès de DPAM, en s'appuyant sur plusieurs constats :

- Les titres et diplômes ne sont pas délivrés ;
- Le temps en mer d'un marin n'est pas facilement retraçable ; de fait les marins ou capitaines, ne peuvent faire valoir leurs droits ou leurs expériences professionnelles ;
- Le paiement des timbres fiscaux est problématique pour les inscriptions ou délivrance des titres ;
- Les dossiers des marins existent principalement en version papier. Or, il devient extrêmement difficile de stocker du papier. De plus, cela ne permet aucune sécurisation des données ni analyses fiables.

L'organisation de la gestion de la carrière des marins dans les îles de Polynésie française constitue un enjeu majeur de diverses politiques publiques : gestion des compétences pour déterminer les besoins de formation, cibler les stratégies de formation pour favoriser l'employabilité des marins, suivi des équipages (liste équipage) au titre de la sécurité des personnes, application du droit du travail (temps de repos à bord).

Ce projet comporte de multiples volets : administratif, réglementaire, ressources humaines, technique, formation des agents, mais au préalable, il s'agit de traiter le volet numérique pour définir et établir un système centralisé et coordonné qui pourra bénéficier à l'ensemble des administrations pour leurs besoins.

Ainsi, pour favoriser et garantir la sécurité de la carrière des marins dans les îles de Polynésie française, il convenait de créer un téléservice, portail dédié aux usagers et aux professionnels.

14.1.1 LES OBJECTIFS DU TELESERVICE

L'objectif principal est de permettre la gestion organisée de la carrière des marins dans les îles de Polynésie française, notamment par un téléservice :

- Qui s'adressera à une population cible élargie (usagers souhaitant s'inscrire à un examen, usagers souhaitant avoir un accès à son expérience professionnel, usagers souhaitant avoir un accès à l'ensemble de sa carrière, professionnels de la formation qui assurent pour leurs clients l'inscription aux examens, et armateurs qui assurent pour leurs employés le suivi des temps de travail en mer) ;
- Qui apportera des fonctionnalités :
    - Paiement en ligne pour les droits d'inscription aux examens via Payzen

- Saisie de formulaires dématérialisés pour :
    - La création de comptes marins, compte armateurs et comptes organisme de formation,
    - La saisie des listes d'équipages
    - La saisie des formations
    - L'inscription aux examens
    - La demande d'immatriculation, de modification de navires, et de radiation
  - Statistiques avec Power BI
  - Diplôme sur la blockchain.
- Qui améliorera et digitalisera l'existant tant pour les utilisateurs externes qu'internes (ergonomie, fonctionnalités).
- Qui améliorera la sécurité grâce à une meilleure connaissance des marins et des relevés des temps de navigations
- Qui a pour ambition de représenter un Compte « Carrière en Ligne » simplifié pour le marin

14.1.2 LES FONCTIONNALITES DU TELESERVICE

➔ Profil du marin : permettant d'avoir accès, en back office pour les agents DPAM et en front office pour le marin lui-même, à l'expérience professionnelle du marin, ses titres, ses relevés de notes ainsi que ses informations personnelles. Le marin pourra s'inscrire lui-même ;

➔ Gestion des examens : permettant aux organismes de formation de transmettre leur planning de formation et à la DPAM de créer les sessions d'examens. Les organismes de formations pourront alors inscrire les candidats en ligne et payer les frais d'inscriptions à certains examens. La DPAM pourra contrôler les inscriptions et ensuite procéder à la notation des candidats avant convocation de la commission d'examen ;

➔ Gestion de l'expérience : permettant aux armateurs de fournir à la DPAM les temps de navigation des marins pour chaque campagne de pêche ;

➔ Gestion des titres : permettant à la DPAM, en fonction des diplômes obtenus et de l'expérience en mer, de pouvoir générer les titres professionnels à l'aide de la blockchain. Les titres seront alors disponibles en ligne et également téléchargeables ;

Gestion des navires : permettant à la DPAM d'avoir un registre des navires de Polynésie française. Les particuliers pourront demander une immatriculation, déclarer tous changements sur le navire et demander la radiation du navire. Pour les utilisations du navire autres que le loisir, la DPAM pourra suivre les visites annuelles de sécurités du navire et délivrer le permis de navigation. Dans le cadre d'une utilisation de loisir, la DPAM pourra délivrer une carte de circulation. L'ancien logiciel de registre des navires « GREPNAV » étant devenu obsolète, l'IHITAI va en récupérer les données

14.1.3 LES PRINCIPES DU TELESERVICE

Front office

Les marins, les organismes de formation et les armateurs utilisent le téléservice 'IHITAI disponible sur navigateur web.

Le marin consulte son profil, où est mis à disposition son temps de navigation en mer, ses titres et relevés de notes. Il maintient à jour ses informations de contact.

L'armateur saisit les listes d'équipages affectés aux campagnes de pêches, l'administrateur attribue des droits différents aux personnes qu'il invite dans la société.

L'organisme de formation saisit ses sessions de formations, il inscrit les marins aux examens, peut payer dans certains cas les frais à la place du marin et envoie les attestations de formations pour les sessions qui le requièrent.

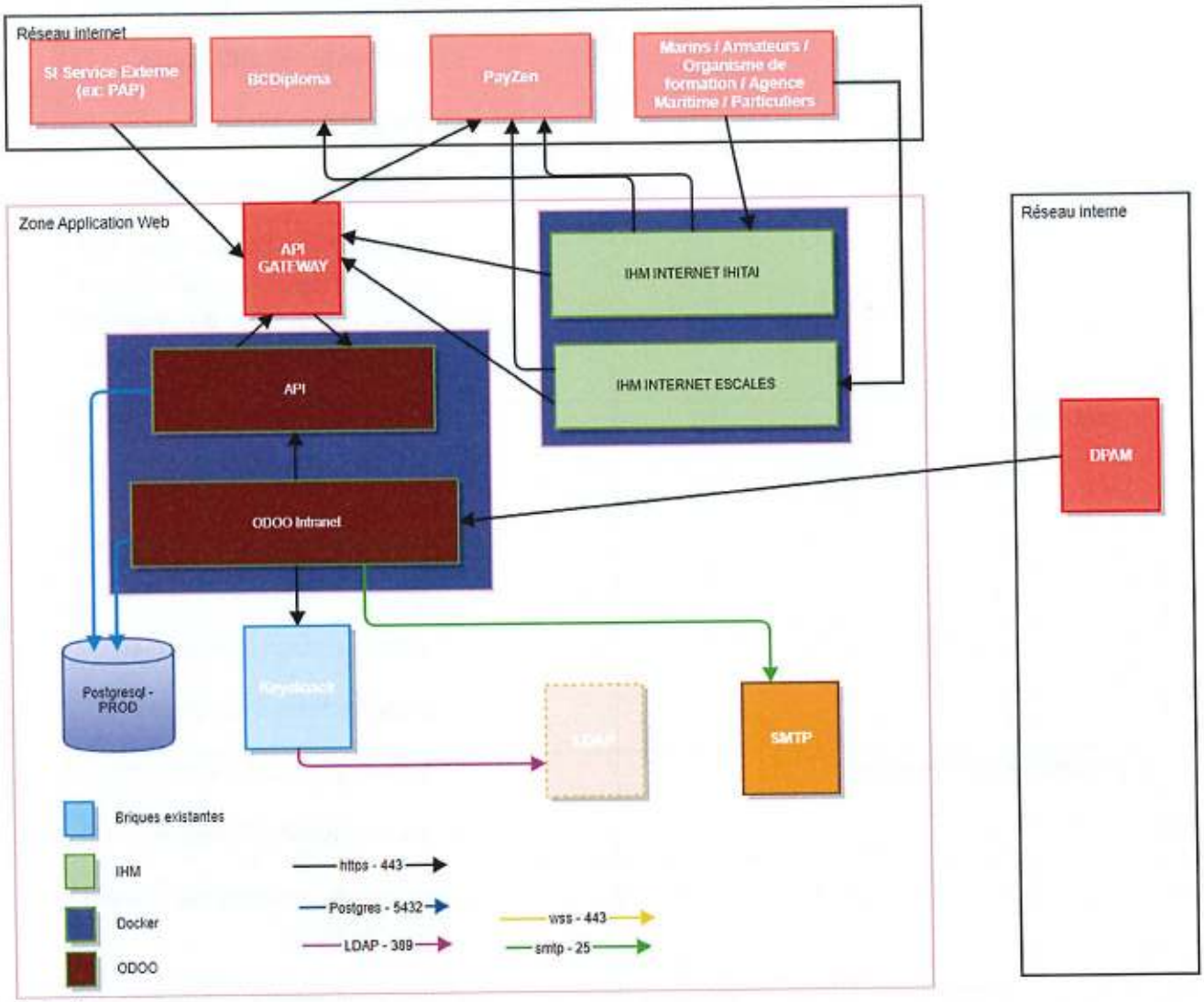
Back office
Les agents de la DPAM utilisent l'application dans différents cadres.
Les agents en charge de la formation disposent d'un ordinateur déjà fourni et durci par le DSI.
L'ordinateur aura accès à l'application via Internet en https.
Ils établissent le planning des sessions d'examens à partir du planning de sessions de formation fourni par les organismes de formations. Ils valident les listes d'équipages fournies par les armateurs. Ils notent les examens et génèrent les titres des marins.

Les agents en charge de la sécurité bénéficient de tablettes disposant d'un accès réseau mobile (4G) pour accéder au système d'information via VPN. Les tablettes et l'abonnement au réseau mobile sont dédiés exclusivement à cet usage.
L'agent réalise les visites de sécurité des navires, établit le rapport de visite et génère le permis de navigation des navires professionnels.

Les agents en charge de l'immatriculation disposent d'un ordinateur déjà fourni et « durci » par le DSI.
L'ordinateur aura accès à l'application via Internet en https.
Son rôle essentiel est de s'assurer de l'immatriculation des navires, des modifications liées à ces derniers et à leur radiation.
L'administrateur :
L'ordinateur aura accès à l'application via Internet en https.
Il gère les droits des agents et effectue les contrôles administratifs liés à l'utilisation du téléservice par les agents.

14.1.4 MODULES ET FONCTIONNALITES

14.1.4.1 **MODULES**



Brique 1
API : Il s'agit de la brique contenant tout le cœur métier. Elle propose des API REST aux autres modules qui se connectent dessus ainsi qu'à l'IHM.
Développée en XML/Python

Brique 2
Base de données : Base Postgresql contenant les informations métier

Brique 3
Odoo intranet - Se connecte à la brique BDD pour fournir une interface utilisateurs à la DPAM ainsi qu'aux agents de la DSI pour l'exploitation. Développée avec ODOO.

Brique 4
IHM internet : Téléservice destiné aux utilisateurs externes

Brique 5
Utilisation de Keyclock pour l'authentification

14.1.4.2 **FONCTIONNALITES**

Le marin	- Créé un compte / s'authentifie - Joint les justificatifs requis - S'inscrit à un examen - Paye les droits dûs en ligne - Consulte son compte pour voir ses informations générales, ses titres, ses relevés de notes, et ses temps de navigation en mer
L'amateur	- Créé un compte / s'authentifie - Joint les justificatifs requis - Créé une demande de compte pour le marin - Inscrit un marin à un examen - Saisie les listes d'équipages
L'organisme de formation	- Créé un compte / s'authentifie - Joint les justificatifs requis - Créé une demande de compte pour le marin - Inscrit un marin à un examen - Saisit les déclarations de formation - Paye pour un marin - Envoie les attestations de formations
L'agent de la cellule formation	- Se connecte via son LDAP - Vérifie les demandes de compte et les documents joints - Vérifie les listes d'équipages - Créé les sessions examens à partir des sessions de formation

	déclarées - Vérifie les inscriptions à l'examen - Entre les notes obtenues à l'examen - Créé les titres professionnels
L'agent de la cellule immatriculation	- Se connecte via son compte LDAP - Vérifie les dossiers des navires immatriculés - Génère une carte de circulation - Génère un certificat de radiation du registre d'immatriculation des navires - Saisit les référentiels des décisions d'approbations, moteurs, et constructeur - Génère une décision d'approbation
L'agent de la cellule sécurité	- Se connecte via son LDAP - Formalise les visites du navire et des modèles (coques) - Génère les rapports de visite - Génère le permis de navigation

14.1.5 PARTIES PRENANTES

Parties prenantes 'IHITAI	**Rôles 'IHITAI**
DPAM	Maître d'ouvrage
DSI	Développement, hébergement
Invitu, sous-traitant de la DPAM	Développement Odoo
BCDiploma, sous-traitant de la DPAM	Création et stockage du diplôme du Marin sur la blockchain (par API)
Payzen de l'OSB, sous-	Paiement en ligne des droits d'entrée ou de délivrance d'examen

traitant de la DPAM	implémenté par clé d'API
Azure, sous-traitant BCDiploma	Hébergement des diplômes des marins, Platform as a Service
Agent DPAM	Utilisation du Back-Office pour : Cellule Formation : pour gérer la formation professionnelle et la carrière des Marins Cellule Immatriculation : pour gérer l'immatriculation, la modification et la radiation des navires Cellule Sécurité : pour gérer les visites de sécurité
Utilisateurs externes	Organismes de formation : utilisation du FrontOffice pour faire la déclaration des sessions de formations, inscrire les marins aux examens et fournir les attestations de formations Armateur : utilisation du FrontOffice pour faire la déclaration des listes d'équipages et suivre le renouvellement des modules et des visites médicales des marins travaillant pour lui Marin : utilisation du FrontOffice pour suivre sa carrière

14.1.6 TECHNOLOGIES

Sujet	Choix
Service API REST (Serveur HTTP)	ASP.net
Application organisme de formation / armateur / marins	Angular
Base de données	PostgreSQL
Application DPAM	ODOO
Envoi du courriel	Outlook
Hébergement	DSI
Authentification	Keycloack et ODOO

14.1.7 DESCRIPTION DES API

Objectif de mise à disposition des API GET pour les autres services. Liste des API prévisionnelle :

- GET / POST / PUT : informations générales marin / expériences / titres / diplômes
- GET / POST / PUT : informations sur le compte usager
- GET / POST / DELETE / PUT : sessions de formation
- GET : sessions d'examens
- GET / POST / DELETE / PUT : campagnes de pêches
- GET / POST : paiement des sessions d'examens
- GET / POST / PUT : Liste des navires et documents relatifs

14.2 GESTION DES ESCALES

Ce projet piloté par la DPAM s'inscrit dans la démarche de digitalisation de ses services (tout comme Revatua et 'IHITAI).

La Vice-Présidence, ministère en charge des transports interinsulaires, a confié à la DPAM une mission de conception et de coordination d'un projet dont l'objectif est d'assurer la gestion des escales des navires dans les îles de Polynésie française.

L'organisation de la gestion des escales des navires dans les îles de Polynésie française constitue un enjeu majeur de diverses politiques publiques. Cette organisation comporte de multiples volets : administratif, réglementaire, ressources humaines, technique, formation des gestionnaires. Au préalable, il s'agit de traiter le volet numérique pour définir et établir un système centralisé et coordonné.

Ainsi, pour favoriser et garantir la sécurité des escales de navires dans les îles de Polynésie française, il s'agit de créer un téléservice, portail de réservations, dédié aux navires de plaisance, yachts, navires de croisières, navires de commerce, navires de pêche, sollicitant une escale avec réservation d'une place dédiée dans les îles de Polynésie française (hors circonscription portuaire).

Ce téléservice simplifie également l'application de la réglementation métier, notamment la réglementation sanitaire telle que l'arrêté 525 CM du 13 mai 2020 portant mesures d'entrée et de surveillance *sanitaire* des arrivants en Polynésie française dans le cadre de la lutte contre la covid 19.

Cet arrêté ne s'applique plus mais des dispositions similaires pourraient être adoptées si l'état d'urgence sanitaire devait être déclaré à nouveau.

La réservation de place de stationnement des navires (amarrage, mouillage) pourrait être associée au paiement d'une redevance d'occupation du domaine public maritime modulable en fonction des services proposés.

Le service gestionnaire du téléservice est la DPAM.

De manière générale, l'enjeu est d'éviter une situation dans laquelle deux navires se retrouveraient en même temps au même endroit (place dédiée au stationnement du navire), ou empêchant les opérations des uns ou des autres.

Un autre enjeu concerne la mutualisation des moyens, il s'agit de simplifier et d'accélérer les démarches, pour l'usager (éviter de redemander ou de faire une copie des papiers), comme pour les services.

Aujourd'hui, il arrive qu'un voilier en escale 24 heures et parte le lendemain, avant la réalisation de tout contrôle.

Le téléservice sera le point d'entrée (et de sortie) obligatoire sans distinction du type de navire. Sur le principe, la déclaration (entrée ou sortie) se fera avec un minimum de documents, qui seront visés et gérés par une autorité unique et légale.

L'ensemble des déclarations est centralisé et pourrait être consultable : soit par interconnexion avec les différents acteurs, soit par transmission automatisée au gestionnaire concerné. Les acteurs conserveront ainsi la gestion de leurs propres procédures.

Ceci évitera :

- De solliciter plusieurs fois de l'usager les mêmes documents ou informations ;
- D'avoir des versions différentes de ces informations, souvent déclaratives ;

Cela permettra de faciliter et d'accélérer une procédure en cours (ex : chercher le propriétaire d'un navire, sa date d'entrée, son itinéraire).

Les acteurs sont la DPAM, les agents maritimes, les compagnies maritimes, les plaisanciers, la station de pilotage maritime, le port autonome de Papeete, la direction de l'équipement (DEQ), le cluster maritime de Polynésie française (https://cluster-maritime.pf/) et les services de l'Etat.

La DSI et la DPAM ont la charge de la réalisation de ce projet.

14.2.1 LES OBJECTIFS DU TELESERVICE

Ce projet « Gestion des escales » a pour finalité de dématérialiser l'obligation de déclaration et de réservation avant toute arrivée de navire en Polynésie française (hors circonscription portuaire). Le téléservice doit être conçu de sorte qu'il devienne de l'intérêt de l'agent maritime ou de l'usager de passer par la future solution numérique et de bien communiquer ses renseignements (meilleure expérience usager, moins de retards causés par les conflits d'usage, etc.).

14.2.2 LES FONCTIONNALITES DU TELESERVICE

Profil du réservant : permettant d'avoir accès à l'historique des réservations, des voyages, des informations et documents du compte, des informations et documents du navires, des documents fournis pour la réservation. Pour une société, il sera possible d'inviter un nouvel usager ;

Gestion des réservations : permettant aux usagers de faire une demande de réservation. La DPAM pourra contrôler les demandes et ensuite procéder à la gestion des conflits et à la facturation des droits dûs ;

Gestion des déclarations d'entrées : permettant aux usagers de fournir à la DPAM les documents nécessaires pour la réservation, de confirmer leur réservation 48h avant l'arrivé ;

Gestion des mouillages : permettant à la DPAM de tenir à jour les informations relatives aux mouillages et zones, mais également d'en créer ou en supprimer ;

Gestion des navires : permettant à la DPAM d'avoir un registre des navires faisant escales en Polynésie française.

14.2.3 LES PRINCIPES DU TELESERVICE

Front office
Les particuliers et agences maritimes utilisent le téléservice ESCALES disponible sur navigateur web.

Le particulier consulte son profil, s'enregistre au préalable lui-même et son ou ses navires, saisit des demandes de réservations, déclare son arrivé 48h à l'avance en envoyant les documents nécessaires et paye en ligne ses réservations et autres droits, le cas échéant ;

L'agence maritime consulte son profil, s'enregistre au préalable lui-même et son ou ses navires, saisit des demandes de réservations, déclare une arrivé 48h à l'avance en envoyant les documents nécessaires,

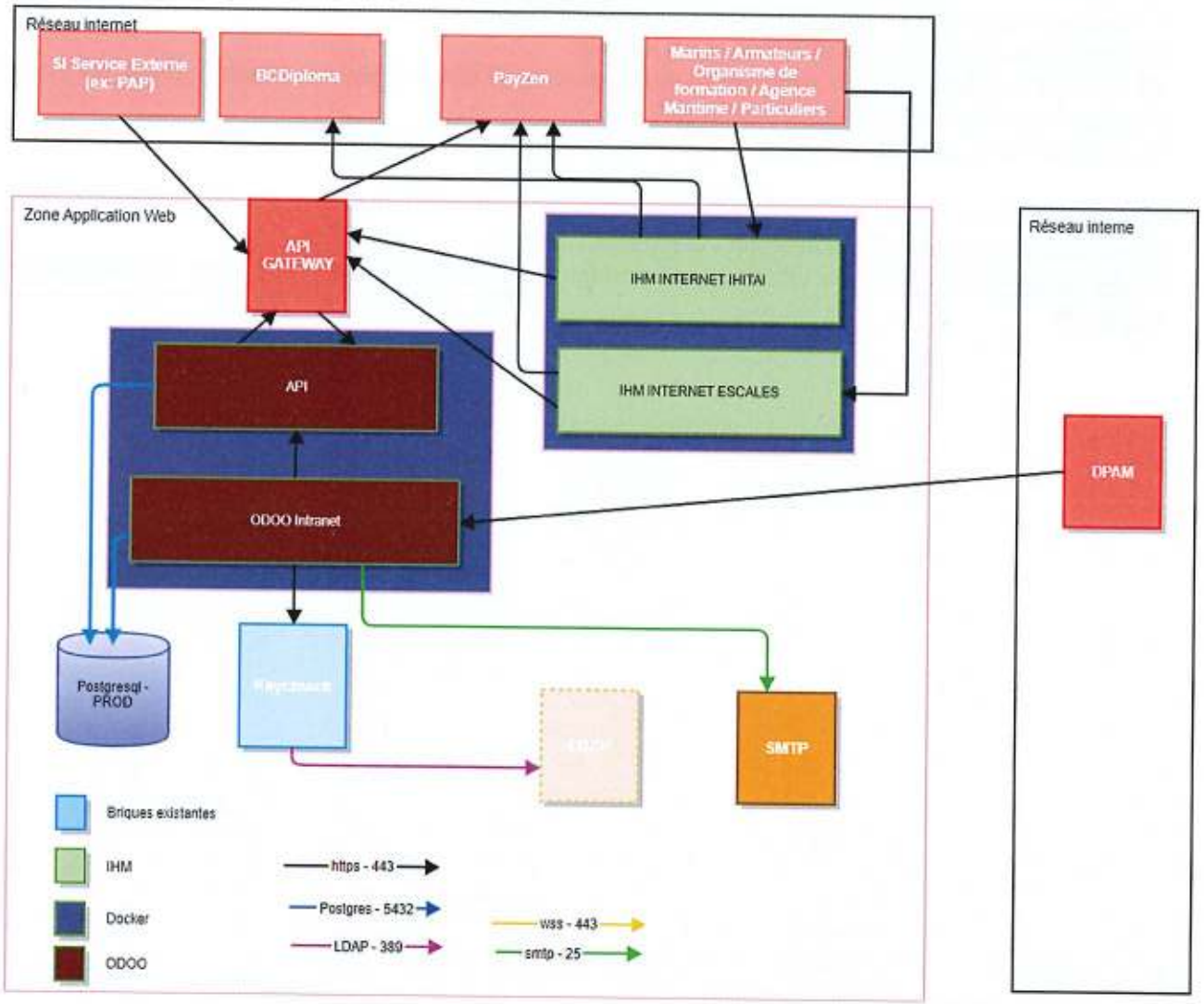
importe des voyages par csv, invite des utilisateurs dans sa société, paye en ligne ses réservations et autres droits, le cas échéant ;

Back office
Les agents en charge des escales, disposent d'un ordinateur déjà fourni et durci par le DSI.
L'ordinateur aura accès à l'application via Internet en https.
Il a accès aux mêmes fonctionnalités que les usagers.
Ils valident les demandes de comptes et de navires, les demandes de réservation, gèrent les conflits d'usage, les référentiels navires et mouillages.
Ils vérifient les documents d'entrées, et les envoient aux services compétents.

L'administrateur :
L'ordinateur aura accès à l'application via Internet en https.
Il gère les droits des agents et effectue les contrôles administratifs liés à l'utilisation du téléservice par les agents.

14.2.4 MODULES ET FONCTIONNALITES

14.2.4.1 **MODULES**



Brique 1
API : Il s'agit de la brique contenant tout le cœur métier. Elle propose des API REST aux autres modules qui se connectent dessus ainsi qu'à l'IHM.
Développée en XML/Python

Brique 2
Base de données : Base Postgresql contenant les informations métier

Brique 3
Odoo intranet - Se connecte à la brique BDD pour fournir une interface utilisateurs à la DPAM ainsi qu'aux agents du DSI pour l'exploitation. Développée avec ODOO.

Brique 4
IHM internet : Téléservice destiné aux utilisateurs externes

Brique 5
Utilisation de Keyclock pour l'authentification

14.2.4.2 **FONCTIONNALITES**

L'**agence maritime** (ou **consignataire**, est employé par un armateur ou un affréteur pour le représenter dans un port lors de l'escale d'un navire.)	- Créé un compte / s'authentifie - Joint les justificatifs requis - Fait une demande de création de navire - Modifie les informations et les justificatifs sur le navire - Créé / Supprime des réservations - Importe des voyages - Déclare l'entrée pour une première touchée
Le **particulier** qui détient ou exploite un navire	- Créé un compte / s'authentifie - Joint les justificatifs requis - Fait une demande de création de navire - Modifie les informations et les justificatifs relatifs au navire - Créé / Supprime des réservations - Importe des voyages - Déclare l'entrée pour une première touchée
L'agent de la cellule escales (DPAM)	- Se connecte via son LDAP - Vérifie les demandes de compte et les documents joints - Vérifie les demandes concernant le navire et les documents joints - Vérifie les documents d'entrée - Vérifie les réservations et les conflits d'usage - Configure les zones / les

	mouillages - Configure les tarifs des mouillages

14.2.5 PARTIES PRENANTES

Parties prenantes	Rôles
DPAM	Maître d'ouvrage
DSI	MOE, gestion de projet, développement, hébergement
Digital Techno, sous-traitant de la DPAM	Développement, maintenance corrective et évolutive
Payzen de l'OSB, sous-traitant de la DPAM	Paiement en ligne des droits d'escale implémenté par clé d'API
API Revatua, DPAM	Récupération des réservations du planning des navires par l'API Revatua
OpenStreetMap	Outil de cartographie Open Source (zones d'escale)
Agent DPAM	Utilisation du Back-Office par la cellule escales pour organiser les escales et gérer les conflits d'usage.
Utilisateurs externes	Utilisation du FrontOffice par les agences maritimes et usagers

14.2.6 TECHNOLOGIES

Sujet	Choix
Service API REST (Serveur HTTP)	ASP.net
Application organisme de formation / armateur / marins	Angular
Base de données	PostgreSQL
Application DPAM	ODOO
Envoi du courriel	Outlook
Hébergement	DSI
Authentification	Keycloack et ODOO

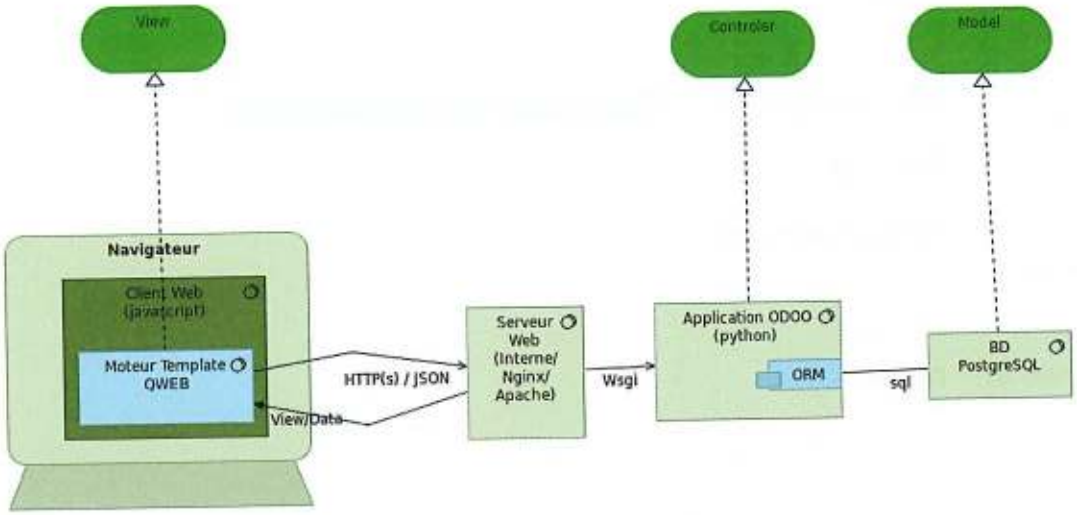
14.2.7 DESCRIPTION DES API

Objectif de mise à disposition des API GET pour les autres services. Liste des API prévisionnelle :

- GET / POST / DELETE : réservations
- GET / POST / PUT / DELETE : navires
- GET / POST / PUT / DELETE : déclaration d'entrée
- GET / POST / PUT / DELETE : clearance de sortie
- GET : mouillages / zones / îles / archipels

14.3 PLATEFORME TECHNIQUE ODOO

Les deux backoffice sont construits sur le même socle technique Odoo et les 2 téléservices sous Angular.



L'application Odoo DPAM comprend les applications de Odoo S.A. suivantes :

Nom de module	Nom technique	Source
Achats	purchase	https://www.odoo.com/page/purchase
Calendrier	calendar	
Congés	hr_holidays	https://www.odoo.com/page/leaves
Contacts	contacts	
Contrats des employés	hr_contract	https://www.odoo.com/page/employees
CRM	crm	https://www.odoo.com/page/crm
Dépenses	hr_expense	https://www.odoo.com/page/expenses
Discussion	mail	https://www.odoo.com/page/discuss
Employés	hr	https://www.odoo.com/page/employees
Facturation	account	https://www.odoo.com/page/billing
Inventaire	stock	https://www.odoo.com/page/warehouse
Notes	note	https://www.odoo.com/page/notes
Parc Automobile	fleet	https://www.odoo.com/page/fleet
Projet	project	https://www.odoo.com/page/project-management

Site web	website	https://www.odoo.com/page/website-builder
Sondages	survey	https://www.odoo.com/page/survey
Tableaux de bord	board	
Ventes	sale_management	https://www.odoo.com/page/sales
Base rest	base_rest	
Billeterie d'evenements en ligne	website_event_sale	
Link partner to events	partner_event	

L'application Odoo DPAM comprend les applications suivantes développées en interne.

Nom de module	Nom technique
PF: GOV	l10n_pf_gov
PF: GOV: DPAM	l10n_pf_gov_dpam
PF: Iles	l10n_pf_state
Polynésie française	l10n_pf
Référentiel	referentiel
DPAM Fleet Boat	dpam_fleet_boat

L'application Odoo DPAM comprend les applications/modules suivants communautaires suivants :

Nom de module	**Nom technique**	**Auteur**
Web	web	Odoo S.A.
Importation de base	base_import	Odoo S.A.
Module d'importation de base	base_import_module	Odoo S.A.
test-import-export	test_impex	Odoo S.A.
CRM Only Security Groups	crm_security_group	Tecnativa, Odoo Community Association (OCA)
Odoo Enterprise Theme	legion_enterprise_theme	Bytelegion
Multi Step Wizard	multi_step_wizard	Camptocamp (OCA)
Odoo Web Login Screen	odoo_web_login	Xao Xao Digital CO., LTD
Partner first name and last name	partner_firstname	(OCA)
Project Template	project_template	Patrick Wilson (OCA)

Purchase Order Type	purchase_order_type	Camptocamp (OCA)
OSB Payment Acquirer	payment_osb	Lyra Network
Mail Attach Existing Attachment	mail_attach_existing_attachment	Tecnativa
Partner Identification Numbers	partner_identification	Tecnativa
Partner contact birthplace	partner_contact_birthplace	AgileBG
	Password_security	
	Calendar_count	
	Gdpr_cookie_notice	
	Query_deluxe	
	Sh_blackmate_theme_adv	
	Sh_cookie_notice	
	Sh_message	
	Sh_website_gdpr	

L'application Odoo DPAM comprend les modules suivants développés par la société INVITU et DIGITAL TECHNNO :

Nom de module	**Nom technique**	**Auteur**
DPAM Exam - Website	dpam_website_seaman_exam	INVITU SARL
Gestion des marins - Website	dpam_website_seaman_profile	INVITU SARL
Base Rest Fleet	dpam_base_rest_fleet	INVITU SARL

DPAM		
DPAM Fleet BOAT	dpam_fleet_boat	INVITU SARL
DPAM	dpam_profile	INVITU SARL
DPAM Seaman Diploma	dpam_seaman_diploma	INVITU SARL
DPAM Seaman Exam	dpam_seaman_exam	INVITU SARL
DPAM Seaman Profile	dpam_seaman_profile	INVITU SARL
DPAM Seaman website experience	Dpam_website_seaman_experience	INVITU SARL

Nom de module	**Nom technique**	**Auteur**
DPAM - Gestion des escales	dpam_stopover_management	DIGITAL TECHNO
DPAM - Gestion des escales portail	dpam_website_stopover_management	DIGITAL TECHNO

Modules Python

Nom
libass
openpyxl
psycopg2
pip
pyquerystring

Nom
parse-accept-language
apispec
marshmallow
marshmallow-objects
openpyxl
zxcvbn
boto3
pandas
pysaml2
python-jose
lxml
minio
git+https://github.com/apache/chemistry-cmislib.git@py3_compat#egg=cmislib
cx_Oracle
docx-mailmerge
cachetools
cerberus

15 ANNEXE 1 – EVALUATION DES ENJEUX

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.				2 'Ihitai 3 Escales	
	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.				2 'iHitai 3 Escales	
	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		

B.P. 9005 – 98716 Pirae – TAHITI - Polynésie française
Immeuble SAT NUI, N°12, voie M, Fare Ute, Papeete
Tél. : (689) 40 54 45 00 - Fax. : (689) 40 54 45 04 - Email : accueil.dpam@maritime.gov.pf –
Sites : www.maritime.gov.pf / www.service-public.pf/dpam

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 ?				3	
	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		
	Question n° 9 : Quel est le niveau de sophistication des attaques potentielles contre le SI ?				2	
	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.		
	Question n° 10 : Quelle est la visibilité des attaques potentielles contre le SI ?				2	
	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		
	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**

16 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

17 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