

MARCHE PUBLIC DE TECHNIQUES DE L'INFORMATION ET DE LA
COMMUNICATION



FOURNITURE DE PRESTATIONS D'ASSISTANCE A MAITRISE
D'ŒUVRE POUR LA DSI DE LA BRANCHE RECOUVREMENT DU
REGIME GENERAL DE LA SECURITE SOCIALE

LOT 5
SÉCURITÉ

N° de procédure

P	2	6	1	2	-	A	O	O	-	D	S	I
---	---	---	---	---	---	---	---	---	---	---	---	---

Cahier des Clauses Techniques Particulières (C.C.T.P.)

Sommaire

1	PREAMBULE.....	3
1.1	OBJET DE LA CONSULTATION	3
2	DESCRIPTION DU PERIMETRE DU LOT	3
2.1	COUVERTURE ET ORGANISATION	3
2.2	DESCRIPTION DU PERIMETRE	4
2.3	TECHNOLOGIE	4
2.4	ENJEUX, PROJETS ET EVOLUTIONS A VENIR	7
2.5	RISQUES.....	8
2.5.1	<i>La sensibilité des données.....</i>	8
2.5.2	<i>La confidentialité des informations.....</i>	9
2.5.3	<i>La manipulation de système de protection et de détection d'incidents.....</i>	9
2.6	CERTIFICATIONS.....	10
3	DESCRIPTION DES PRESTATIONS ATTENDUES	11
3.1	LISTE DES PRESTATIONS ATTENDUES	11
3.2	DETAIL DES PRESTATIONS ATTENDUES	12
3.2.1	<i>Globalisé</i>	12
3.2.2	<i>Expertise.....</i>	14
3.2.3	<i>Service</i>	33
3.2.4	<i>Activité</i>	44
4	MODALITES DES PRESTATIONS	45
4.1	GOUVERNANCE DU LOT	45
4.2	INDICATEURS DE NIVEAUX DE SERVICES	48
4.3	CONDITIONS GENERALES D'EXECUTION DES PRESTATIONS.....	48
4.3.1	<i>Applicables aux prestations d'initialisation du lot</i>	48
4.3.2	<i>Applicables aux prestations de réversibilité.....</i>	48
4.3.3	<i>Applicables au service Digital Signature Service (DSS).....</i>	49
4.3.4	<i>Applicables au service Usine d'Anonymisation des Données (UAD)</i>	49
4.3.5	<i>Applicables au service Force d'Intervention Rapide (FIR).....</i>	50
4.3.6	<i>Applicables au service Test d'intrusion.</i>	50
4.3.7	<i>Applicables au service Forensic.....</i>	51
4.3.8	<i>Applicables au service Threat Intelligence</i>	51
4.3.9	<i>Accès aux expertises de niche.</i>	52
4.3.10	<i>Exigences de sécurité</i>	53
5	CAS PRATIQUE	54
5.1	ÉVALUATION DE LA MATURITE DE LA SECURITE	54
5.2	ACCOMPAGNEMENT EN EXPERTISE TECHNIQUE CLOUD	54

1 Préambule

1.1 Objet de la consultation

Ce document constitue le Cahier des Clauses Techniques Particulières de ce lot. Il s'inscrit en complément au CCTP commun. Il décrit aux soumissionnaires les conditions spécifiques propres au lot en objet en matière de périmètre et de prestations à exercer.

Ce cahier des charges fait partie du DCE (Dossier de Consultation des Entreprises) et des documents contractuels constituant l'Accord Cadre conclu avec le titulaire.

2 Description du périmètre du lot

2.1 Couverture et organisation

Les enjeux de sécurité des systèmes d'information et de protection des données sont aujourd'hui au cœur des préoccupations de la Caisse Nationale.

Les enjeux principaux sont :

- L'évolution du cadre réglementaire avec notamment la désignation des organismes de la branche Recouvrement comme opérateurs de services essentiels (OSE) et la nécessité de respecter le règlement général sur la protection des données (RGPD),
- L'évolution de la cybermenace liée tant au contexte géopolitique qu'à l'évolution des technologies.
- La multiplication des tentatives de compromission du Système d'Information de l'ACOSS
- La conduite d'audits mettant en évidence certaines vulnérabilités et la nécessité d'adapter en permanence le niveau de sécurité du Système d'Information à ces menaces.

3 chaînes composent le dispositif de sécurité de la branche recouvrement :

- Une chaîne décisionnelle incarnée par la fonction d'autorité du Directeur Général et des instances créées pour piloter la stratégie et la mise en œuvre,
- Une chaîne fonctionnelle représentée par un RSSI de branche,
- Une chaîne opérationnelle représentée par un Département SSI sous l'autorité d'un Directeur Adjoint Architecture, Infrastructure et Sécurité rattaché au DSI.

Le Département Sécurité du SI a pour mission de :

- Piloter la sécurité opérationnelle et fournir un appui aux missions du RSSI,
- Gérer les plans de continuité et de reprise informatique de la DSI en particulier sous un angle cyber,
- Concevoir, mettre en place et gérer les capacités Sécurité pour anticiper et détecter les incidents de sécurité,
- Concevoir, mettre en place et gérer les capacités Sécurité pour répondre et remédier aux incidents de sécurité,
- Concevoir, mettre en place et gérer les capacités Sécurité pour anticiper et remédier aux vulnérabilités SI,
- Concevoir, mettre en place et gérer les capacités liées à la gestion des identités et des accès,
- Concevoir, mettre en place et gérer les briques de sécurité des réseaux et des systèmes au sein du SI de l'ACOSS,
- Intégrer la sécurité tout au long du cycle de vie des projets en collaboration avec le Département Architecture

Pour cela, la DAAIS-SSI est organisée en 2 pôles : Vulnérabilité/Résilience et Opérations de Sécurité de l'Information.

Dans sa réponse, le candidat décrira l'organisation spécifique qu'il mettra en œuvre pour réaliser sa mission sur le LOT SECURITE. Il devra démontrer qu'il a la capacité d'aider l'ACOSS dans ses missions de Sécurité

	cf. CRT	2.3.1.1 Organisation du lot
---	---------	-----------------------------

2.2 Description du périmètre

Le lot Sécurité concerne l'ensemble des activités de sécurité de la DSI ACOSS et en particulier :

- Définition et mise en œuvre de :
 - Solutions de sécurité (infrastructures, composants, progiciels etc...),
 - Architectures sécurisées du SI,
 - Processus opérationnels de détection et de réaction aux incidents.
- Accompagnement des équipes MOE métier pour la conception et la réalisation d'applications sécurisées et résilientes,
- Traitements des incidents de sécurité et surveillance du SI,
- Détection des vulnérabilités du SI et suivi des corrections des vulnérabilités
- Travaux sur la résilience opérationnelle en particulier dans son volet cyber.

Le candidat décrira dans sa réponse, sa capacité en termes de moyens humains, profils potentiels qu'il sera capable de mobiliser pour répondre aux besoins de Sécurité

	cf. CRT	2.3.1.2 Couverture et périmètre spécifique au lot
---	---------	---

2.3 Technologie

Les activités de l'expertise technique nécessitent donc la connaissance des environnements techniques qui concourent au périmètre décrit ci-après.

Pilier Protection :

- Gestion des identités et des accès :
 - Annuaires AD,
 - Annuaire d'entreprise et des applications LDAP v3,
 - Connecteur de synchronisation LDAP,
 - Workflow d'habilitations basé sur l'approche RBAC,
 - Protocole de fédération d'identité basée sur SAML (ADFS, AWS et InterOPS),
 - Solution MFA de type carte à puce et OTP (poste de travail, VPN nomade, Cloud public et privé, MS O365),
 - SSO client basé sur E-SSO d'Atos,
 - FreeRadius adossé à AD et à LDAP,
 - Produits ACOSS de gestion des identités et des accès ;

- TBC.
- Sécurisation API :
 - Sécurisation de web services (SOAP, REST) par une solution d'API management configurée avec les mécanismes Oauth2, OpenID Connect et compatible avec les jetons JWT + SAML.
- Sécurité de la donnée :
 - Solution de gestion d'intégrité et de signature + horodatage (DSS),
 - PKI et boîtiers HSM (séquestre de clefs),
 - Coffre-fort électronique (Vault, keepass),
 - Chiffrement du transport TLS,
 - Chiffrement de la donnée stockée (cryptographie symétrique, cryptographie asymétrique),
 - Solution d'anonymisation de données persistantes/statiques (cas des jeux de données/tests) pour les bases de données relationnelles et fichiers plats.
- Sécurité des infrastructures :
 - Composants de filtrage ;
 - Firewall réseau pour le filtrage TCP/IP, URL ou filtrage par 5dentité au niveau AD
 - Firewall applicatif/ WAF,
 - Protection de la messagerie :
 - VPN ou portail de connexion SSL, VPN Ipsec, ZTNA, SASE
 - Sondes IDS/IPS,
 - Anti-DDOS on prem
 - Outils de gestion et administration de la Sécurité ;
 - Console d'administration centralisée des constructeurs. Outils constructeurs : SmartConsole, Fortimanager, FortiAnalyzer, FortiAuthenticator, F5, Cisco ASDM/FMG,
 - Outils d'orchestration des stratégies de sécurité réseau.
 - Outils de supervision et d'analyse de logs
 - Sécurité des points d'accès/terminaux ;
- EPP (Endpoint Protection Platform) et EDR (Endpoint Detection and Response)
 - Passerelle de messagerie (Antivirus, SPF, DKIM et DMARC, antispam),
 - Proxy internet sortant (antivirus, analyse de réputation),
 - Sandbox (AMP),
 - Chiffrement des postes de travail (Sophos safeguard).
- Solution cloud privée ;
 - Technologie Kubernetes/OpenShift
 - Filtrage CNI (Cilium, Calico)
 - OPA/Gatekeeper
- Outil d'automatisation de déploiement, de mise à l'échelle (Ansible, terraform) et de gestion des applications conteneurisées (basé sur Kubernetes),
- Plateforme d'Intégration Continue (Jenkins, AWC),

- Application Centric Infrastructure (ACI / Cisco).
- Traçabilité des équipements de sécurité ;
- Brique ELK pour l'analyse de logs et journaux des équipements de sécurité.
- Sécurité dans le cycle de développement :
 - Usine logicielle (Gitlab, Jenkins, Nexus, SonarQube, OWASP Dependency check, OWASP Track, Trivy, Snyk, OWASP Zap),
 - Politiques techniques de sécurité par directives thématiques.
- Sécurité Office 365 :
 - MS Office 365,
 - ADFS,
 - MobileIron UEM,
 - MobileIron Access.

Pilier détection/réponse :

- Gestion des incidents :
 - Développement interne basé sur script Python et Bash ;
 - Outillage ;
 - Détection : IDS, IPS, Analyse comportementale endpoint et réseau, WAF,
 - Gestion des logs: Kibana, fluentd, opensearch, rsyslog, Sekoia
 - Gestion d'incident : TheHive, Cortex, MISP, ORC, Velociraptor, Sekoia
 - Automatisation : Playbook,
 - ThreatIntel : OSINT, Recorded Futur
 - Gestion de version : client Git Serveur,
 - Conteneurs et virtualisation,
 - SIEM.
- Supervision des vulnérabilités :
 - 70.000 assets supervisés
 - Environnement Windows, Linux, Cloud privé, Infrastructure et réseaux.
 - Solutions de supervision des vulnérabilités,
 - Solutions de surveillance de la surface d'attaque,
 - Solutions de corrélations des résultats d'audits et d'analyses
 - Développements de script, requêtes et exploitations d'API
- Audits de sécurités et tests d'intrusion :
 - Tests d'intrusions sites Internet et Intranet, API et applications mobiles
 - Audits de sécurités OS, réseaux, applications, IA, ...
 - Outils d'audits de configuration
 - Outils de tests d'intrusion
 - Outils de prise d'empreinte
 - Outils d'exploitation des vulnérabilités

- Outils de maintien d'accès
- Outils de reporting
- Scripting

Dans sa réponse le candidat indiquera le nombre d'experts confirmés présents au sein de son organisation et démontrera qu'il est en capacité de répondre aux besoins d'experts liés aux technologies de l'ACOSS

 cf. CRT	2.3.1.3 Technologies spécifiques au lot
--	--

2.4 Enjeux, Projets et évolutions à venir

Au-delà de ces enjeux généraux du SDSI, ce lot est porteur des enjeux spécifiques suivants :

Dans le cadre de la prochaine période conventionnelle, les enjeux de sécurité pour la chaîne opérationnelle portent principalement sur 4 axes :

- Accélérer la mise en conformité de la branche vis-à-vis des différents référentiels et textes réglementaires applicables :
 - Poursuivre et finaliser la démarche de mise en conformité relative au statut d'OSE,
 - Développer la confiance numérique à destination des usagers du SI de la branche.
- Renforcer la protection des actifs critiques nécessaires aux missions essentielles de la branche :
 - Renforcer et structurer la sécurité des infrastructures et des applications,
 - Renforcer la sécurité dans les projets liés aux systèmes d'information,
 - Refondre la gestion des identités et des accès pour l'adapter à l'évolution des activités et à la transformation numérique de la branche.
- Accroître les capacités à détecter, à s'adapter et à réagir à une menace évolutive sur tous les périmètres pertinents :
 - Renforcer les moyens humains et techniques de détection et de réaction pour réagir à des menaces nouvelles et multiples,
 - Se mettre en capacité de gérer les crises majeures.
- Garantir la résilience des missions de la branche face aux sinistres majeurs :
 - S'organiser dans une logique d'amélioration continue de la continuité d'activité,
 - Mettre en œuvre la stratégie de résilience et tester les dispositifs mis en œuvre.

L'utilisation de services de sécurité est clairement identifiée pour faciliter et accélérer l'atteinte des objectifs de la branche.

Dans ce cadre, le candidat devra aider l'ACOSS par :

- L'apport d'expertise sécurité pour la production d'études stratégiques et techniques,
- Le renforcement des équipes internes par l'apport de compétences au cœur des équipes de sécurité,
- Le développement de services.

 cf. CRT	2.3.1.4 Enjeux, Projets et évolutions spécifiques au lot
--	---

2.5 Risques

Au regard des risques spécifiques exposés ci-dessus, l'ACOSS pose pour ce lot des exigences spécifiques, relatives notamment au niveau de certification des titulaires et de leurs intervenants et la localisation des prestation, assorties de possibilités de contrôles renforcées.

2.5.1 La sensibilité des données

Description :

Les prestations attendues par ce lot couvrent l'ensemble des aspects de sécurité présents et futurs du Système d'Information de l'ACOSS.

Les titulaires de ce lot pourront donc avoir à connaître ou manipuler des données représentant directement le niveau de sécurité du système d'Information, comme les failles de sécurités ou les règles de configurations des équipements de sécurité.

Impact :

Une fuite de données sensibles pourrait constituer un risque majeur pour la sécurité de l'ACOSS.

Le secteur public est une cible privilégiée pour les cyberattaques (ransomware, espionnage). Les conséquences d'une faille peuvent impacter la confiance des citoyens, la souveraineté nationale ou la stabilité des services publics (ex : blocage des systèmes de santé ou de transports).

Mesures particulières :

Les exigences de sécurité des CCAT et CCTP sont particulièrement à prendre en considération pour ce lot, et plus particulièrement les clauses relatives au Ressources Humaines et Contrôles d'accès (Chapitre 8), à la Gestion des biens et des données (Chapitre 9), et au Traitement des Incidents de Sécurité (Chapitre 10).

Plus particulièrement, les titulaires de ce lot devront privilégier l'utilisation de solutions souveraines (hébergement en France, logiciels labellisés SecNumCloud, etc.) et éviter les outils ou sous-traitants soumis à des législations extra-européennes (ex : Cloud Act américain).

A la demande de l'ACOSS, il pourra être demandé des vérifications des casiers judiciaires et des liens avec des entités étrangères pour les intervenants des titulaires ainsi que des accords de confidentialité renforcés, ainsi que des engagements de non-divulgation à des tiers, y compris aux autorités étrangères.

Dans le cas de stockage de données de l'ACOSS dans des équipements des titulaires, ces équipements devront être chiffrés par des algorithmes approuvés par l'ANSSI, et l'accès à ces données strictement limité selon le droit d'en connaître et tracé de manière sécurisé.

Enfin, les intervenants du Titulaire ayant à connaître des données sensibles de l'ACOSS devront être sensibilisés à la nature de ces données, au risque de fuite et aux mesures de précautions à mettre en œuvre. Cette sensibilisation pour être faite par l'ACOSS mais il incombe aux titulaires de s'assurer de sa bonne compréhension par les intervenants.

- **E-CRISE-RESP-01** : Le service inclut la mise à disposition en cas de crise d'un responsable qui sera le pilote opérationnel de l'équipe d'analyse et le point de contact privilégié vis à vis du client.

2.5.2 La confidentialité des informations

Description :

Dans le cadre des prestations attendues par ce lot, les titulaires de ce lot pourront avoir à connaître des informations confidentielles touchant ou non à la sécurité du système d'informations comme par exemple des orientations stratégiques de l'ACOSS ou l'impact d'incidents de sécurité.

Impact :

Une fuite d'informations confidentielles pourrait constituer un préjudice majeur pour l'ACOSS et les usagers avec le même impact que pour la sensibilité des données.

Mesures particulières :

Les exigences de sécurité des CCAT et CCTP sont particulièrement à prendre en considération pour ce lot, et plus particulièrement les clauses relatives aux Ressources Humaines et Contrôles d'accès (Chapitre 8), à la Gestion des biens et des données (Chapitre 9), et au Traitement des Incidents de Sécurité (Chapitre 10).

Plus particulièrement, les titulaires de ce lot devront disposer d'un système de classification interne (ex : "Interne", "Réservé", "Confidentiel"), ou repris de celui en vigueur au sein de l'ACOSS. Les documents confidentiels devront être clairement identifiés et marqués comme tel (ex : "Confidentiel – Diffusion restreinte") et leur diffusion autorisée uniquement avec les personnes explicitement désignées par l'organisation ayant le besoin d'en connaître.

La diffusion des informations confidentielles se fera à travers un canal sécurisé, après chiffrement, et à l'exclusion de tout canal grand public (Gmail, WhatsApp, etc.), support amovible (clés USB, disques durs externes) ou impressions non contrôlées. Les solutions mises à disposition par les services de la DINUM ou validées par l'ANSSI seront à privilégier.

Les titulaires de ce lot s'engagent à ne pas utiliser les informations dont ils auront connaissance dans le cadre de ce lot pour d'autres missions ou clients, et pourront avoir à accepter une clause explicite sur la non-divulgence des informations confidentielles, même après la fin du contrat.

L'accès aux documents confidentiels se fera uniquement à partir d'un compte individuel, dans un environnement sécurisé (écrans protégés des regards, ...), et sera tracé pour toutes ouvertures, modifications et transferts, avec un archivage sécurisé des traces.

Les titulaires s'assureront de la désactivation immédiate des accès en cas de fin de mission ou de changement d'intervenants.

Les collaborateurs et sous-traitants du titulaire ayant accès à des données confidentielles de l'ACOSS devront être formés ou sensibilisés sur les risques liés à la divulgation involontaire (ex : discussions en public, écrans visibles).

Enfin, Les titulaires de ce lot signaleront à l'ACOSS tout doute sur une divulgation accidentelle dès qu'ils en auront connaissance et lanceront une analyse des causes en cas de perte ou de mauvaise manipulation d'informations confidentielles. Cette analyse sera communiquée à l'ACOSS.

2.5.3 La manipulation de système de protection et de détection d'incidents

Description :

Dans le cadre des prestations attendues par ce lot, les titulaires de ce lot pourront avoir à intervenir dans le cadre de projets ou d'activités courantes sur les systèmes contribuant à la protection du Système d'Information de l'ACOSS ou à la détection d'incidents de sécurité.

Impact :

Une mauvaise manipulation de ces systèmes pourrait constituer un risque de sécurité majeur pour l'ACOSS.

Mesures particulières :

Les exigences de sécurité des CCAT et CCTP sont particulièrement à prendre en considération pour ce lot, et plus particulièrement les clauses relatives aux Ressources Humaines et Contrôles d'accès (Chapitre 8), à la Gestion des biens et des données (Chapitre 9), et au Traitement des Incidents de Sécurité (Chapitre 10).

Plus particulièrement, les intervenants des titulaires de ce lot devront disposer d'une expérience significative sur les technologies mises en œuvre par l'ACOSS. Cette expérience sera formalisée chaque fois que cela est possible par une formation ou une certification sur la technologie concernée ou à défaut sur une technologie comparable.

Les actions sensibles telles que définies par l'ACOSS seront réalisées exclusivement par des intervenants approuvés par l'ACOSS en utilisant des droits limités aux seuls besoins techniques de l'action, en excluant à priori l'utilisation de compte aux droits étendus de type root ou administrateurs.

Les interventions sur des modifications de règle de détection ou de configuration de protection, si elles doivent être faites en autonomie par les titulaires des lots devront faire l'objet de précautions particulières dont notamment une simulation des impacts, une procédure écrite et validée par l'ACOSS de réalisation et de retour arrière, une double validation des commandes, un enregistrement automatique et immuable de toutes les commandes exécutées sur les outils de sécurité (ex : logs des changements de configuration). Chaque fois que cela est possible, les interventions seront testées préalablement dans un environnement hors production.

Les incidents survenus lors d'interventions, mêmes mineurs, feront l'objet d'une analyse a posteriori. Cette analyse sera partagée avec l'ACOSS.

Dans sa réponse, le candidat devra préciser les mesures particulières, moyens et les processus qu'il mettra en œuvre afin de réduire, voire éliminer, les 3 risques identifiés par l'ACOSS

 cf. CRT	2.3.2. Risques spécifiques au lot
--	-----------------------------------

2.6 Certifications

Code UO	Libellé	Souhaits de certification/qualification de la société	Souhaits de certification/qualification des intervenants
UO_5_E_SEC_PIL_1	Appui à la planification stratégique sécurité		Certification type CISSP, CISM ou équivalent
UO_5_E_SEC_PIL_2	Pilotage de projet sécurité - environnements sensibles		Certification type CISSP, CISM ou équivalent
UO_5_A_SEC_AUD_PASSI	Tests d'intrusion PASSI	PASSI (ou en cours de certification)	Certification avancée en sécurité offensive (OSCP ou équivalent).
UO_5_A_SEC_FRS_P	Expertise Forensic	PRIS (ou en cours)	Certification avancée en digital forensic (Computer

			Hacking Investigator ou équivalent)	Forensic
--	--	--	--	----------

Le candidat devra indiquer dans sa réponse les certifications valides qu'il possède, ou que certains de ses collaborateurs possèdent (avec le dénombrement associé), qui lui semblent pertinentes sur le périmètre considéré en complément des souhaits exprimés dans le tableau ci-dessus.

 cf. CRT	2.3.4.4 Formation et certification des collaborateurs
--	---

3 Description des prestations attendues

3.1 Liste des prestations attendues

La liste des prestations attendues par type de d'Unité d'œuvre et par phase est la suivante :

Code UO	Type UO	Phase/Thématique	Libellé	Profil
UO_5_G_INIT_LOT	Globalisé	Initialisation	Initialisation du Lot	
UO_5_G_INIT_SERV	Globalisé	Initialisation	Initialisation d'un service	
UO_5_G_REV_LOT	Globalisé	Réversibilité	Réversibilité du lot	
UO_5_G_REV_SERV	Globalisé	Réversibilité	Réversibilité d'un service	
UO_5_E_SEC_PIL_1	Expertise	Pilotage	Appui à la planification stratégique sécurité	Chef de projet technique.
UO_5_E_SEC_PIL_2	Expertise	Pilotage	Pilotage de projet sécurité - environnements sensibles	Chef de projet technique.
UO_5_E_SEC_RES_1	Expertise	Résilience / Continuité	Accompagnement au pilotage de la démarche de mise en place de PCA (BIA, PCM, ...)	Expert Continuité d'activité.
UO_5_E_SEC_RES_2	Expertise	Résilience / Continuité	Expertise PCA/PCI/Cyber résilience	Expert cyber sécurité /
UO_5_E_SEC_ISP_1	Expertise	Protection du SI	Accompagnement sécurité de projets	Expert sécurité informatique.
UO_5_E_SEC_ISP_2	Expertise	Protection du SI	Expertise sécurité applicative et sécurité du code	Architecte Sécurité technique
UO_5_E_SEC_ISP_3	Expertise	Protection du SI	Accompagnement sécurité applicative, Cloud et DevSecOPS	Architecte Sécurité technique
UO_5_E_SEC_UAD	Expertise	Protection du SI	Expertise anonymisation des données	Architecte Cloud
UO_5_E_SEC_SYS	Expertise	Protection du SI	Expertise sécurité des systèmes (OS, BDD, MiddleWare, K8S, OPK PIC, ACI)	Expert technique/Sécurité en charge de projets d'anonymisation.
UO_5_E_SEC_INF	Expertise	Protection du SI	Expertise sécurité des réseaux (FW, VPN, WAF, IDS / IPS, SDWAN, RP etc ..)	Expert technique/Sécurité spécialisé en Sécurité des systèmes.
UO_5_E_SEC_SOL	Expertise	Protection du SI	Expertise autres solutions de sécurité (AV, XDR, O365, CASB, PKI, Chiffrement, etc ...)	Expert technique/Sécurité spécialisé en Sécurité des réseaux.
UO_5_E_SEC_IAM_1	Expertise	Protection du SI	Evolutions et MCO des produits de gestion des identités et des accès	Expert technique/Sécurité.
UO_5_E_SEC_AUD	Expertise	Cyberdéfense du SI	Expertise Audits et tests de vulnérabilité	Analyste/concepteur, Auditeur Sécurité. Pentesteur
UO_5_E_SEC_ANV	Expertise	Cyberdéfense du SI	Cyber analyse VOC	Expert cybersécurité.
UO_5_E_SEC_ANS	Expertise	Cyberdéfense du SI	Cyber analyse SOC	Expert cybersécurité.
UO_5_E_SEC_ANC	Expertise	Cyberdéfense du SI	Cyber analyse CSIRT	Expert cybersécurité.
UO_5_E_SEC_ANT	Expertise	Cyberdéfense du SI	Cyber analyste Threat Intelligence	Expert cybersécurité.

UO_5_E_SEC_SCI	Expertise	Cyberdéfense du SI	Evolution fonctionnelle ou technique du SOC	Expert cybersécurité.
UO_5_E_SECSY	Expertise	Cyberdéfense du SI	Conseil Cybersécurité	Expert cybersécurité.
UO_5_S_SEC_FIR_ABO	Service	Cyberdéfense du SI	Force d'Intervention Rapide - Abonnement	
UO_5_S_SEC_FIR_HP	Service	Cyberdéfense du SI	Force d'Intervention Rapide - Intervention HORS qualification PRIS	
UO_5_S_SEC_FIR_P	Service	Cyberdéfense du SI	Force d'Intervention Rapide - Intervention sous qualification PRIS	
UO_5_S_SEC_DSS_TMA	Service	Protection du SI	Digital Signature Service - TMA	
UO_5_S_SEC_UAD_TMA	Service	Protection du SI	Usine d'Anonymisation des Données - TMA	
UO_5_S_SEC_UAD_INTEG	Service	Protection du SI	Usine d'Anonymisation des données - Intégration	
UO_5_A_SEC_AUD	Service	Cyberdéfense du SI	Test d'intrusion	
UO_5_A_SEC_AUD_PASSI	Service	Cyberdéfense du SI	Test d'intrusion sous qualification PASSI	
UO_5_A_SEC_FRS	Service	Cyberdéfense du SI	Service Forensic	
UO_5_A_SEC_FRS_P	Service	Cyberdéfense du SI	Service Forensic sous qualification PRIS	
UO_5_A_SEC_THI	Service	Cyberdéfense du SI	Service Threat Intelligence	
UO_5_A_T_AST	Activité	Astreinte	Astreinte	
UO_1_A_A_TDHNO	Activité	Astreinte	Travail décalé en HNO	

3.2 Détail des prestations attendues

3.2.1 Globalisé

3.2.1.1 Initialisation

Code UO	UO_5_G_INIT_LOT
Libellé UO	Initialisation du Lot
Type d'UO	Globalisé
Phase	Initialisation
Description	La prestation établit : (cf. CCTP commun modalité d'exécution) ▪ L'organisation des acteurs du titulaire ; ▪ Le récapitulatif de la documentation et des logiciels ; ▪ La communication, et les instances avec les responsables ACOSS ; ▪ Les processus, méthodes, normes, et procédures ; ▪ Les environnements et les outils.
Entrant	▪ Notification Accord Cadre et DCE
Livrable	▪ Le PAQ instancié du lot ; ▪ Le PAS instancié du lot ; ▪ La réponse au questionnaire sécurité initié par l'ACOSS ; ▪ La documentation du lot (dont document d'accueil, actualisation de la documentation de référence, dans le respect des normes documentaires en vigueur à la DSI) ; ▪ Les métriques industrielles ou méthodes d'estimation des charges applicables ; ▪ le plan de réversibilité du lot avec son coût.
Complexité	NA

Profils et compétences associés	A définir par le titulaire en s'appuyant sur la grille des profils (Annexe : « Grille des profils »)
--	--

Code UO	UO_5_G_INIT_SERV
Libellé UO	Initialisation d'un service
Type d'UO	Globalisé
Phase	Initialisation
Description	La phase d'initialisation d'un service consiste à : - Prendre en compte le périmètre du service - Décrire le processus d'utilisation de ce service - Identifier l'équipe en charge de ce service
Entrant	- Cadre contractuel. - Périmètre d'intervention et engagements de services.
Livrable	- Document descriptif des personnes participants au centre de service et son organisation. - Processus de gestion du service Cette UO est utilisé pour un des services suivants pour une charge de 5 jours - Service Usine d'Anonymisation des Données - Service Digital Signature Service
Complexité	NA
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

3.2.1.2 Réversibilité

Code UO	UO_5_G_REV_LOT
Libellé UO	Réversibilité du lot
Type d'UO	Globalisé
Phase	Réversibilité
Description	La prestation établit pour le transfert vers le repreneur du lot : - L'organisation des acteurs du titulaire, - Le récapitulatif de la documentation et des logiciels, - La communication, et les instances avec les responsables ACROSS, - Les processus, méthodes, normes, et procédures, - Les environnements et les outils.
Entrant	Le plan de réversibilité
Livrable	Un plan de réversibilité mis à jour,

	Un bilan de réversibilité une fois l'ensemble des réversibilités du lot réalisées.
Complexité	NA
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »)

Code UO	UO_5_G_REV_SERV
Libellé UO	Réversibilité d'un service
Type d'UO	Globalisé
Phase	Réversibilité
Description	La prestation établit pour le transfert vers le repreneur : - L'organisation des acteurs du titulaire, - Le récapitulatif de la documentation et des logiciels, - La communication, et les instances avec les responsables ACOSS, - Les processus, méthodes, normes, et procédures, - Les environnements et les outils.
Entrant	- Le plan de réversibilité, - Périmètre et niveaux de services tels que définis au moment de la réversibilité.
Livrable	- Un plan de réversibilité mis à jour, - Un bilan de réversibilité une fois l'ensemble des réversibilités du lot réalisées.
Complexité	NA
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »)

3.2.2 Expertise

Il est attendu du candidat une capacité à mobiliser des équipes expérimentées pour la production de livrables sur les domaines de la sécurité précisés après.

- Les interventions pourront se faire sur l'ensemble des sites de l'URSSAF ou de l'ACOSS. Ces derniers sont précisés suivant les unités d'œuvre mais peuvent être amenés à évoluer sur les 4 prochaines années.

Code UO	UO_5_E_SEC_PIL_1
Libellé UO	Appui à la planification stratégique sécurité.
Type d'UO	Expertise.
Phase	Pilotage
Description	- Assiste le sous-directeur dans la planification stratégique des activités et des projets de sécurité, - Assure la préparation des instances de gouvernance de la sécurité,

	- Détecte les dysfonctionnements et propose et/ou engage des actions correctrices et en assure le suivi, - Coordonne des projets, des équipes et des interlocuteurs multiples,
Entrant	- Connaît les méthodes et outils de gestion de projets, - Connaît les principes et standards de sécurité.
Livrable	- Supports de comités, - Planning, - Suivi des actions, du budget.
Complexité	Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevée permettant l'accès à des informations sensibles.
Bassin Géographique Prévisionnel	Tous les sites ACOSS, particulièrement Lyon et Montreuil.
Profils et compétences associés	Chef du projet technique Des qualifications individuelles en sécurité sont un plus

Code UO	UO_5_E_SEC_PIL_2
Libellé UO	Pilotage de projet sécurité - environnements sensibles.
Type d'UO	Expertise.
Phase	Pilotage
Description	- Planification de l'activité et des livrables, - Gérer le budget et les commandes, - Assurer la relation client avec la chaîne fonctionnelle de sécurité (reporting, anticipation et proactivité ...), - Connaissance technique et fonctionnelle générale des composants de sécurité du projet, - Maîtrise des techniques et outils de gestion de projet (planning, suivi budgétaire, reporting), - Coordination des équipes et interlocuteurs multiples.
Entrant	- Connaît les méthodes et outils de gestion de projets, - Connaît les principes et standards de sécurité.
Livrable	- Support de comité, - Synthèse des solutions techniques, - Planning, - Plan de gestion des risques, - Suivi des actions, du budget.
Complexité	Moyen, Complexe,
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevée permettant l'accès à des informations sensibles.
Bassin Géographique prévisionnel	Tous les sites ACOSS.

Profils et compétences associés	Chef de projet technique. . Des qualifications individuelles en sécurité sont un plus.
--	---

Code UO	UO_5_E_SEC_RES_1
Libellé UO	Accompagnement au pilotage de la démarche de mise en place de PCA (BIA, PCM, ...).
Type d'UO	Expertise.
Phase	Résilience / Continuité.
Description	- Planification de l'activité et des livrables, - Coordination des équipes et interlocuteurs multiples (articulation métier / technique), - Animation de réunions techniques et organisationnelles, - Optimisation de la documentation, - Réalisation de Bilan d'Impact sur les Activités, - Réalisation de Plans de Continuité Métier, - Réalisation de plans de test, - Réalisation de plans d'amélioration continue.
Entrant	- Connaît les méthodes et outils de gestion de projets, - Connaît les principes et standards de continuité d'activité.
Livrable	- Supports de comités, - Planning, - Suivi des actions, - Documentation continuité : PCA BIA PCM, - Plans de tests, - Plans d'amélioration, - BIA, - PCM.
Complexité	Moyen, Complexe.
Spécificité de l'environnement technique	N/A.
Profils et compétences associés	Expert Continuité d'activité. Des qualifications individuelles en sécurité sont un plus.

Code UO	UO_5_E_SEC_RES_2
Libellé UO	Expertise PCA/PCI/Cyber résilience.
Type d'UO	Expertise.
Phase	Résilience / Continuité.
Description	- Capacité à articuler cybersécurité et gestion de continuité d'activité, - Planification de l'activité et des livrables, - Connaissance technique et fonctionnelle en cyber sécurité, - Connaissance technique et fonctionnelle en cyber résilience, - Coordination des équipes et interlocuteurs multiples, - Maîtrise des techniques et outils de gestion de projet.
Entrant	Connaît les méthodes et outils de gestion de projets,

	▪ Connaît les principes et standards de cybersécurité, ▪ Connait les principales normes : EBIOS ISO/IEC 27005 27001 27032.
Livrable	▪ Supports de comités, ▪ Planning, ▪ Suivi des actions, ▪ Documentation continuité / résilience : PCA PCI PCR, ▪ Plans de tests, ▪ Plans d'amélioration,
Complexité	Moyen, Complexe.
Spécificité de l'environnement technique	N/A.
Bassin géographique prévisionnel	▪ Tous les sites ACOSS.
Profils et compétences associés	Expert cyber sécurité / Expert sécurité informatique. Des qualifications individuelles en résilience (ISO 22301) et qualité/méthode sont un plus.

Code UO	UO_5_E_SEC_ISP_1
Libellé UO	Accompagnement sécurité de projets.
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Réaliser des ateliers d'accompagnements de MOE pour sécuriser leurs projets (identification des cas d'usage, cadrage et identification des exigences de sécurité à appliquer, participation aux ateliers en toute autonomie, échanges avec les architectes transverses, application de pattern d'architecture sécurisé, suivi de la prise en compte par la MOE, contrôle de conformité des exigences applicables, reporting et communication) ▪ Documenter l'accompagnement de chaque projet suivi par une prise de notes brute et synthétiques au fur et à mesure et selon les jalons du projet ▪ Enrichir le catalogue de mesures de sécurité technique, développer la conformité ▪ Être force de propositions pour traiter la sécurité de nouveaux cas d'usage, ▪ Contribuer aux études techniques (seul ou en appui des architectes de sécurité),
Entrant	▪ Connaît les principes et standards de sécurité, ▪ Maîtrise des sujets techniques et capacité d'échanger avec les experts techniques sur un grand panel de technologies, ▪ Connait l'infrastructure des SI et leurs composants, ▪ Connait les principes et standards de développement applicatif, ▪ Connait l'intégration de la sécurité dans un projet et les relations avec les MOE, ▪ Sens du collectif pour la coopération avec les équipes d'architecture et de sécurité, ▪ Dispose de bonnes capacités de communication orale et écrite,

	▪ Effectue de la veille technologique.
Livrable	▪ Schémas d'architecture sécurisée, ▪ Fiche de sécurité du projet, ▪ Suivi des actions et reporting,
Complexité	Moyen, Complexe.
Spécificité de l'environnement technique	▪ La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles, ▪ L'ensemble des environnements techniques de l'ACOSS sont concernés.
Bassin géographique prévisionnel	▪ Tous les sites ACOSS.
Profils et compétences associés	Architecte Sécurité technique.

Code UO	UO_5_E_SEC_ISP_2
Libellé UO	Expertise sécurité applicative et sécurité du code.
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Réaliser des accompagnements de MOE dans leur phase de réalisation (développement de livrables) pour sécuriser leurs projets (sécurité dans le code, bonnes pratiques, expertise pour remédier à des vulnérabilités identifiées), ▪ Être force de propositions pour aider les développeurs et des équipes de tests, ▪ Contribuer aux travaux permettant de proposer des tests de sécurité aux développeurs, ▪ Contribuer aux travaux permettant à des équipes de tests d'effectuer une recette sécurité.
Entrant	▪ Connaît les principes et standards de sécurité applicative, ▪ Dispose de solides connaissances dans le développement applicatif, ▪ Connaît les outils de tests de sécurité (SCA, SAST, DAST, IAST), ▪ Connaît la mise en œuvre de tests de sécurité et le suivi des développeurs sur la prise en compte des corrections de sécurité, ▪ Dispose de bonnes capacités de communication orale et écrite, ▪ Effectue de la veille technologique.
Livrable	▪ Fiche de sécurité du projet, ▪ Suivi des actions et reporting, ▪ Tableau de bords des vulnérabilités des projets.
Complexité	Moyen, Complexe.
Spécificité de l'environnement technique	▪ La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles. ▪ L'environnement technique : AngularJS, Java, SCA, SAST, DAST, IAST, PIC, K8S.

Bassin géographique prévisionnel	Tous les sites ACOSS.
Profils et compétences associés	Architecte Sécurité technique. Une certification avancée en sécurité offensive serait un plus.

Code UO	UO_5_E_SEC_ISP_3
Libellé UO	Expertise sécurité applicative, Cloud et DevSecOPS.
Type d'UO	Expertise.
Phase	Protection du SI.
Description	- Réaliser les travaux d'intégration sécurisée des applications sur les offres Cloud - Réaliser des travaux de sécurisation des offres Cloud, - Réaliser des travaux de sécurité sur les processus liés au Cloud, - Être force de propositions pour traiter la sécurité de nouveaux cas d'usage, - Contribuer aux études techniques (seul ou en appui des architectes de sécurité), - Enrichir le catalogue de mesures de sécurité.
Entrant	- Connaît les principes et standards de sécurité, - Dispose de solides connaissances techniques Cloud, - Connaît l'infrastructure des SI et leurs composants, - Connaît des infrastructures Cloud, - Connaît les principes et standards de développement applicatif lié au Cloud, - Connaît l'intégration de la sécurité dans un projet et les relations avec les MOE, - Dispose de bonnes capacités de communication orale et écrite, - Effectue de la veille technologique.
Livrable	- Schémas d'architecture sécurisée, - Fiche de sécurité du projet, - Suivi des actions et reporting.
Complexité	Moyen, Complexe.
Spécificité de l'environnement technique	- La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles, - L'environnement technique : Cloud interne, Cloud externe, PAAS, IAAS, SAAS.
Bassin géographique prévisionnel	Tous les sites ACOSS.
Profils et compétences associés	Architecte Cloud avec expérience en sécurité. Une certification CCSP serait un plus.

Code UO	UO_5_E_SEC_UAD
Libellé UO	Expertise anonymisation des données.
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Mettre en œuvre les règles d'anonymisation qui seront réutilisables pour toutes les applications (catalogue de règles communes), ▪ Préparer, paramétrer et tester la bonne anonymisation pour le périmètre des données du projet, ▪ S'assurer de l'adéquation des résultats des tests et de l'expression de besoin, ▪ Faire valider par le demandeur l'adéquation entre sa demande et le résultat, ▪ Améliorer si besoin les performances du traitement d'anonymisation ▪ Réaliser et optimiser l'anonymisation des données, ▪ Lancer le traitement d'anonymisation sur l'ensemble des données à rendre anonymes, ▪ Obtenir le PV de recette du client sur le correct fonctionnement des tests fonctionnels, ▪ Capitaliser au sein de l'équipe en vue de créer une boucle d'amélioration continue.
Entrant	▪ Description des applications et écosystèmes à anonymiser : schémas d'architecture, flux de données, référentiels de données etc., ▪ Fiche d'anonymisation initiée avec la MOE cliente.
Livrable	▪ Règles d'anonymisation (développement dans l'outil), ▪ Projet d'anonymisation (configuration dans l'outil), ▪ Document de recette répondant aux besoins de la MOE Cliente, ▪ Assistance et support technique à l'équipe projet Acoss, ▪ Fiche d'anonymisation à jour (si nécessaire).
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	▪ Outil d'anonymisation Dot-A de l'éditeur Arcad Software, ▪ SGBD : postgresql et oracle + big data.
Bassin géographique prévisionnel	▪ Tous les sites ACOSS (déplacements très ponctuels).
Profils et compétences associés	Expert technique/Sécurité en charge de projets d'anonymisation.

Code UO	UO_5_E_SEC_SYS
Libellé UO	Expertise sécurité des systèmes (OS, BDD, MiddleWare, K8S, OPK PIC, ACI).
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Initialisation : Prise en compte des prérequis fournis par l'ACOSS, ▪ Etude comparative des solutions, ▪ Mise en œuvre de l'environnement de tests (élaboration du plan détaillé de la mise en œuvre de la solution en test en tenant compte que la mise en œuvre de la solution impacte au minimum la production de l'ACOSS, suivi de la mise en œuvre de tests), ▪ Mise en œuvre de l'environnement d'intégration (élaboration du plan d'intégration de la solution dans l'environnement de production de l'ACOSS, suivi de l'intégration), ▪ Mise en œuvre de la nouvelle fonction validée, ▪ Réalisation et déroulement des tests unitaires dans le cadre de la nouvelle fonction et analyse, ▪ Intégration et recette usine de la nouvelle fonction, ▪ Assurance qualité, ▪ Création de la documentation technique et d'utilisation, ▪ Rédaction du rapport final,
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Exécutions (binaires, librairies, etc.), ▪ Maquettes et prototypes, ▪ Documentation technique, ▪ Jeux de tests validés, ▪ Support technique, ▪ Rapport final comprenant : L'intégration de la nouvelle fonction déployée, Le processus de déploiement et d'utilisation de la nouvelle fonction, Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés, ▪ Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	▪ Voir Chapitre Environnement sécurité.
Bassin géographique prévisionnel	▪ Nantes, Marseille, Toulouse.
Profils et compétences associés	Expert technique/Sécurité spécialisé en Sécurité des systèmes.

Code UO	UO_5_E_SEC_INF
Libellé UO	Expertise sécurité des réseaux (FW, VPN, WAF, IDS / IPS, SDWAN, RP etc. ...).
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Initialisation : Prise en compte des prérequis fournis par l'ACOSS, ▪ Etude comparative des solutions, ▪ Mise en œuvre de l'environnement de tests (élaboration du plan détaillé de la mise en œuvre de la solution en test en tenant compte que la mise en œuvre de la solution impacte au minimum la production de l'ACOSS, suivi de la mise en œuvre de tests), ▪ Mise en œuvre de l'environnement d'intégration (élaboration du plan d'intégration de la solution dans l'environnement de production de l'ACOSS, suivi de l'intégration), ▪ Mise en œuvre de la nouvelle fonction validée, ▪ Réalisation et déroulement des tests unitaires dans le cadre de la nouvelle fonction et analyse, ▪ Intégration et recette usine de la nouvelle fonction, ▪ Assurance qualité, ▪ Création de la documentation technique et d'utilisation, ▪ Rédaction du rapport final.
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Exécutions (binaires, librairies, etc.), ▪ Maquettes et prototypes, ▪ Documentation technique, ▪ Jeux de tests validés, ▪ Support technique, ▪ Rapport final comprenant : L'intégration de la nouvelle fonction déployée, Le processus de déploiement et d'utilisation de la nouvelle fonction, Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés. ▪ Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	▪ Voir Chapitre Environnement sécurité.
Bassin géographique prévisionnel	▪ Nantes, Marseille, Toulouse.
Profils et compétences associés	Expert technique/Sécurité spécialisé en Sécurité des réseaux.

Code UO	UO_5_E_SEC_SOL
Libellé UO	Expertise autres solutions de sécurité (AV, XDR, O365, CASB, PKI, Chiffrement, etc. ...).
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Initialisation : Prise en compte des prérequis fournis par l'ACOSS, ▪ Etude comparative des solutions, ▪ Mise en œuvre de l'environnement de tests (élaboration du plan détaillé de la mise en œuvre de la solution en test en tenant compte que la mise en œuvre de la solution impacte au minimum la production de l'ACOSS, suivi de la mise en œuvre de tests), ▪ Mise en œuvre de l'environnement d'intégration (élaboration du plan d'intégration de la solution dans l'environnement de production de l'ACOSS, suivi de l'intégration), ▪ Mise en œuvre de la nouvelle fonction validée, ▪ Réalisation et déroulement des tests unitaires dans le cadre de la nouvelle fonction et analyse, ▪ Intégration et recette usine de la nouvelle fonction, ▪ Assurance qualité, ▪ Création de la documentation technique et d'utilisation, ▪ Rédaction du rapport final.
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Exécutions (binaires, librairies, etc.), ▪ Maquettes et prototypes, ▪ Documentation technique, ▪ Jeux de tests validés, ▪ Support technique, ▪ Rapport final comprenant : L'intégration de la nouvelle fonction déployée, Le processus de déploiement et d'utilisation de la nouvelle fonction, Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés. ▪ Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	▪ Voir Chapitre Environnement sécurité.
Bassin géographique prévisionnel	▪ Nantes, Marseille, Toulouse.
Profils et compétences associés	Expert technique/Sécurité.

Code UO	UO_5_E_SEC_IAM_1
Libellé UO	Evolutions et MCO des produits de gestion des identités et des accès.
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Initialisation : Prise en compte des prérequis fournis par l'ACOSS, ▪ Etude comparative des solutions, ▪ Mise en œuvre de l'environnement de tests (élaboration du plan détaillé de la mise en œuvre de la solution en test en tenant compte que la mise en œuvre de la solution impacte au minimum la production de l'ACOSS, suivi de la mise en œuvre de tests), ▪ Mise en œuvre de l'environnement d'intégration (élaboration du plan d'intégration de la solution dans l'environnement de production de l'ACOSS, suivi de l'intégration), ▪ Mise en œuvre de la nouvelle fonction validée, ▪ Réalisation et déroulement des tests unitaires dans le cadre de la nouvelle fonction et analyse, ▪ Intégration et recette usine de la nouvelle fonction, ▪ Assurance qualité, ▪ Création de la documentation technique et d'utilisation, ▪ Rédaction du rapport final.
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Exécutions (binaires, librairies, etc.), ▪ Maquettes et prototypes, ▪ Documentation technique, ▪ Jeux de tests validés, ▪ Support technique, ▪ Rapport final comprenant : L'intégration de la nouvelle fonction déployée, Le processus de déploiement et d'utilisation de la nouvelle fonction, Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés. ▪ Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	▪ Voir Chapitre Environnement sécurité.
Bassin géographique prévisionnel	▪ Nantes, Marseille, Toulouse, Lyon.
Profils et compétences associés	Analyste/concepteur, développeur sécurité.

Code UO	UO_5_E_SEC_IAM_2
Libellé UO	Expertise solutions IAM (dont Authentification, MFA, Fédération d'identité).
Type d'UO	Expertise.
Phase	Protection du SI.
Description	▪ Initialisation : Prise en compte des prérequis fournis par l'ACOSS, ▪ Etude comparative des solutions, ▪ Mise en œuvre de l'environnement de tests (élaboration du plan détaillé de la mise en œuvre de la solution en test en tenant compte que la mise en œuvre de la solution impacte au minimum la production de l'ACOSS, suivi de la mise en œuvre de tests), ▪ Mise en œuvre de l'environnement d'intégration (élaboration du plan d'intégration de la solution dans l'environnement de production de l'ACOSS, suivi de l'intégration), ▪ Mise en œuvre de la nouvelle fonction validée, ▪ Réalisation et déroulement des tests unitaires dans le cadre de la nouvelle fonction et analyse, ▪ Intégration et recette usine de la nouvelle fonction, ▪ Assurance qualité, ▪ Création de la documentation technique et d'utilisation, ▪ Rédaction du rapport final.
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Exécutions (binaires, librairies, etc.), ▪ Maquettes et prototypes, ▪ Documentation technique, ▪ Jeux de tests validés, ▪ Support technique, ▪ Rapport final comprenant : L'intégration de la nouvelle fonction déployée, Le processus de déploiement et d'utilisation de la nouvelle fonction, Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés. ▪ Transfert de connaissance au profit des équipes internes pour ce qui concerne les travaux réalisés.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	▪ Voir Chapitre Environnement sécurité.
Bassin géographique prévisionnel	▪ Nantes, Marseille, Toulouse, Lyon.
Profils et compétences associés	Expert technique/Sécurité.

Code UO	UO_5_E_SEC_AUD
Libellé UO	Expertise Audits et tests de vulnérabilité.
Type d'UO	Expertise.
Phase	Cyberdéfense du SI.
Description	▪ Réalisation de la phase de test technique (qu'il soit interne, externe, de surface/exposition, réseaux ou autre selon le besoin), ▪ Point d'avancement quotidien durant la période de test, ▪ Restitution à chaud des éléments découverts en fin de période de test. ▪ Rédaction du rapport final.
Entrant	▪ Mise à disposition des solutions d'analyse de vulnérabilité.
Livrable	▪ Rapport final de test incluant : une synthèse managériale, une synthèse technique détaillée, avec les éléments de remédiation et les recommandations ainsi que les annexes pouvant faire sens au vu de l'audit, ▪ Réunion de restitution.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	▪ Nantes.
Profils et compétences associés	Auditeur Sécurité. Pentesteur . Une certification avancée en sécurité offensive (OSCP, CEH ou équivalent).

Code UO	UO_5_E_SEC_ANV
Libellé UO	Cyber analyse VOC.
Type d'UO	Expertise.
Phase	Cyberdéfense du SI.
Description	▪ Prise en charge des alertes de vulnérabilités, ▪ Analyse des équipements concernés et des risques opérationnels, ▪ Communication vers les départements concernés et le management, ▪ Lancement et suivi des plans de remédiation, ▪ Maintien en conditions opérationnelles et évolution des solutions, ▪ Gestion des données (classification, contrôle, ...), ▪ Création et publication des rapports et des extractions, ▪ Programmation des API et des requêtes, ▪ Rédaction de procédures opérationnelles.
Entrant	▪ Solutions d'analyse de vulnérabilité du SI. ▪ Procédures d'alertes et de suivi.
Livrable	▪ Messages d'alertes, tickets de remédiation et rapports de suivi. ▪ Analyses de risque lié aux vulnérabilités ▪ Solutions techniques opérationnelles. ▪ Automatisation des opérations
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	▪ Nantes.
Profils et compétences associés	Expert cybersécurité. Maitrise d'un outils de supervision des vulnérabilités (Tenable, Cyberwatch, Qualys, Rapid7, ..) Maitrise de la classification des vulnérabilités (CVSS, EPSS, ..).

Code UO	UO_5_E_SEC_ANS
Libellé UO	Cyber analyse SOC.
Type d'UO	Expertise.
Phase	Cyberdéfense du SI.
Description	▪ Maîtrise des techniques d'intrusion et de corruption, ▪ Maîtrise des règles de sécurité des systèmes d'informations, ▪ Prise en charge des alertes, triage des alertes ▪ Analyse les détections et alertes sur évènements de sécurité, ▪ Enrichissement des alertes ▪ Escalade, déclaration d'incident ▪ Proposition dans le cadre de l'amélioration continue des systèmes de détections, ▪ Recherche d'indices de compromission, ▪ Participation aux cellules technique de crises, ▪ Veille sécurité sur les méthodes et outils, ▪ Accompagnement les analystes N1 dans leur montée en compétences. ▪ Organisation des transferts de compétences.
Entrant	▪ Mise à disposition de source de journaux (log) applicatifs/réseaux/équipements... ainsi qu'un point central de communication pour la remontée d'information (adresse email suivi par les analystes N1/N2 côté ACOSS).
Livrable	▪ Rédaction des rapports d'analyses, ▪ Création des cases d'incidents ▪ Rédactions de fiches reflexes, ▪ Rédactions de procédures.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.
Profils et compétences associés	Expert cybersécurité. Des qualifications individuelles en sécurité sont un plus.

Code UO	UO_5_E_SEC_ANC
Libellé UO	Cyber analyse CSIRT.
Type d'UO	Expertise.
Phase	Cyberdéfense du SI.
Description	▪ Maîtrise des techniques d'intrusion et de corruption, ▪ Maîtrise des règles de sécurité des systèmes d'informations, ▪ Prise en charge des cas d'incidents. ▪ Analyse, confinement éradication des incidents ▪ Enrichissement des cas d'incidents ▪ Escalade managériale ▪ Proposition dans le cadre de l'amélioration continue des systèmes de détections, ▪ Recherche d'indices de compromission, ▪ Coordonne les cellules techniques, ▪ Participation aux cellules opérationnelles de crises, ▪ Veille sécurité sur les méthodes et outils, ▪ Accompagnement les analystes COS dans leurs investigations. ▪ Organisation des transferts de compétences.
Entrant	▪ Mise à disposition de source de journaux (log) applicatifs/réseaux/équipements... ainsi qu'un point central de communication pour la remontée d'information (adresse email suivi par les analystes N1/N2 côté ACOSS).
Livrable	▪ Rédaction des rapports d'incidents, ▪ Rédaction des RETEX ▪ Rédaction des plans d'actions, ▪ Rédactions de fiches reflexes, ▪ Rédactions de procédures.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevée permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.
Profils et compétences associés	Expert cybersécurité. Des qualifications individuelles en sécurité sont un plus.

Code UO	UO_5_E_SEC_ANT
Libellé UO	Cyber analyste Threat Intelligence
Type d'UO	Expertise.
Phase	Cyberdéfense du SI.
Description	• Surveillance et analyse de l'évolution du paysage de la menace • Collecte et exploitation de sources de renseignement techniques, opérationnelles et stratégiques • Identification et analyse de campagnes d'attaque ou d'acteurs malveillants • Analyse des techniques, tactiques et procédures (TTP) utilisées par les attaquants • Cartographie des menaces au regard du référentiel MITRE ATT&CK • Enrichissement et qualification d'indicateurs de compromission (IOC) • Contribution aux investigations menées par le SOC ou le CSIRT • Production de bulletins d'alerte ou de notes d'analyse • Formulation de recommandations visant à améliorer les capacités de détection, de protection et de réponse à incident
Entrant	▪ Accès aux plateformes de Threat Intelligence utilisées par le client ▪ Flux de renseignement externes (CERT, partenaires, éditeurs, OSINT, communautés de partage) ▪ Indicateurs de compromission à analyser ▪ Alertes ou investigations issues du SOC ▪ Journaux techniques issus des outils de sécurité (SIEM, EDR, NDR, etc.) ▪ Documentation interne relative au contexte de menace et aux actifs du système d'information.
Livrable	▪ Notes d'analyse sur des menaces émergentes ▪ Rapports d'analyse de campagnes d'attaque ou d'acteurs malveillants ▪ Enrichissement et qualification d'indicateurs de compromission ▪ Bulletins de veille ou d'alerte ▪ Recommandations pour l'amélioration des capacités de détection et de réponse.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.
Profils et compétences associés	Expert cybersécurité. Des qualifications individuelles en sécurité sont un plus.

Code UO	UO_5_E_SEC_SCI
Libellé UO	Evolution fonctionnelle ou technique du SOC.
Type d'UO	Expertise.
Phase	Cyberdéfense du SI.
Description	▪ Participer aux projets du SOC, ▪ Qualifier et réaliser les demandes d'évolution des outils du SOC, ▪ Définition et mise en œuvre de stratégies et de scénarios de détection des incidents de sécurité, ▪ Amélioration continue des mécanismes de détection, ▪ Analyse des remontées de logs, ▪ Configuration de règles de détection, agrégation, corrélation, ▪ Parsing de logs, ▪ Configuration de playbook dans le cadre de l'orchestration et automatisation, ▪ Participer à l'évolution de l'écosystème de gestion d'incident et de vulnérabilités, ▪ Administrer les outils.
Entrant	▪ Cahier des charges.
Livrable	▪ Corrections et évolutions fonctionnelles des moyens techniques du SOC, ▪ Rédaction de procédures techniques, ▪ Rédaction de fiches reflexes, ▪ Rédaction de dossiers d'exploitation et d'administration.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.
Profils et compétences associés	Expert cybersécurité.

Code UO	UO_5_E_SEC_CSY
Libellé UO	Conseil Cybersécurité.
Type d'UO	Expertise.
Phase	Cyberdéfense du SI.
Description	▪ Conseil sécurité, ▪ Élaboration et amélioration de stratégies de sécurité, ▪ Pilotage ou coordinations d'action Sécurité, ▪ Suivi des plans d'actions opérationnels en lien avec les plans d'action de gouvernance, ▪ Gestion des reportings, ▪ Coordination de la comitologie "Sécurité".
Entrant	▪ Expression de besoin, ▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Rédaction de synthèse, ▪ Support de présentation, ▪ Tableaux de bords de suivis, ▪ Indicateurs.
Complexité	Simple, Moyen, Complexe.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.
Profils et compétences associés	Expert cybersécurité. Des qualifications individuelles en sécurité sont un plus.

3.2.3 Service

Code UO	UO_5_S_SEC_FIR_ABO
Libellé UO	Force d'Intervention Rapide - Abonnement
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	Abonnement mensuel au service de Force d'Intervention Rapide comprenant : ▪ Garantie de réponse pour toute sollicitation d'incident d'envergure, ▪ Méthodologie reconnue (PRIS, ISO 27035, ISO 27037), ▪ Expertise technique requise (rétro ingénierie de code, analyse forensics système et réseau), ▪ Outillage adapté avec des possibilités d'intervention à distance, ▪ Messagerie sécurisée, ▪ Rappel par un expert sous 4h JO HO + JO HNO + weekend/jours fériés, ▪ Réservation de ressources garanties (au moins 2 personnes), ▪ Déploiement de l'équipe en France sous 1 JO, ▪ Définition des processus de gestion d'incident et de sollicitation, ▪ Participation à un exercice de crise cyber. Exigences de base : Voir chapitre 4.3.5 du présent CCTP.
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Processus et procédure d'alerte et d'intervention, ▪ Dossier d'architecture.
Complexité	NA.
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

Code UO	UO_5_S_SEC_FIR_HP
Libellé UO	Force d'Intervention Rapide – Intervention Hors PRIS.
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	Intervention d'une équipe de spécialistes cyber dans le cadre du déclenchement de la Force d'Intervention Rapide. (Hors PRIS) Utilisation d'une plateforme d'analyse spécifique. Activités ▪ Déterminer l'état des lieux suite à l'incident, ▪ Déterminer le périmètre impacté par l'incident, ▪ Déterminer les causes exactes de l'incident : dans le cas d'une attaque, déterminer le mode opératoire de l'attaquant, la séquence des événements, le vecteur d'intrusion et les moyens d'élévation de privilèges et de déplacement horizontal. ▪ Archiver de façon sécurisée les preuves et autres traces collectées lors de l'investigation, ▪ Présenter la chronologie exhaustive de l'incident, ▪ Proposer des recommandations pour prévenir la récurrence de l'incident. L'exigence E-FIR-PRIS-01 décrite dans le chapitre 4.3.10 du présent CCTP n'est pas exigé sur cette UO Exigences de base : Voir chapitre 4.3.5 du présent CCTP.
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Rapport d'intervention : Synthèse compréhensible par des non experts, Description précise du mode opératoire de l'attaquant, Liste des ressources et des comptes compromis, Liste des indicateurs de compromission, Mesures de remédiation, leur périmètre et le séquençement de mise en œuvre. ▪ PV de restitution des éléments et de destruction des preuves, ▪ Réunion de clôture de l'incident.
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'une intervention en fonction de la complexité sont les suivants : • SIMPLE : 3 jours • MOYEN : 5 jours • COMPLEXE : 10 jours
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

Code UO	UO_5_S_SEC_FIR_P
Libellé UO	Force d'Intervention Rapide – Intervention sous qualification PRIS
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	Intervention d'une équipe de spécialistes cyber dans le cadre du déclenchement de la Force d'Intervention Rapide. L'ensemble des activités demandées doivent suivre les processus, méthodes, outils et environnements respectant la qualification PRIS. Activités : ▪ Déterminer l'état des lieux suite à l'incident, ▪ Déterminer le périmètre impacté par l'incident, ▪ Déterminer les causes exactes de l'incident : dans le cas d'une attaque, déterminer le mode opératoire de l'attaquant, la séquence des événements, le vecteur d'intrusion et les moyens d'élévation de privilèges et de déplacement horizontal. ▪ Archiver de façon sécurisée les preuves et autres traces collectées lors de l'investigation, ▪ Présenter la chronologie exhaustive de l'incident, ▪ Proposer des recommandations pour prévenir la récurrence de l'incident. Exigences de base : Voir chapitre 4.3.5 du présent CCTP.
Entrant	▪ Tout élément nécessaire à la réalisation de la prestation.
Livrable	▪ Rapport d'intervention : Synthèse compréhensible par des non experts, Description précise du mode opératoire de l'attaquant, Liste des ressources et des comptes compromis, Liste des indicateurs de compromission, Mesures de remédiation, leur périmètre et le séquençage de mise en œuvre. ▪ PV de restitution des éléments et de destruction des preuves, ▪ Réunion de clôture de l'incident.
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'une intervention en fonction de la complexité sont les suivants : • SIMPLE : 3 jours • MOYEN : 5 jours • COMPLEXE : 10 jours
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevée permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

Code UO	UO_5_S_SEC_DSS_TMA
Libellé UO	Digital Signature Service - TMA
Type d'UO	Service.
Phase	Protection du SI
Description	Service mensuel permettant d'assurer les activités suivantes : Maintenir la solution et ces 2 socles OS : - OVA sur socle vmware (VM) - Package+Chart Helm sur socle Kubernetes (K8S) Garantir la comptabilité avec les composants : - Kubernetes - Modules cryptographiques : HSM Atos Trustway proteccio EL et HR avec librairies PKCS11 - Socles packaging : VMware, chart Helm V3 - Outils de traçabilité : rsyslog, fluentd, prometheus - Outil de supervision : Zabbix Les 2 versions VM et K8S devront être maintenues à jour et il sera nécessaire d'apporter un correctif en cas de détection de faille de sécurité ou d'obsolescence sur l'un de ses composants. Il est demandé d'identifier une ressource unique au suivi du compte de la branche Recouvrement pour les aspects techniques et administratifs. La prestation devra organiser au bout de 3 mois consécutifs un comité opérationnel décrit dans le chapitre 4.1. Exigences de base : Voir chapitre 4.3.6 du présent CCTP.
Entrant	▪ Dossier d'exploitation et d'architecture. ▪ Fourniture des codes sources de la solution ▪ Procédure d'installation
Livrable	▪ Compte rendu de la réunion trimestrielle ▪ Validation des versions et maintien en condition opérationnelle
Complexité	NA.
Spécificité de l'environnement technique	La nature de l'activité nécessite une compétence sur la librairie JAVA DSS (Digital signature service), K8s, openshift, java, bash.
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

Code UO	UO_5_S_SEC_UAD_TMA
Libellé UO	Usine d'Anonymisation des Données - TMA
Type d'UO	Service.
Phase	Protection du SI
Description	Service mensuel permettant le maintien en condition opérationnelle du service d'anonymisation comprenant : La partie technique : ▪ Mise à jour des versions du produit et des OS sur l'ensemble des serveurs constituant l'architecture de la solution. ▪ Validation des tests de non-régression suite aux modifications ▪ Suivi des indicateurs de stabilité de la plateforme (CPU, Mémoire et disque) et amélioration des tableaux de bords Zabbix et Grafana. ▪ Gestion de l'adressage des serveurs et des flux nécessaires à son fonctionnement ▪ Modification du paramétrage technique de la plateforme ▪ Prise en charge et mise en place de moyen nécessaire à la résolution des tickets d'incident ▪ Lancement de process d'anonymisation incluant la copie des fichiers ou la mise à disposition de la base de données et le processus de déclenchement de l'anonymisation ▪ Maintien du jeu de règles et prise en charge de fonctionnalités sur l'évolution de celle-ci. La partie fonctionnelle : ▪ Lancement de process d'anonymisation incluant la copie des fichiers ou la mise à disposition de la base de données et le processus de déclenchement de l'anonymisation ▪ Maintien du jeu de règles et prise en charge de fonctionnalités sur l'évolution de celle-ci. ▪ La prestation devra organiser au bout de 3 mois consécutifs un comité opérationnel décrit dans le chapitre 4.1. Toutes les demandes seront tracées dans l'outil de gestion de demande de l'ACOSS Exigences de base : Voir chapitre 4.3.4 du présent CCTP.
Entrant	▪ Dossier d'exploitation et d'architecture. ▪ Compte de connexion à la plateforme ▪ Machine de type VM/compte nominatif pour la réalisation des actions nécessaire
Livrable	▪ Validation des versions et maintien en condition opérationnelle ▪ Un comité opérationnel avec les métriques : ○ Nombre de mises à jour réalisées ○ Nombre d'incidents relevés ○ Volume de donnée anonymisées ○ Nombre de traitements réalisés ○ Nombre de fiches d'anonymisation créée Nombre d'incidents ▪ Traitement des anomalies d'anonymisation.
Complexité	NA.
Spécificité de l'environnement technique	La nature de l'activité nécessite une formation sur le produit DOT-A d'Arcad Software
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

Code UO	UO_S_SEC_UAD_INTEG
Libellé UO	Usine d'Anonymisation des Données – Intégration
Type d'UO	Service.
Phase	Protection du SI
Description	Service mensuel comprenant : ▪ Réalisation de l'étude permettant l'identification des cas d'usages, de la cartographie des données et la définition des règles d'anonymisation. ▪ Création du document de synthèse des éléments à anonymiser appelé fiche d'anonymisation. ▪ Développement du jeu de règle permettant la gestion du jeu de données ; ▪ Configuration des composants pour la mise en place de l'anonymisation (répertoire, transfert) ▪ Commande au niveau de la production des mécanismes d'automatisation ▪ Recette et test de validation. Toutes les demandes seront tracées dans l'outil de ticketing de l'ACOSS Exigences de base : Voir chapitre 4.3.4 du présent CCTP.
Entrant	▪ Identification des traitements de données à anonymiser ▪ Fourniture des contacts MOE pour l'étude des données ▪ Fichier exemple pour les fiches d'anonymisation ▪ Machine de type VM/compte nominatif pour la réalisation des actions nécessaire
Livrable	▪ Fiche d'anonymisation complétée et validée par la MOA ▪ Fiche de recette validant le fonctionnement des données anonymisées
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'une intégration UAD en fonction de la complexité sont les suivants : • SIMPLE : 5 jours • MOYEN : 10 jours • COMPLEXE : 20 jours
Spécificité de l'environnement technique	La nature de l'activité nécessite une formation sur le produit DOT-A d'Arcad Software
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

Code UO	UO_5_S_SEC_AUD
Libellé UO	Test d'intrusion.
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	Cette unité d'œuvre correspond à la réalisation d'un test d'intrusion sans qualification PASSI. L'exigence E-PASSI-LOT5-01 décrite dans le chapitre 4.3.10 du présent CCTP <u>n'est pas exigé sur cette UO</u> Exigences de base : Voir chapitre 4.3.6 du présent CCTP.
Entrant	▪ Mise à disposition de l'environnement cible. Environnement similaire aux conditions de productions des applications ACOSS.
Livrable	▪ Rapport final de test incluant : une synthèse managériale, une synthèse technique détaillée, avec les éléments de remédiation et les recommandations ainsi que les annexes pouvant faire sens au vu de l'audit ; ▪ Réunion de restitution.
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'un Test d'intrusion en fonction de la complexité sont les suivants : • SIMPLE : 10 jours • MOYEN : 20 jours • COMPLEXE : 30 jours
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevée permettant l'accès à des informations sensibles.

Code UO	UO_5_S_SEC_AUD_PASSI
Libellé UO	Test d'intrusion sous qualification PASSI.
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	Cette unité d'œuvre correspond à la réalisation d'un test d'intrusion sous qualification PASSI. L'activité sera qualifiée PASSI par l'ANSSI Exigences de base : Voir chapitre 4.3.6 du présent CCTP.
Entrant	▪ Mise à disposition de l'environnement cible. Environnement similaire aux conditions de productions des applications ACOSS.
Livrable	▪ Rapport final de test incluant : une synthèse managériale, une synthèse technique détaillée, avec les éléments de remédiation et les recommandations ainsi que les annexes pouvant faire sens au vu de l'audit ; ▪ Réunion de restitution.
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'un Test d'intrusion en fonction de la complexité sont les suivants : • SIMPLE : 10 jours • MOYEN : 20 jours • COMPLEXE : 30 jours
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.

Code UO	UO_5_S_SEC_FRS
Libellé UO	Service Forensic
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	Cette unité d'œuvre correspond à la réalisation d'une activité de FORENSIC sans qualification PRIS. L'exigence E-FIR-PRIS-01 décrite dans le chapitre 4.3.10 du présent CCTP <u>n'est pas exigé sur cette UO</u> Exigences de base : Voir chapitre 4.3.7 du présent CCTP.
Entrant	▪ Mise à disposition d'un accès au périmètre à analyser ainsi que toutes informations technique complémentaires nécessaires à l'exécution de l'analyse. (Données compromises, composants, système d'exploitation...etc...).
Livrable	▪ Établissement d'une chronologie forensic, ▪ Rapport final d'investigation, ▪ Rédaction de fiches reflexes, procédures techniques.
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'un FORENSIC en fonction de la complexité sont les suivants : • SIMPLE : 3 jours • MOYEN : 5 jours • COMPLEXE : 10 jours
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.

Code UO	UO_5_S_SEC_FRS_P
Libellé UO	Service Forensic sous qualification PRIS
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	Cette unité d'œuvre correspond à la réalisation d'une activité de FORENSIC sous qualification PRIS. L'ensemble des activités demandées doivent suivre les processus, méthodes, outils et environnements respectant la qualification PRIS de l'entreprise. Exigences de base : Voir chapitre 4.3.7 du présent CCTP.
Entrant	▪ Mise à disposition d'un accès au périmètre à analyser ainsi que toutes informations technique complémentaires nécessaires à l'exécution de l'analyse. (Données compromises, composants, système d'exploitation...etc...).
Livrable	▪ Établissement d'une chronologie forensic, ▪ Rapport final d'investigation, ▪ Rédaction de fiches reflexes, procédures techniques.
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'un FORENSIC en fonction de la complexité sont les suivants : • SIMPLE : 3 jours • MOYEN : 5 jours • COMPLEXE : 10 jours
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevé permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.

Code UO	UO_5_S_SEC_THI
Libellé UO	Service Threat Intelligence
Type d'UO	Service.
Phase	Cyberdéfense du SI.
Description	La prestation consiste en l'analyse de renseignement sur les menaces cyber, portant sur un périmètre défini par le client et donnant lieu à la production d'un rapport d'analyse structuré Sauf indication contraire dans la commande, l'activité porte au maximum sur : - l'analyse d'un ensemble 5 indicateurs de compromission ; - l'analyse d'une campagne ou d'une menace spécifique Exigences de base : Voir chapitre 4.3.8 du présent CCTP.
Entrant	• Description du besoin d'analyse • Liste d'indicateurs de compromission à analyser • Artefacts techniques associés à un incident ou une menace • Flux de Threat Intelligence accessibles • Documentation relative au contexte technique ou métier
Livrable	Un rapport d'analyse Threat Intelligence comprenant au minimum : • Le contexte et le périmètre de l'analyse • Les sources exploitées • La liste des indicateurs analysés et leur qualification • L'analyse des techniques et modes opératoires identifiés • La cartographie des techniques au regard du référentiel MITRE ATT&CK • L'évaluation du niveau de menace pour le système d'information • Des recommandations opérationnelles (détection, protection, remédiation)
Complexité	Le nombre de jours estimés par l'ACOSS pour réaliser toutes les étapes d'un THREAT INTEL en fonction de la complexité sont les suivants : • SIMPLE : 3 jours • MOYEN : 5 jours • COMPLEXE : 10 jours
Spécificité de l'environnement technique	La nature de l'activité nécessite une qualification en sécurité élevée permettant l'accès à des informations sensibles.
Bassin géographique prévisionnel	NA.
Profils et compétences associés	A définir par le candidat en s'appuyant sur la grille des profils (Annexe : « Grille des profils »).

3.2.4 Activité

Des prestations complémentaires peuvent être demandées soit au travers d'astreintes sans intervention en dehors des plages habituelles du lundi au vendredi 8h-19h, soit au travers de prestations de travail décalé, notamment durant les mises en production.

- Astreinte
- Travail décalé en HNO

Code UO	UO_5_A_A_AST		
Libellé UO	Astreinte		
Type d'UO	Activité		
Phase	Astreinte		
Description	Astreinte, par les intervenants habituels sur le projet, durant les périodes critiques de bascule à blanc, bascule réelle ou post mise en production. Ce peut être aussi durant des périodes particulières de traitement pour l'application (rattrapages, cycles annuels ou trimestriels, ...). Il s'agit principalement d'être disponible pour répondre par téléphone aux éventuelles sollicitations. Cette unité d'œuvre ne donne pas lieu à une intervention physique (couverte par l'UO ci-dessous).		
Entrant	N.A.		
Livrable	▪ Rapport d'astreinte		
Complexité	1	2	3
	Nuit de 19h à 8h,	Samedi de 8h à 19h,	Dimanche et JF de 8h à 19h.

Code UO	UO_5_A_A_TDHNO		
Libellé UO	Travail décalé en HNO		
Type d'UO	Activité		
Phase	Transverse		
Description	Appui aux équipes internes dans le cadre d'interventions à des moments particuliers entre autres de 19H à 8H en semaine, ou le samedi, ou le dimanche. Les nuits de vendredi à samedi, de samedi à dimanche, et de dimanche à lundi sont exclues.		

Entrant	N.A.		
Livrable	▪ Rapport d'astreinte		
Complexité	1	2	3
	Nuit de 19h à 8h,	Samedi de 8h à 19h,	Dimanche et JF de 8h à 19h.

 cf. CRT	2.3.4 Gestion des dispositifs
--	--------------------------------------

4 Modalités des prestations

4.1 Gouvernance du lot

Les instances opérationnelles décrites ci-après viennent en complément des instances de pilotage décrites dans le CCTP Commun.

- **Comitologie liée aux services Usine d'Anonymisation des Données**

	Comité opérationnel UAD
Rôle	Il permet de suivre les évolutions de la plateforme et de l'activité de TMA. Il devra notamment indiquer : - les mises à jour réalisées, - les demandes et incidents observés sur la période - la roadmap de l'outil - les anonymisation mise en place durant le trimestre - Les évolutions de la configuration des règles d'anonymisation - Les erreurs potentielles d'anonymisation - Le suivi des indicateurs : ○ GTI et GTR sur la période ○ Volume de donnée anonymisées ○ Nombre de traitements réalisés ○ Nombre de fiches d'anonymisation créée ○ Nombre de MOE applicatives accompagnées
Participants	ACOSS : • Responsable produit UAD • Expert participant à la MCO de l'outil Titulaire : • Prestataire réalisant la prestation • Le référent du compte
Fréquence	Trimestriel

Durée	1 heure maximum. Réunion par visioconférence.
Convocation	Le titulaire envoie une convocation à l'ensemble des participants avec l'ordre du jour. Néanmoins, la date de la réunion sera déjà indiquée dans le compte-rendu précédent.
Entrants	Le titulaire fournit à l'ACOSS au plus tard trois jours ouvrés avant le comité : Un rapport permettant de traiter les sujets de l'ordre du jour.
Sortants	Un compte-rendu de la réunion, à la charge du titulaire, diffusé dans un délai de 5 jours.

- **Comitologie liée aux services Digital Signature Service Infrastructure**

	Comité Opérationnel Digital Signature Service
Rôle	Il permet le suivi de la gestion de la plateforme. Le comité permet d'aborder les incidents sur la période écoulée, la préconisation en maintenance préventive, la prise en compte des nouvelles demandes d'évolution, la planification des interventions à venir. Il devra également permettre de suivre les indicateurs suivants: ○ GTI et GTR sur la période ○ Nombre d'incidents ○ Délai de résolution ○ Nombre de mise à jour
Participants	ACOSS : • Responsable produit DSS • Expert participant à la MCO de l'outil DSS Titulaire : • Interlocuteur technique et administratif privilégié de l'ACOSS. • Le référent du compte
Fréquence	Trimestriel
Durée	1 heure maximum. Réunion par visioconférence.
Convocation	Le titulaire envoie une convocation à l'ensemble des participants avec l'ordre du jour. Néanmoins, la date de la réunion sera déjà indiquée dans le compte-rendu précédent.
Entrants	Le titulaire fournit à l'ACOSS au plus tard trois jours ouvrés avant le comité un rapport permettant de traiter les sujets de l'ordre du jour.
Sortants	Un compte-rendu de la réunion, à la charge du titulaire, diffusé dans un délai de 5 jours.

Cette gouvernance sera proposée par le soumissionnaire et sera inscrite aux plans qualité du titulaire.

 cf. CRT	2.3.1.1 Organisation du lot
--	------------------------------------

4.2 Indicateurs de niveaux de services

Identification des souhaits pour les typologies de prestations suivantes :

- Services.
 - Indicateurs.
 - **E-INDIC-01** : Le service devra mettre en œuvre et suivre des indicateurs permettant de mesurer la qualité du service délivré. La liste d'indicateurs sera approuvée par le prestataire et le Recouvrement au démarrage du service.

Les indicateurs de niveaux service du lot doivent répondre aux exigences exprimées dans le CCTP commun paragraphe intitulé 'Niveaux de services en complément du souhait exprimé ci-dessus.

 cf. CRT	2.1.3.2 Indicateurs transverses au marché
--	---

4.3 Conditions générales d'exécution des prestations

4.3.1 Applicables aux prestations d'initialisation du lot

- Services,
 - **E-INIT-01** : La mise en œuvre de la prestation s'appuie sur un processus structuré incluant à minima des ateliers de découverte du Système d'Information couvert par le service, une comitologie, une organisation dédiée et un plan de charge prévisionnel.

Les prestations d'initialisation du lot doivent, en complément de l'exigence ci-dessus, répondre aussi aux exigences exprimées dans le CCTP commun paragraphe intitulé 'Phase d'initialisation du marché'.

 cf. CRT	2.1.3.5 Phase d'initialisation du marché
--	--

4.3.2 Applicables aux prestations de réversibilité

- Services,
 - **E-REVER-01** : Le service prévoit une phase de réversibilité à l'issue de la prestation.
 - Cette phase de réversibilité s'appuie sur un processus structuré incluant une comitologie, une organisation dédiée, une identification des éléments restitués et un plan de charge prévisionnel.

Les prestations de réversibilité du lot doivent répondre, en complément de l'exigence ci-dessus, répondre aussi aux exigences exprimées dans le CCTP commun paragraphe intitulé 'Phase de réversibilité du marché'.

 cf. CRT	2.1.3.6 Phase de réversibilité du marché
--	--

4.3.3 Applicables au service Digital Signature Service (DSS).

Délais contractuels :

- **E-DSS-INC-01** : En cas d'incident sur l'infrastructure, il est demandé de respecter les garanties suivantes :
 - Garantie de temps d'intervention sur environnement de production/pré-production) =H+4
 - GTR_P (Garantie de temps de rétablissement sur environnement de production/pré-production)=J+1
 - GTI_H (Garantie de temps d'intervention sur environnement de développement/intégration/validation) = J+1
 - GTR_H (Garantie de temps de rétablissement sur environnement développement/intégration/validation) = J+5

Service attendu :

- **E-DSS-RESP-01** : En plus du service décrit dans la prestation, l'ACOSS demande un interlocuteur privilégié pour assurer les fonctions suivantes :
 - Il sera le garant de la Qualité du Service sur l'ensemble du périmètre par l'animation de réunions périodiques avec le coordinateur de l'ACOSS et il veillera au respect des engagements contractuels.
 - Il gèrera l'évolution du contrat en s'assurant que l'environnement technique soit pris en compte dans le contrat de maintenance selon les conditions énoncées par l'ACOSS.
 - Il prendra en compte l'environnement spécifique ACOSS.
 - Il organisera des réunions trimestrielles de suivi permettant d'aborder les incidents sur la période écoulée, la préconisation en maintenance préventive, la prise en compte des nouvelles demandes d'évolution, la planification des interventions à venir. En d'autres termes, il sera l'interlocuteur technique et administratif privilégié de l'ACOSS.
 - Il sera nécessaire de mettre à disposition une interface d'accès web pour le support. Cet accès devra permettre d'ouvrir des tickets pour la gestion des demandes et des incidents, de joindre des journaux de logs, d'échanger des sources d'installation.

 cf. CRT	2.3.3.1 Service Digital Signature Service
---	---

4.3.4 Applicables au service Usine d'Anonymisation des Données (UAD)

Délais contractuels :

- **E-UAD-INC-01** : En cas d'incident sur la plateforme il est demandé de respecter les garanties suivantes :
 - Garantie de temps d'intervention sur environnement =H+6
 - GTR=J+2

Service attendu :

- **E-UAD-RESP-01** : En plus du service décrit dans la prestation, l'ACOSS demande un interlocuteur privilégié pour assurer les fonctions suivantes :
 - Organisation des comités trimestriels
 - Coordonnée les échanges avec l'éditeur de la solution Dot-A

 cf. CRT	2.3.3.2 Service d'Anonymisation des Données (UAD)
---	---

4.3.5 Applicables au service Force d'Intervention Rapide (FIR)

Délais contractuels :

- **E-FIR-GEO-01** : Les interventions sont possibles sur n'importe quel point du territoire métropolitain français dans les délais prévus contractuellement.
- **E-FIR-RAPPEL-01** : Le délai maximum de première prise en charge par un expert est de 4h en jours ouvrés entre 08h à 20h, y compris les week-end et jours fériés.
- **E-FIR-INTER-01** : Le délai maximum d'intervention sur n'importe quel point de France métropolitaine est de 24 heures ouvrés maximum.

Service attendu :

- **E-FIR-MOYENS-01** : Le service s'appuie sur un outillage à l'état de l'art et adapté à une prestation de FIR, y compris des moyens d'intervention à distance.
- **E-FIR-COMM-01** : Le service inclut un canal de communication dédié incluant à minima une boîte mail ou un espace de chat avant ou pendant une intervention.
- **E-FIR-PARTA-01** : Le service inclut un espace de travail sécurisé permettant le partage d'information avant ou pendant une intervention.
- **E-FIR-RESP-01** : Le service inclut la mise à disposition en cas de crise d'un responsable qui sera le pilote opérationnel de l'équipe d'analyse et le point de contact privilégié vis à vis du client.
- **E-FIR-RAPP-01** : Les rapports d'investigation numérique produits suite à une intervention devront évoquer à minima les sujets suivantes :
 - une chronologie détaillée des événements constituant l'incident,
 - les indicateurs de compromission liés à l'incident,
 - les éléments de renseignements liés aux agents de menace,
 - un plan d'action pour rétablir la situation nominale et éviter la reproduction de l'incident,
 - un rapport managérial reprenant les constats clés afin de contextualiser les risques liés à l'incident et le plan d'action.
- **E-FIR-TRAC-01** : Le service inclut la mise à disposition en cas de crise d'un responsable qui sera le pilote opérationnel de l'équipe d'analyse et le point de contact privilégié vis à vis du client.

 cf. CRT	2.3.3.3 Service Force d'Intervention Rapide
--	---

4.3.6 Applicables au service Test d'intrusion.

Le service de Test d'intrusion devra inclure les étapes suivantes :

- Réunion de lancement de la prestation : présentation du périmètre et des prérequis,
- Réalisation de la phase de test technique (qu'il soit interne, externe, de surface/exposition, réseaux ou autre selon le besoin),
- Point d'avancement quotidien durant la période de test,
- Restitution à chaud des éléments découverts en fin de période de test,
- Rédaction du rapport final,
- Présentation à froid du rapport final avec synthèse managériale.

Le candidat devra composer une équipe capable de répondre aux besoins d'AUDIT de l'ACOSS.

 cf. CRT	2.3.3.4 Service Test d'intrusion
--	----------------------------------

4.3.7 Applicables au service Forensic

Le candidat devra mener les tâches suivantes dans le cadre du service FORENSIC

- Détermination des causes racines d'un incident,
- Estimation de l'impact technique et métier,
- Analyse la plus exhaustive possible des actions de l'attaquant sur le périmètre compromis,
- Conception et développement d'outils d'aide à l'analyse,
- Recherche de vulnérabilités sur des solutions software et hardware dans le cadre d'un incident,
- Recherche d'indices de compromissions,
- Investigation numérique sur tout type de système d'exploitation,
- Analyse de la mémoire vive,
- Analyse de malware (serveurs contactés, mécanismes de persistance, artefacts permettant de le détecter sur l'ensemble d'un parc, propagation, etc...),
- Reverse engineering et déchiffrement de tout élément lié à un malware (communications réseau, fichier de configuration, fichier stockant les données volées, etc...).

L'ACOSS a identifié 5 types de périmètres possibles d'analyses :

1. Système Windows
2. Système Linux
3. Analyse de mémoire
4. Analyse d'équipements d'infrastructure
5. Analyse réseaux

Le candidat devra composer une équipe capable de répondre aux besoins de FORENSIC de l'ACOSS.

 cf. CRT	2.3.3.5 Service Forensic
---	--------------------------

4.3.8 Applicables au service Threat Intelligence

Le candidat devra mener les tâches suivantes dans le cadre du service Threat Intelligence

- Analyse du besoin :
 - prise en compte du contexte et du périmètre de la demande ;
 - identification des objectifs de l'analyse ;
 - identification des sources de renseignement pertinentes.
- Collecte d'informations

- collecte d'informations issues de sources ouvertes (OSINT) ;
- exploitation des flux de Threat Intelligence disponibles ;
- exploitation des sources internes mises à disposition par le client.
- Qualification et enrichissement
 - qualification des indicateurs de compromission fournis ;
 - enrichissement des indicateurs via des sources externes ;
 - identification de relations entre indicateurs, infrastructures malveillantes et campagnes d'attaque.
- Analyse de la menace
 - identification des techniques, tactiques et procédures (TTP) utilisées ;
 - cartographie des techniques observées au regard du référentiel MITRE ATT&CK ;
 - identification d'éventuels groupes d'attaquants associés ;
 - évaluation du niveau de menace pour le périmètre du client.
- Production d'une synthèse
 - consolidation des informations collectées ;
 - rédaction d'un rapport d'analyse ;
 - formulation de recommandations opérationnelles

Le candidat devra composer une équipe capable de répondre aux besoins de THREAT INTEL de l'ACOSS.

 cf. CRT	2.3.3.6 Service Threat Intelligence
---	-------------------------------------

4.3.9 Accès aux expertises de niche.

- Spécificité des prestations **UO_5_E_SEC_ISP_1** « Accompagnement sécurité de projets » :

Il est attendu que le candidat démontre sa capacité à répondre au besoin de l'ACOSS en nombre et type de profils sur ce type de prestation. En effet, la nature de l'activité, du profil nécessaire et du suivi des dossiers, nécessite une pérennité des moyens humains mis en œuvre.

La mise en place d'une structure de type pôle de compétence d'architecture sécurisée et d'intégration de la sécurité dans les projets serait par exemple un plus.

 cf. CRT	2.3.4.1 Dimensionnement des dispositifs
---	---

- Les profils nécessaires à ces prestations étant très spécifiques, **le candidat devra aussi démontrer sa capacité à faire appel à de la sous-traitance adaptée à des prestations de renfort des équipes internes de l'ACOSS sur de longues durées.**

Service Force d'Intervention Rapide (FIR) :

- **E-FIR-EXPERTISE-01** : Le service est assuré par des analystes disposant d'une expertise technique dans les domaines de rétro ingénierie de code et d'analyses forensiques.
- **E-FIR-EXPERIENCE-01** : Le service est assuré par des analystes disposant d'une expérience significative en gestion d'incident de cybersécurité et d'accompagnement des clients touchés par ce type d'évènement.

 cf. CRT	2.3.4.5 Modalités d'appel à la sous-traitance ou à la co-traitance 2.3.4.6 Modalités de suivi et maitrise de la sous-traitance ou de la co-traitance
---	---

4.3.10 Exigences de sécurité

Les exigences de sécurité ci-dessous viennent en complément des exigences sécurité du CCAP et du CCTP commun.

- **E-C-RH-LOT5-01** : Le candidat effectue des vérifications d'antécédents, lorsque cela est autorisé par la loi, sur les employés qui interviennent sur des prestations du lot.
- **E-PRIS-LOT5-01** : Le candidat est qualifié ou en cours de qualification PRIS auprès de l'ANSSI.
- **E-PASSI-LOT5-01** : Le candidat est qualifié ou en cours de qualification PASSI auprès de l'ANSSI.

 cf. CRT	2.3.4.4 Formation et certification des collaborateurs
--	--

5 Cas pratique

5.1 Évaluation de la maturité de la sécurité

L'ACOSS souhaite évaluer sa maturité en matière de sécurité pour identifier les domaines d'amélioration. Il est attendu du candidat de décrire les étapes à suivre pour évaluer la maturité de la sécurité, y compris la sélection des outils et des méthodes, la collecte des données et l'analyse des résultats.

5.2 Accompagnement en expertise technique Cloud

L'Acoss souhaite évaluer les compétences du candidat pour fournir des services d'expertise spécialisée en sécurisation d'infrastructures cloud. Le cas pratique est une migration d'une architecture technique vers un cloud public. L'objectif est de garantir un niveau de sécurité élevé.

La proposition de candidat devra indiquer la méthodologie et les outils qu'elle utilisera pour cet accompagnement en mettant en évidence les éléments améliorant le niveau de sécurité pour les points suivant :

- **Gestion du projet** : Le candidat devra notamment détailler les méthodes et les tâches nécessaires pour aider à définir les besoins sécurité.
- **Architecture Sécurisée** : Le candidat indiquera les principes utilisés pour proposer une architecture sécurisée par design, en identifiant les éléments clés à sécuriser.
- **Sécurité** : Le candidat devra donner la méthode pour définir les différentes solutions de sécurisation à utiliser, en tenant compte des menaces et des risques dans cet environnement.
- **Conformité aux Réglementations** : Le candidat devra indiquer comment identifier les réglementations et les normes applicables dans ce cas
- **Organisation et Profil** : Le candidat devra détailler l'organisation à mettre en place pour proposer un profil correspondant à la demande d'expertise, ainsi que la phase de transfert de compétences pour garantir la pérennité du projet après la prestation.
- **Éléments Supplémentaires** : Le candidat pourra inclure dans sa proposition tout élément supplémentaire qui pourrait aider à la réalisation de cet accompagnement, tel que des outils, des méthodologies ou des bonnes pratiques en matière de sécurité.

L'Acoss attend une proposition détaillée et complète, qui répond aux exigences ci-dessus et qui démontre la capacité du candidat à fournir des expertises sécurité de haute qualité.

 cf. CRT	2.3.5 Cas pratique
--	--------------------