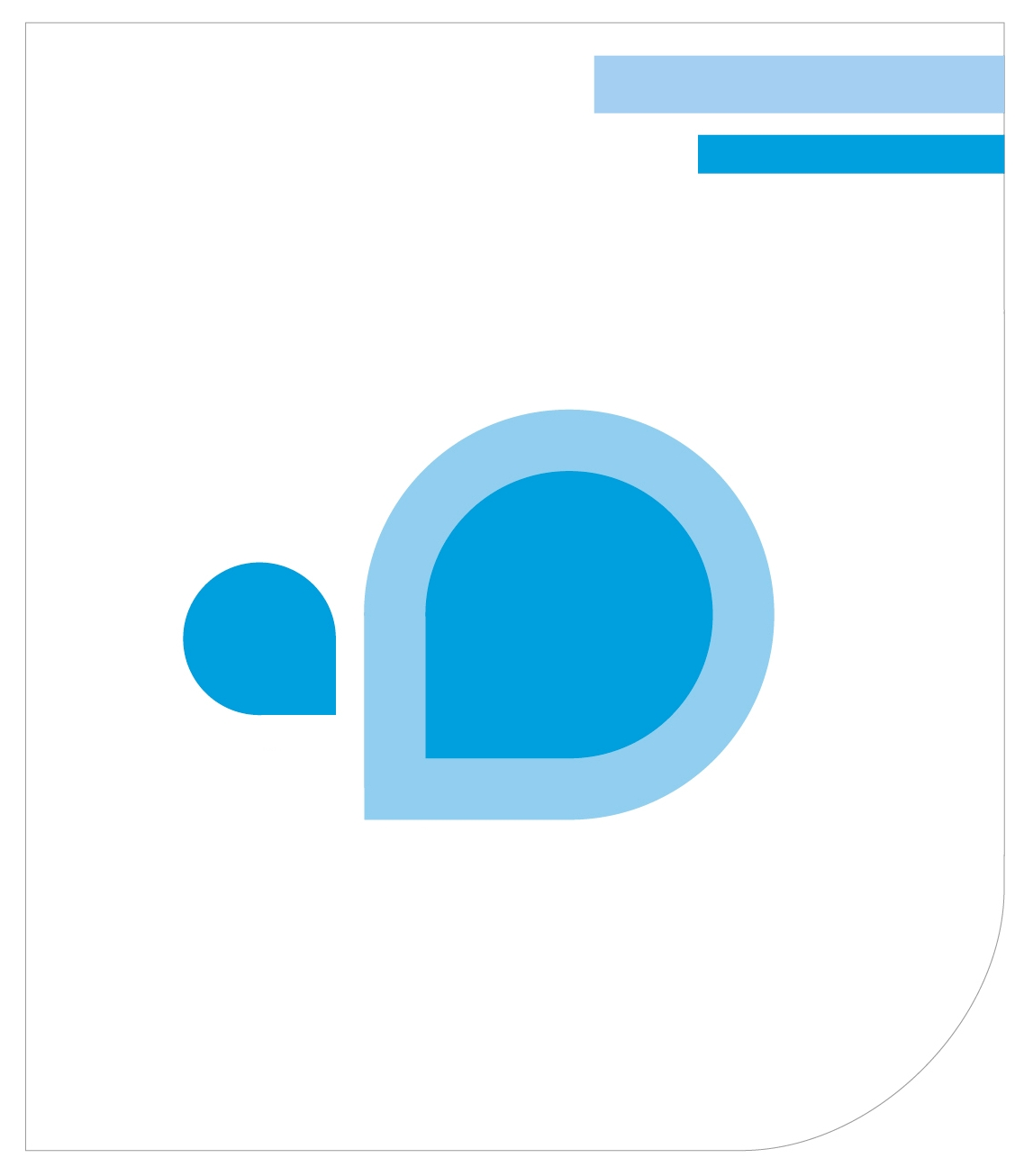
ANNEXE CCTP - EXIGENCES de SECURITE

Caisse nationale du réseau des Urssaf



**Sécurité Informatique**

**Orientations Générales**

CCTP ANNEXE

EXIGENCES DE SECURITE

Table des matières

[1. PREAMBULE 1](#_Toc100940563)

[1.1 Objet du document 1](#_Toc100940564)

[2.1 Questionnaire d’évaluation de la maturité 1](#_Toc100940565)

[2. EXIGENCES 2](#_Toc100940566)

[3.1 Tableau de synthèse des exigences applicables 2](#_Toc100940567)

[4.1 Exigences de sécurité 5](#_Toc100940568)

1. PREAMBULE
2. Objet du document

Ce document s’inscrit en complément au CCTP commun.

Il décrit aux soumissionnaires les exigences de sécurité ACOSS applicables aux différentes prestations à exercer.

Le document se compose d’un tableau présentant les références des exigences applicables à chaque type d’UO des différents lots, puis du descriptif complet de chaque exigence.

Le soumissionnaire doit décrire dans son PAS comment il répond aux différentes exigences pour les lots sur lesquels il est candidat.

1. Questionnaire d’évaluation de la maturité

Le Titulaire doit par ailleurs compléter le document nommé « Evaluation de Maturité de Sécurité des Fournisseurs » et répondre à l’ensemble des questions mentionnées.

Le questionnaire de sécurité est en lien avec les exigences de sécurité du présent document et est un outil utilisé par l’ACOSS pour traiter les réponses au présent marché. Cet outil servira à apprécier le niveau de sécurité déclaré par chaque candidat. Ne pas répondre au questionnaire impliquera inévitablement la note minimale à l’appréciation du niveau de sécurité du candidat.

1. EXIGENCES
2. Tableau de synthèse des exigences applicables

Indique que l’exigence (ou le souhait) est applicable aux UO concernées.



Indique que l’exigence (ou le souhait) n’est pas applicable aux UO concernées.



| **UO concernées** | **UO services lots 1,2,3,4,6** | **UO services lot 9** | **UO services lot 8** | **UO services lot 10** | **UO expertises** | **UO activités** |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref. exigence CCTP** |  |  |  |  |  |  |
| SEC\_C\_POL\_1 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_POL\_2 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_POL\_4 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ORG\_1 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ORG\_2 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ORG\_3 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ORG\_4 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ORG\_9 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_RH\_1 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_RH\_2 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_RH\_3 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_RH\_4 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_RH\_7 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_RH\_8 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_ENV\_1 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_ENV\_2 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_ENV\_6 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_ENV\_7 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_ENV\_9 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_ENV\_10 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_COM\_1 |  |  | **X** |  |  |  |
| SEC\_C\_COM\_7 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_COM\_8 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_COM\_16 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_COM\_17 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_COM\_21 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_COM\_22 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_COM\_26 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_COM\_31 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_COM\_32 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_1 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_ACC\_3 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_4 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_5 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_6 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_7 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_11 | **X** | **X** | **X** | **X** |  |  |
| SEC\_C\_ACC\_12 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_18 | **X** | **X** | **X** | **X** |  |  |
| SEC\_C\_ACC\_26 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_27 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_ACC\_29 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_DEV\_4 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_DEV\_6 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_DEV\_8 | **X** | **X** |  |  |  |  |
| SEC\_C\_DEV\_10 | **X** |  |  |  |  |  |
| SEC\_C\_DEV\_11 | **X** |  |  |  |  |  |
| SEC\_C\_DEV\_13 | **X** | **X** |  |  |  |  |
| SEC\_C\_DEV\_14 |  |  |  | **X** |  |  |
| SEC\_C\_DEV\_17 | **X** |  |  | **X** |  |  |
| SEC\_C\_DEV\_23 | **X** |  |  |  |  |  |
| SEC\_C\_DEV\_24 | **X** |  |  |  |  |  |
| SEC\_C\_DEV\_25 | **X** |  |  |  |  |  |
| SEC\_C\_DEV\_26 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_DEV\_27 | **X** | **X** | **X** | **X** |  | **X** |
| SEC\_C\_INC\_1 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_INC\_2 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_INC\_3 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_INC\_4 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_INC\_5 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_INC\_6 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_INC\_7 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_INC\_8 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONT\_1 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONT\_2 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONT\_5 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONT\_6 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONT\_7 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_1 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_2 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_6 | **X** | **X** | **X** | **X** |  |  |
| SEC\_C\_CONF\_7 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_8 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_9 | **X** | **X** | **X** | **X** |  |  |
| SEC\_C\_CONF\_10 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_11 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_13 | **X** | **X** | **X** | **X** | **X** | **X** |
| SEC\_C\_CONF\_15 | **X** | **X** | **X** | **X** | **X** | **X** |

1. Exigences de sécurité

| **Ref. exigence** | **Description de l'exigence** |
| --- | --- |
|  | **Politique de Sécurité** |
| SEC\_C\_POL\_1 | Le Titulaire doit disposer d'une PSSI complète, documentée et approuvée formellement par sa direction. |
| SEC\_C\_POL\_2 | Le Titulaire s’engage à ce que toute personne (employé, prestataire) en contact avec son SI ait connaissance de sa « charte utilisateurs du SI » et de sa politique de sécurité. |
| SEC\_C\_POL\_4 | Le Titulaire doit être conforme à sa PSSI durant toute la durée de la prestation pour l'ACOSS. |
|  | **Organisation de la Sécurité de l'Information** |
| SEC\_C\_ORG\_1 | Le titulaire doit mettre en oeuvre des procédures et dispositifs de sécurité pour se protéger contre le traitement non autorisé ou illégal, le transfert à un tiers, la perte ou la destruction d'informations appartenant à l'ACOSS. |
| SEC\_C\_ORG\_2 | Le Titulaire doit disposer d'un référent sécurité en charge de l'application et du maintien de la PSSI. |
| SEC\_C\_ORG\_3 | La PSSI du Titulaire doit définir avec précision les rôles et les responsabilités pour les activités liées à la sécurité de l'information. |
| SEC\_C\_ORG\_4 | Il est souhaité que le Titulaire définisse et mette en œuvre les processus de sécurité fondamentaux suivants : a. Évaluation des risques liés à l'information, b. Réponse à incident, c. Sensibilisation à la sécurité, d. Gestion des correctifs, e. Surveillance des vulnérabilités, f. Gestion des fournisseurs, g. Gestion des incidents. |
| SEC\_C\_ORG\_9 | Le Titulaire doit corriger dans des délais acceptables par l'ACOSS les problèmes pouvant entraîner une violation majeure de la sécurité. |
|  | **Sécurité des Ressources Humaines** |
| SEC\_C\_RH\_1 | La PSSI du Titulaire documente les rôles de sécurité clés (par exemple, le responsable de la sécurité de l'information, le responsable de la protection des données). Le Titulaire doit communiquer à l'ACOSS les coordonnées des personnes en charge de ces rôles lors de la phase d'initialisation. |
| SEC\_C\_RH\_2 | Il est souhaité que le titulaire effectue des vérifications d'antécédents, lorsque cela est autorisé par la loi, sur les employés qui traitent des données qui appartiennent à l'ACOSS ou qui accèdent au SI de l'Acoss. |
| SEC\_C\_RH\_3 | Le Titulaire doit former les nouveaux membres du personnel (à temps plein, à temps partiel, sous-traitants) sur leurs responsabilités en matière de sécurité dès leur prise de fonction. |
| SEC\_C\_RH\_4 | Le Titulaire doit dispenser une formation régulière de sensibilisation à la sécurité à tout le personnel pour lui rappeler ses responsabilités et l'éduquer sur l'identification et la réponse aux menaces nouvelles et émergentes. |
| SEC\_C\_RH\_7 | Le Titulaire doit limiter les droits d'accès au réseau et à l'accès physique aux bâtiments au stricte nécessaire à l'activité des personnes. |
| SEC\_C\_RH\_8 | Ces droits d'accès doivent être supprimés pour les membres du personnel dont le contrat, l'emploi ou l'accord a été supprimé. |
|  | **Sécurité Physique et Environnementale** |
| SEC\_C\_ENV\_1 | Le Titulaire doit limiter l'accès aux seuls utilisateurs autorisés sur les installations physiques abritant les systèmes qui contiennent des informations de l'ACOSS et les infrastuctures réseaux qui permettent l'accès au SI ACOSS. |
| SEC\_C\_ENV\_2 | Le Titulaire doit enregistrer l'accès physique du personnel sur les installations physiques abritant les systèmes qui contiennent des informations de l'ACOSS et les infrastuctures réseaux qui permettent l'accès au SI ACOSS. |
| SEC\_C\_ENV\_6 | Le Titulaire doit disposer d'une politique de bureau propre pour empêcher les fuites de données (c'est-à-dire que des copies papier de données appartenant à l'ACOSS soient volées dans le bâtiment). |
| SEC\_C\_ENV\_7 | Les copies papier des données de l'ACOSS doivent être déchiquetées lorsqu'elles ne sont plus nécessaires. |
| SEC\_C\_ENV\_9 | Le Titulaire doit contrôler de manière appropriée les points d'entrée tels que les zones de livraison et de chargement. |
| SEC\_C\_ENV\_10 | Le Titulaire doit surveiller la sécurité des zones physiques sensibles (par exemple, zones de livraison et de chargement, entrées du batiment), le cas échéant avec des techniques de surveillance appropriées (télésurveillance). |
|  | **Communications et Operations** |
| SEC\_C\_COM\_1 | Le Titulaire doit documenter, réviser et maintenir toutes les procédures d'exploitation du SI de l'ACOSS. |
| SEC\_C\_COM\_7 | Le Titulaire doit disposer d'outils de contrôle permettant de détecter et d'empêcher l'exécution de code malveillant et de code mobile non autorisé sur tout système contenant des informations de l'ACOSS ou permettant l'accès au SI ACOSS. |
| SEC\_C\_COM\_8 | Ces outils de contrôles doivent être régulièrement mis à jour (par exemple en déployant les signatures les plus récentes lorsqu'elles sont disponibles) pour assurer la détection, la prévention des logiciels malveillants avancés. |
| SEC\_C\_COM\_16 | En cas d'utilisation d'infrastructures partagées, le Titulaire doit s'assurer de la séparation logique des données de l'ACOSS. |
| SEC\_C\_COM\_17 | Il est souhaité que le Titulaire utilise le chiffrement pour transmettre ou recevoir les données sensibles de l'ACOSS. |
| SEC\_C\_COM\_21 | Le Titulaire doit s'assurer que des contrôles sont définis et mis en œuvre pour empêcher l'accès non autorisé aux informations de l'ACOSS hébergées dans le SI du Titulaire. |
| SEC\_C\_COM\_22 | Le Titulaire doit configurer de façon sécurisée les équipements de sécurité interconnectés au SI ACOSS, afin de n'autoriser que le trafic identifié et strictement nécessaire. |
| SEC\_C\_COM\_26 | Le Titulaire doit s'assurer que les journaux des événements permette de déterminer qui a fait quoi à quel moment, et soient archivés pour un minimum de 90 jours. |
| SEC\_C\_COM\_31 | Le Titulaire doit s'assurer que des contrôles sont en place pour signaler tout dysfonctionnement sur les systèmes contenant des informations appartenant à l'ACOSS et que des mesures correctives sont prises. |
| SEC\_C\_COM\_32 | Sur ses postes de travail utilisateur ayant accès aux informations de l'ACOSS, le Titulaire doit mettre en oeuvre des contrôles de filtrage de l'accès et de protection à Internet. |
|  | **Contrôle d'accès** |
| SEC\_C\_ACC\_1 | Le Titulaire doit disposer d'une politique de contrôle d'accès à son système d'information et ses données. |
| SEC\_C\_ACC\_3 | Le Titulaire doit disposer de processus et de procédures formels pour prendre en charge la création, la modification et la suppression sécurisées de comptes d'utilisateurs dans le système ou les applications. |
| SEC\_C\_ACC\_4 | Le Titulaire doit assurer régulièrement une revue des comptes des utilisateurs de son SI (privilèges, inactivité, …). |
| SEC\_C\_ACC\_5 | Il est souhaité que le Titulaire puisse disposer de mécanismes d'authentification et de contrôle d'accès à l'état de l'art. |
| SEC\_C\_ACC\_6 | Il est souhaité que le Titulaire puisse disposer de contrôles permettant l'examen des droits d'accès |
| SEC\_C\_ACC\_7 | Le Titulaire doit surveiller en permanence l'utilisation non autorisée des comptes d'utilisateurs privilégiés. |
| SEC\_C\_ACC\_11 | Le Titulaire doit pouvoir identifier sur demande de l'ACOSS les personnes ayant accès aux données, informations, codes source de l'ACOSS. |
| SEC\_C\_ACC\_12 | Le Titulaire doit s'assurer que l'accès à distance à ses systèmes et applications s'effectuent avec une authentification à deux facteurs et des mesures de chiffrement. |
| SEC\_C\_ACC\_18 | Le Titulaire doit séparer les systèmes et réseaux contenant des informations appartenant à l'ACOSS des systèmes internes prenant en charge les activités non-ACOSS afin d'empêcher le transfert d'informations entre des environnements différents. |
| SEC\_C\_ACC\_26 | Le Titulaire doit disposer d'une politique formalisée pour protéger l'informatique mobile (smartphones, tablettes et ordinateurs portables, par exemple). |
| SEC\_C\_ACC\_27 | Le Titulaire doit s'assurer que les appareils mobiles et les systèmes de stockage externes sont chiffrés avant d'autoriser le stockage de données de l'ACOSS. |
| SEC\_C\_ACC\_29 | Il est souhaité que le Titulaire puisse empêcher le personnel d'avoir des droits d'accès administrateur sur les terminaux ayant accès aux informations de l'ACOSS afin de minimiser la surface d'attaque des logiciels malveillants. |
|  | **Acquisition, Développement et Maintenance des Systèmes d'Information** |
| SEC\_C\_DEV\_4 | Il est souhaité que le Titulaire puisse disposer d'une politique de gestion des mécanismes cryptographiques mis en œuvre pour la protection des informationsqui lui sont confiées par l'ACOSS. |
| SEC\_C\_DEV\_6 | Il est souhaité que le Titulaire puisse limiter l'installation de logiciels sur les terminaux qui accèdent aux données ou au SI de l'ACOSS uniquement aux utilisateurs autorisés. |
| SEC\_C\_DEV\_8 | Le Titulaire doit s'assurer que les jeux de tests utilisés ne sont constitués que de données anonymisées. |
| SEC\_C\_DEV\_10 | Le Titulaire doit utiliser un outil de gestion de code pour s'assurer que le code est accessible uniquement par les développeurs autorisés et pour permettre un suivi des modifications. |
| SEC\_C\_DEV\_11 | Il est souhaité que le Titulaire puisse mettre en place des procédures formalisées de contrôle des modifications afin de maintenir la sécurité de l'application tout en minimisant l'impact sur les informations appartenant à l'ACOSS. |
| SEC\_C\_DEV\_13 | Le Titulaire doit s'assurer que les modifications apportées au code des applications de l'ACOSS sont rigoureusement testées pour s'assurer qu'elles ne compromettent pas la sécurité de l'application, des données ou du SI de l'Acoss . |
| SEC\_C\_DEV\_14 | Le Titulaire doit mettre en place des contrôles pour éviter les fuites d'informations de l'ACOSS(par exemple une solution DLP). |
| SEC\_C\_DEV\_17 | Les correctifs de sécurité doivent être appliqués mensuellement sur les actifs (OS et applications) nécessaires à la réalisation du service pour l'ACOSS. |
| SEC\_C\_DEV\_23 | Le Titulaire doit disposer d'une politique pour le développement d'applications couvrant l’ensemble du cycle de vie du développement de systèmes (SDLC). |
| SEC\_C\_DEV\_24 | Le Titulaire forme obligatoirement son personnel sur le développement sécurisé et les vulnérabilités classiques. Il garantit à l’ACOSS que cette formation sera régulièrement renouvelée, au maximum tous les trois ans, et dûment mise à jour |
| SEC\_C\_DEV\_25 | Le Titulaire doit utiliser des outils tels que l'analyse de code ou les scanners de vulnérabilités, et vérifier la correction des résultats liés à la sécurité pour garantir l'absence de vulnérabilités dans le code livré à l'ACOSS. |
| SEC\_C\_DEV\_26 | Pour chaque projet une personne disposant des compétences en sécurité technique (architecture et développement) doit être nommée par le Titulaire. Elle apportera son expertise aux équipes projets du Titulaire durant les différentes étapes du cycle de vie des projets. |
| SEC\_C\_DEV\_27 | La sécurité doit être intégrée nativement dans tous les projets conduits par le Titulaire. A ce titre, celui-ci doit documenter les mesures mises en œuvre pour répondre à ce besoin. |
|  | **Gestion des Incidents** |
| SEC\_C\_INC\_1 | Le Titulaire doit disposer d'un processus pour informer l'équipe de sécurité ACOSS dans un délai de 12 heures en cas d'incident impliquant ses systèmes d'information |
| SEC\_C\_INC\_2 | Le Titulaire doit disposer de processus pour collaborer avec l'ACOSS et d'autres parties concernées pour isoler l'incident, identifier la nature de l'incident, déterminer l'ampleur de l'impact et travailler à la reprise des activités normales sur tous les systèmes affectés par un incident. |
| SEC\_C\_INC\_3 | Le Titulaire doit disposer de processus et de procédures pour gérer les communications liées aux incidents, afin de garantir que des informations relatives à l'ACOSS ne soient pas divulguées sans l'approbation du RSSI ACOSS, sauf si la loi l'exige. |
| SEC\_C\_INC\_4 | Il est souhaité que le Titulaire dispose d'un processus permettant à son personnel d'informer immédiatement l'équipe sécurité de l'ACOSS de toute activité suspecte, de toute faiblesse ou de toute violation concernant les données, applications ou toute autres éléments en lien avec le SI de l'Acoss. |
| SEC\_C\_INC\_5 | Le Titulaire doit disposer de procédures détaillées de réponse aux incidents. |
| SEC\_C\_INC\_6 | Il est souhaité que le Titulaire dispose d'un plan formalisé d'intervention sur incident présentant l'articulation de l'ensemble des procédures concernées. |
| SEC\_C\_INC\_7 | Le Titulaire doit utiliser un système de suivi des incidents pour enregistrer les informations liés aux données ou aux prestations pour l’ACOSS. |
| SEC\_C\_INC\_8 | Le Titulaire doit disposer de procédures pour garantir que l'intégrité des données relatives à un incident de sécurité est préservée au cas où cela serait requis par un tribunal. |
|  | **Gestion de la Continuité d'Activité** |
| SEC\_C\_CONT\_1 | Le Titulaire doit maintenir un plan formalisé garantissant la continuité des activités relatives aux prestations pour l'Acoss. |
| SEC\_C\_CONT\_2 | Le plan de continuité des activités doit assurer la disponibilité des services conformément aux objectifs de temps de récupération établis dans le contrat ou l'accord de niveau de service. |
| SEC\_C\_CONT\_5 | Le Titulaire doit disposer d'un plan de reprise après sinistre. |
| SEC\_C\_CONT\_6 | Le plan de reprise après sinistre doit assurer la disponibilité des services conformément aux objectifs de temps de rétablissement établis dans le contrat ou l'accord de niveau de service. |
| SEC\_C\_CONT\_7 | Le Titulaire doit tester les plans de continuité d'activité et de reprise après sinistre. |
|  | **Conformité** |
| SEC\_C\_CONF\_1 | Les données de l'ACOSS doivent être traitées, stockées, sauvegardées en France, à minima en Europe. Les exceptions doivent être documentées, expliquées par des besoins métiers et approuvées par l'ACOSS. Elles font alors l'objet d'un Plan d'Assurance Sécurité et d'exigences particulières définies à l'initialisation de la prestation. |
| SEC\_C\_CONF\_6 | Le Titulaire doit maintenir un inventaire des systèmes contenant des données de l'ACOSS. |
| SEC\_C\_CONF\_7 | Le Titulaire doit disposer de procédures et de politiques garantissant qu'elle respecte toutes les exigences légales et réglementaires relatives aux contrôles cryptographiques, telles que les restrictions à l'exportation des algorithmes de chiffrement. |
| SEC\_C\_CONF\_8 | Il est souhaité que le Titulaire puisse disposer de preuves démontrant la conformité à toutes les politiques et normes de sécurité relatives aux actifs et aux informations de l'ACOSS. |
| SEC\_C\_CONF\_9 | Il est souhaité que le Titulaire puisse planifier toutes les activités d'audit, les tests et les revues des systèmes d'exploitation pour éviter tout impact sur la disponibilité des systèmes nécessaires aux prestations. |
| SEC\_C\_CONF\_10 | L'ACOSS ou un tiers mandaté doit être autorisé à réaliser des audits (fonctionnels et tests d'intrusion) de la solution / des système(s) sur le périmètre de prestations pour l'ACOSS. |
| SEC\_C\_CONF\_11 | Le Titulaire doit s'engager à coopérer à toute investigation (par exemple par les autorités de police ou les autorités de contrôle) impliquant les systèmes, les applications ou les informations de l'ACOSS et à coopérer avec l'ACOSS pour soutenir ces enquêtes. |
| SEC\_C\_CONF\_13 | Il est souhaité que le Titulaire puisse analyser les performances et l'efficacité de la sécurité de l'information en ce qui concerne la conformité à ses politiques et normes de sécurité et peut remonter ces résultats à sa direction générale au moins une fois par an. |
| SEC\_C\_CONF\_15 | Il est souhaité que le Titulaire dispose d’un inventaire et d’une cartographie des systèmes d’information dont il a la charge et les maintienne, selon les préconisations de l’ANSSI issues du guide « cartographie des systèmes d’information ». L’inventaire et la cartographie comprennent également la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes avec leur configuration. Ils comportent une base de données de configuration. |