



**PREMIER  
MINISTRE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général de la défense  
et de la sécurité nationale**

**Cahier des clauses  
techniques particulières  
n° 2025-06 du 25 mars 2025**

**Accord-cadre de techniques de l'information et de la communication**

**Pouvoir adjudicateur contractant :**

L'État – Services du Premier ministre  
Secrétariat général de la défense et de la sécurité nationale (SGDSN)  
51, bd de La Tour-Maubourg - 75700 Paris 07 SP

**Objet de l'accord-cadre :**

Production de parcours de formation sur des sujets variés de la cybersécurité et  
hébergement de ces parcours sur une plateforme de formations en ligne.

## **SOMMAIRE**

<b>Article 1 - Présentation générale du projet .....</b>	<b>5</b>
1.1 Introduction.....	5
1.2 Présentation du centre de formation à la sécurité des systèmes d'information .....	5
1.3 Origine et motivation du projet.....	6
<b>Article 2 - Public concerné .....</b>	<b>8</b>
<b>Article 3 - Pilotage et parties prenantes au projet.....</b>	<b>8</b>
<b>Article 4 - Prestations attendues.....</b>	<b>10</b>
4.1 Présentation générale .....	10
4.2 Définition des postes .....	11
4.2.1 Prestation forfaitaire .....	11
4.2.2 Prestation à bons de commande .....	13
4.3 Structure des différents parcours de formation à la cybersécurité .....	14
4.4 Réalisation du « design d'animation » .....	15
4.5 Accessibilité numérique de la plateforme.....	15
4.6 Propriété des contenus .....	15
4.7 Tests d'évaluation.....	16
<b>Article 5 - Exigences techniques.....</b>	<b>16</b>
5.1 Plateforme d'enseignement à distance .....	16
5.2 Contraintes techniques.....	17
5.3 Contraintes de sécurité.....	17
5.4 Garantie d'accès .....	18
5.5 Traçabilité des données utilisateurs .....	18
5.6 Garantie de disponibilité du service.....	18
5.7 Garantie de temps de rétablissement de l'infrastructure.....	18
5.8 Pénalités en cas de non-respect du temps de rétablissement de l'infrastructure .....	19

5.9	Licence illimitée en nombre d'utilisateurs.....	19
5.10	Navigation et orientation.....	19
5.11	Utilisation des résultats de l'accord-cadre et cession des droits.....	19
5.12	Charte graphique.....	19
5.13	Marque blanche .....	20
5.14	Allotissement, cotraitance et sous-traitance.....	20
<b>Article 6 -</b>	<b>Organisation des prestations du poste n° 1 .....</b>	<b>20</b>
6.1	Création de trois parcours sur la formation « Sensibilisation à la Cybersécurité » .....	20
6.2	Date de livraison des trois parcours de formations .....	23
6.3	Procédure de validation .....	23
6.4	Suivi du projet .....	23
6.4.1	<i>Réunion de lancement</i> .....	23
6.4.2	<i>Réunions d'avancement</i> .....	24
6.4.3	<i>Compte rendu de l'exécution des prestations du poste n° 1</i> .....	24
6.4.4	<i>Point sécurité sur l'exécution de l'accord-cadre</i> .....	24
<b>Article 7 -</b>	<b>Organisation des prestations du poste n° 2.....</b>	<b>24</b>
7.1	Exigences relatives à l'hébergement.....	24
7.2	Suivi du projet .....	24
7.3	Réunions de suivi .....	25
<b>Article 8 -</b>	<b>Organisation des prestations du poste n° 3.....</b>	<b>25</b>
8.1	Création de parcours et de modules de formation supplémentaires .....	25
8.2	Modalités d'établissement des prestations du poste n° 3 .....	26
8.2.1	<i>Demande du pouvoir adjudicateur</i> .....	26
8.2.2	<i>Devis estimatif</i> .....	27
8.2.3	<i>Exécution des prestations</i> .....	27
8.3	Date de livraison de ces différents parcours de formations .....	27
8.4	Procédure de validation .....	27

8.5 Suivi du projet .....	28
8.5.1 Réunion de lancement .....	28
8.5.2 Réunions d'avancement .....	28
8.5.3 Compte rendu de l'exécution des prestations du poste n° 3.....	28
8.5.4 Point sécurité sur l'exécution de l'accord-cadre .....	28

## **Article 9 - Référentiels applicables ..... 29**

9.1 Le Référentiel Général d'Accessibilité pour les Administrations (RGAA) .....	29
9.2 Le Design Système de l'État (DSFR) .....	29
9.3 Le Référentiel Général de Sécurité (RGS) .....	30
9.4 Le Règlement Général de Protection des Données (RGPD).....	31

## **Annexe : Exigences particulières de sécurité**

## **Article 1 - Présentation générale du projet**

### **1.1 Introduction**

L'Agence nationale de la sécurité des systèmes d'information (dénommée ANSSI dans le présent document) est un service à compétence nationale placé sous l'autorité du Premier ministre et rattaché au secrétaire général de la défense et de la sécurité nationale.

L'article 6 du décret n° 2009-834 du 7 juillet 2009 portant création de l'ANSSI prévoit que celle-ci favorise la prise en compte de la sécurité dans le développement des technologies de l'information et de la communication (TIC) et qu'elle contribue à la promotion des technologies et des savoir-faire nationaux en matière de sécurité des systèmes d'information (SSI). L'accompagnement de la montée en compétence cyber de ses bénéficiaires, au travers notamment de la formation, est une des missions confiées à l'ANSSI. L'Agence a également vocation à sensibiliser massivement le grand public aux enjeux de la cybersécurité et à le former sur les règles de base d'hygiène informatique.

Ce projet a pour objectif de créer une plateforme de formations en ligne dénommée « SecNumacadémie » contenant des parcours de formation, sur des sujets variés de la cybersécurité. Le public visé est relativement large : il pourra aller du grand public (totalement novice sur le sujet et pour lequel il pourra être proposé de suivre des parcours de sensibilisation à la cybersécurité), aux agents d'entités concernées de près ou de loin par les problématiques de la cybersécurité (pour lesquels des parcours de difficulté moyenne pourront être proposés), jusqu'aux professionnels aguerris de la cybersécurité (qui pourront trouver des formations plus avancées sur le domaine).

### **1.2 Présentation du centre de formation à la sécurité des systèmes d'information**

Au sein de la sous-direction expertise de l'ANSSI, le Centre de formation à la sécurité des systèmes d'information (CFSSI) intervient dans la définition et la mise en œuvre de la politique de formation en sécurité des systèmes d'information de l'ANSSI. Il propose des formations dispensées par des experts de l'ANSSI au profit d'agents de la fonction publique et de certains opérateurs d'importance vitale (OIV), sous la forme de stages courts et d'un cycle long permettant d'obtenir le titre d'expert en sécurité des systèmes d'information (ESSI). Le CFSSI est également impliqué dans plusieurs projets visant à promouvoir la reconnaissance de formations continues ou initiales dans le domaine de la sécurité des systèmes d'information (notamment par l'attribution de labels) et à sensibiliser le grand public (et les jeunes en particulier) aux bons usages du numérique.

Le CFSSI assurera la maîtrise d'ouvrage du projet.

### 1.3 Origine et motivation du projet

L'une des missions du CFSSI est d'accompagner la montée en compétence cyber des bénéficiaires de l'ANSSI en leur proposant une offre de formation adaptée à leurs besoins. Le centre de formation propose ainsi, à titre gratuit, une trentaine de formations en cybersécurité, dispensées par des experts de l'Agence, à la pointe dans leur domaine. Le CFSSI contribue également massivement à la sensibilisation du grand public (mais également des salariés des entreprises) au travers de son MOOC « SecNumAcadémie », mis en ligne en 2017 présentant un panorama de la cybersécurité ainsi que les règles de bonne conduite en matière de sécurité informatique. Ce MOOC est un réel succès puisque l'on compte aujourd'hui plus de 400 000 inscrits sur la plateforme parmi lesquels un peu plus de 100 000 ont suivi le parcours dans son intégralité.

La prise de conscience collective que la cybersécurité est devenue une problématique qui touche l'ensemble des entités économiques et l'adoption prochaine de la loi transcrivant en droit français la directive (UE) 2022/2555 du parlement européen et du conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union dite « Directive NIS2 », font apparaître une nouvelle population de bénéficiaires, plus massive et en demande d'accompagnement à très courts termes pour répondre à leurs nouvelles obligations légales. Les offres proposées aujourd'hui par l'Agence, pour accompagner la montée en compétences de ces acteurs, deviennent trop limitées et moins adaptées aux besoins :

- Les bénéficiaires concernés par les offres de formations du CFSSI sont aujourd'hui trop nombreux pour pouvoir bénéficier de ces offres en quantité raisonnable. Par ailleurs, ils ne disposent pas toujours de moyens ou de ressources financières leur permettant d'accéder à des offres de formations extérieures, payantes.
- Les salariés d'entreprises privées souhaitant se former à la cybersécurité, au travers du MOOC notamment, ne disposent pas nécessairement du temps nécessaire au suivi de ce parcours dans son intégralité (20h de cours environ). Par ailleurs, le suivi d'une partie de ce parcours ne leur permet pas d'obtenir une attestation, de la part de l'ANSSI, attestation qui leur est parfois demandée dans le cadre de leur activité professionnelle. La durée du parcours actuel du MOOC ne semble donc plus adaptée à la demande.
- De nombreuses entités qui se considéraient auparavant comme « non concernées » par les problématiques de cybersécurité, vont très prochainement se retrouver impliquées par l'application de la directive NIS2. Le nombre d'entités souhaitant monter en compétences sur ce domaine va donc passer de quelques centaines à plusieurs milliers. Les offres proposées par l'ANSSI en termes d'accompagnement de ces bénéficiaires seront donc trop limitées et le besoin de proposer des outils numériques/solutions de formations adaptées à ce type de public se fait de plus en plus pressent.

L'objectif de ce projet est donc de mettre à disposition de l'ensemble de ces entités, une nouvelle plateforme d'apprentissage en ligne, contenant de nombreux parcours de formations en cybersécurité. Ces parcours pourraient, pour certains, s'adresser aux novices dans le domaine et proposer des formations de niveau « sensibilisation » en matière de cybersécurité, pour d'autres, s'adresser à des salariés d'entités en lien avec la cybersécurité et souhaitant se former sur des sujets variés du domaine et sur des thématiques d'actualité, par exemple. Enfin, pour les professionnels de la cybersécurité, cette plateforme pourrait proposer des formations de niveau plus avancé sur le domaine.

Les sujets suivants pourraient être abordés dans ces parcours : application de la directive NIS2, cryptographie post-quantique, gestion de crise au sein des entreprises, remédiation (ou encore comment se relever après avoir subi une crise cyber), etc.

L'ANSSI dispose déjà d'une plateforme de formation en ligne, mais celle-ci ne peut prendre en compte les besoins évolutifs des utilisateurs. En effet, elle propose une seule séquence de formation de 20h et il n'est pas possible d'ajouter de nouveaux parcours de formations sans une refonte complète de la plateforme et de son contenu. Par conséquent, à la date de fin du marché d'hébergement de la plateforme actuelle, l'Agence souhaite disposer d'une nouvelle plateforme modulaire adaptable aux profils et besoins des utilisateurs et qui soit évolutive, permettant ainsi une intégration facilitée de nouveaux parcours de formations en ligne.

Cette nouvelle plateforme est l'objet du présent accord-cadre.

Au travers de cet accord-cadre, l'ANSSI cherche donc à :

- Produire différents parcours de formations avec des niveaux de difficulté variés, permettant d'accompagner de nombreux bénéficiaires (grand public, salariés d'entreprises quel que soit le secteur d'activité, professionnels de la cybersécurité, etc.), à monter en compétence dans le domaine de la cybersécurité.
- Faire héberger l'ensemble de ces parcours, sur une plateforme unique de formation en ligne. Cette plateforme doit être évolutive afin de permettre d'héberger des nouveaux parcours de formations qui pourront être créés au fil de l'eau.

Le présent document, constituant le cahier des clauses techniques particulières (dénommé « CCTP »), a pour objet de décrire les prestations et les livrables attendus de l'accord-cadre, à savoir l'accompagnement de l'ANSSI dans la production de multiples parcours de formations dans le domaine de la cybersécurité (avec des niveaux de difficultés variés), ainsi que leur hébergement sur une plateforme commune d'enseignement à distance (numéro de référence 80420000-4 - Services d'enseignement par voie électronique- de la nomenclature CPV).

## Article 2 - Public concerné

Dans le présent CCTP, le public est désigné par le terme « apprenants ».

L'objectif du projet est de mettre en place une plateforme de formation, sur laquelle des utilisateurs, aux profils variés, pourront venir se former sur le sujet de la cybersécurité. Trois types de profil sont identifiés :

- Le grand public, qui viendra sur la plateforme pour se « sensibiliser à la cybersécurité » et apprendre des règles de bonnes pratiques dans leur usage de l'informatique ; Ce public pourra également se former sur des sujets d'actualités en cybersécurité ;
- Des agents d'entités publiques ou privées (entités essentielles (EE) et entités importantes (EI) par exemple), qui viendront sur la plateforme afin de monter en compétence en cybersécurité. Ce type de public pourra également, bien évidemment, trouver des formations sur des sujets d'actualités (NIS2, gestion de crise, etc.) en lien avec leur activité professionnelle ;
- Des professionnels de la cybersécurité, qui pourront trouver, sur la plateforme, des parcours de formation à la cybersécurité sur des sujets parfois très techniques.

L'objectif est de pouvoir contenter l'ensemble de ces apprenants sur une même plateforme, avec un parcours adapté pour chacun d'eux. Il ne s'agira pas de restreindre l'accès à certains parcours de formation, selon les profils des apprenants mais plutôt de les guider sur la plateforme selon leur niveau d'expertise sur le sujet.

A la fin de chaque module de formation (ainsi qu'à la fin de chaque parcours de formation), les apprenants pourront télécharger une attestation de suivi, précisant le sujet du module (ou du parcours le cas échéant), ainsi que son niveau de difficulté.

Ces parcours de formation devront être ouverts à tous et accessibles gratuitement.

## Article 3 - Pilotage et parties prenantes au projet

La réalisation de ces parcours de formation en ligne est un moyen d'atteindre un objectif : faire monter en compétence cyber les bénéficiaires de l'ANSSI, sensibiliser le grand public aux problématiques de la cybersécurité, mais également aider les agents d'entités privées et publiques à mieux comprendre les enjeux de la cybersécurité.

Un tel projet ne peut réussir sans la mise en place d'une collaboration regroupant différentes compétences :

- Celles de l'ANSSI pour la production des contenus techniques et scientifiques, ainsi que la maîtrise d'ouvrage (formateurs – administrateur – bureau communication- juristes). Les référents techniques réalisant les contenus, sont désignés par le terme « formateur ». Le CFSSI est l'administrateur du projet et il est désigné par le terme « responsable technique » pour le pouvoir adjudicateur. Le bureau communication s'assure que le message s'inscrit dans la politique de communication de l'ANSSI.



- Celles du titulaire qui sera (seul ou en association) :
  1. Spécialiste de l'ingénierie pédagogique et de la gestion de projet multimédia pour effectuer les scénarisations adaptées à la pédagogie spécifique de l'enseignement en ligne ;
  2. Créateur de produits audiovisuels, spécialiste de la conception, de la production et de la publication de contenus rationalisés pour la réalisation technique des formations ;
  3. Hébergeur des parcours de formation à la sécurité des systèmes d'information sur une plateforme commune d'enseignement à distance dont il est propriétaire.
  4. Responsable/gestionnaire du support (SAV) des utilisateurs de la plateforme (en ce sens, il devra répondre aux mails envoyés par les apprenants et les aider en cas de problèmes rencontrés sur la plateforme (techniques, pédagogiques, visuels, etc.).

Le titulaire apportera son savoir-faire pédagogique en matière de conception, de production et de publication d'enseignement à distance. Il prendra en charge :

- la relecture critique des contenus en collaboration avec le pouvoir adjudicateur ;
- la recherche de la meilleure présentation pédagogique du contenu, en collaboration avec le pouvoir adjudicateur et en fonction du public visé ;
- la scénarisation des contenus, des illustrations graphiques, vidéo et sonores mettant en valeur les contenus ;
- le conseil et l'assistance en matière de conception de parcours de formation d'enseignement en ligne ;
- la réalisation technique des parcours de formation à la sécurité des systèmes d'information et la mise à jour des contenus de la plateforme.
- la formation à l'utilisation d'outils permettant de visualiser et de recueillir les statistiques des apprenants sur la plateforme (nombre d'attestations émises, niveau atteint, etc.).
- la fourniture des contenus sous un format standard (exemple : SCORM ou équivalent). Pour information, la sous-traitance et la co-traitance étant autorisées, si le prestataire qui gère la partie « ingénierie » réalise les contenus en fonction des contraintes du prestataire hébergeur de la formation, il devra prévoir une version « générique » des contenus afin que ceux-ci soient accessibles au plus grand nombre et afin de permettre leur réversibilité.

## Article 4 - Prestations attendues

Le titulaire prendra la charge complète de l'adaptation au numérique et de l'intégration des contenus sur la plateforme. Toutefois, le pouvoir adjudicateur aura accès au contenu des parcours de formation en cybersécurité et pourra effectuer des modifications mineures sur ces contenus (exemple : corrections orthographiques, remplacements ou ajouts de liens vers des ressources complémentaires, etc.).

### 4.1 Présentation générale

Les prestations attendues sont les suivantes :

- l'ingénierie pédagogique (adaptation des contenus et réalisation de vidéos) ;
- l'hébergement et la maintenance de la solution pendant la période allant de la date de mise en ligne des prestations du poste n° 1 jusqu'à la date de fin de validité de l'accord-cadre ;
- un soutien à la communication, sous pilotage de l'ANSSI, sur la mise en place de ces parcours de formation ;
- un ajout, au fil de l'eau, de parcours de formation additionnels (ou modules) durant toute la durée de validité de l'accord-cadre, sur des thématiques variées d'actualités, dont le contenu technique sera préparé par les agents de l'ANSSI.

L'accord-cadre est décomposé en deux prestations :

La prestation forfaitaire dont les prestations attendues sont elles-mêmes composées de deux postes distincts :

- o Poste n° 1 : Production de trois parcours de formation sur le thème « Sensibilisation à la cybersécurité », pour des profils utilisateurs de différents niveaux : niveau 1, 2 et 3. La quasi-totalité du contenu de ces parcours proviendra du MOOC actuel de l'ANSSI.
- o Poste n° 2 : Hébergement de ces premiers parcours de formations sur une plateforme de formation en ligne et maintenance corrective et évolutive des contenus et de la plateforme, pour la période allant de la date de mise en ligne des prestations du poste n° 1 jusqu'à la date de fin de validité de l'accord-cadre. La plateforme de formation doit être suffisamment dimensionnée pour héberger un MOOC. Elle devra notamment pouvoir supporter un nombre très important de connexions (proche de 1 million).

La prestation à bons de commande dont les prestations attendues sont composées d'un seul poste :

- o Poste n° 3 : Production de nouveaux parcours de formation à la cybersécurité et de nouveaux modules au sein des parcours existants, puis intégration de ces nouveaux parcours (ou nouveaux modules) au sein de la plateforme de formation en ligne. Ces parcours de formation (ou modules) pourront être de technicité différente et dédiés à des publics relativement variés, sur des thématiques d'importance majeure. Ces parcours ou modules pourront être intégrés au fur et à mesure de leur création, pendant toute la durée de maintenance de la plateforme.

## 4.2 Définition des postes

### 4.2.1 Prestation forfaitaire

Les prestations du poste n° 1 comprennent :

- **La production des trois parcours de formations :**

- « Sensibilisation à la cybersécurité », parcours de niveau 1
- « Sensibilisation à la cybersécurité », parcours de niveau 2
- « Sensibilisation à la cybersécurité », parcours de niveau 3

Pour ce faire, le titulaire :

- récupérera le contenu technique et scientifique du MOOC actuel de l'ANSSI, mis à jour par les agents de l'ANSSI (référents techniques) et découpés selon les trois niveaux de difficulté, par les référents techniques du projet, au sein de l'ANSSI.
- scénarisera ces contenus et adaptera les documents au numérique, en créant des activités pédagogiques, des exercices et en proposant une évaluation en fin de parcours.

Le plan détaillé des contenus de ces trois parcours, sera fourni par les experts de l'ANSSI à la date de notification de l'accord-cadre T<sub>0</sub>. Ces experts seront les référents techniques de ces trois parcours de formation pour le pouvoir adjudicateur. Ils travailleront de concert avec le titulaire, afin d'affiner le détail des contenus ;

- **L'ingénierie pédagogique :** la scénarisation des contenus, l'adaptation au numérique des documents, la création des activités pédagogiques, des exercices et de la certification seront réalisées par le titulaire ;
- **La production multimédia :** la réalisation des vidéos, le cadrage, le montage, la production et la postproduction seront réalisés par le titulaire ; il lui appartient de fournir le matériel et les locaux permettant leur réalisation ;
- **L'accessibilité numérique :** La production multimédia devra prendre en compte les problématiques d'accessibilité pour les personnes en situation de handicap, en se conformant notamment aux exigences du référentiel Général d'amélioration de l'accessibilité RGAA (cf. article 4.5 du présent CCTP) ;
- **Les tests :** la qualité des contenus pédagogiques devra être testée par le titulaire pour en déceler les éventuels défauts et pour juger de leur adéquation avec les attentes du public. Il mettra en place un accès restreint qui permettra également au pouvoir adjudicateur de réaliser ses propres tests.
- **La délivrance d'attestations de suivi.** A la fin de chaque module d'un parcours de formation (ainsi qu'à la fin d'un parcours complet), l'apprenant devra pouvoir télécharger une attestation de suivi, précisant le sujet du module (ou du parcours, le cas échéant), ainsi que son niveau de difficulté.

Les prestations du poste n° 2 comprennent :

- **La publication, l'hébergement et la maintenance** : la mise en ligne sur la plateforme, la synchronisation du plan et des éléments multimédia, l'hébergement des parcours de formation et la maintenance corrective et évolutive de la plateforme seront réalisés par le titulaire, pour la période allant de la date de mise en ligne des prestations du poste n° 1 jusqu'à la date de fin de validité de l'accord-cadre ;
- **L'évaluation des parcours de formations par les apprenants** : les apprenants répondront à un questionnaire élaboré conjointement par le pouvoir adjudicateur et le titulaire et concernant les contenus ainsi que les outils disponibles sur la plateforme. Les réponses obtenues seront analysées en vue de les améliorer ;
- **La formation à la modification des contenus** : il est nécessaire d'optimiser continuellement les contenus afin de les rendre les plus explicites possible, de faire évoluer les parcours de formations pour qu'ils répondent aux attentes des apprenants. Une fois en ligne, la mise à jour des contenus pourra se faire :
  - Soit par le bénéficiaire, lorsque les mises à jour seront minimales (corrections orthographiques, mises à jour de liens web à la marge, ou autres).
  - Soit par le titulaire, dans les autres cas.

Dans tous les cas, le titulaire devra former le bénéficiaire aux outils permettant de mettre à jour les contenus sur la plateforme. Il devra notamment lui donner les accès (administration notamment) nécessaires à de telles mises à jour, sur la plateforme.

- **La mise en place d'une boîte mails** de type SAV permettant aux utilisateurs de remonter les problématiques techniques auxquelles ils sont confrontés (soudis de connexion, difficultés de visualisation des contenus de la formation, difficulté d'évaluation, etc.). Le titulaire devra gérer ces aspects techniques et répondre aux apprenants au fil de l'eau.
- **Le dimensionnement de la plateforme et le choix des outils techniques** permettant d'héberger les différents parcours de formation, doivent permettre un très grand nombre de connexions sur la plateforme (de l'ordre de 1 million d'apprenants).

Le projet doit être scalable.

- **Le suivi statistique des apprenants** permettant au pouvoir adjudicateur de collecter un certain nombre d'indicateurs permettant de juger du bon déroulement des apprentissages, mais également du profil des apprenants, de leur taux de réussite aux différents parcours, etc. Le pouvoir adjudicateur fournira au titulaire une liste d'indicateurs qu'il souhaite pouvoir collecter en mode d'utilisation nominale de la plateforme.

#### 4.2.2 Prestation à bons de commande

Les prestations du poste n° 3 comprennent la production par voie de bons de commande, pendant toute la durée de validité de l'accord cadre, de parcours de formations à la cybersécurité et de modules complémentaires sur des parcours de formation existants.

Les sujets envisagés pour ces parcours, dont les niveaux de difficulté seront variés, pourront être les suivants :

- Formation sur l'application de la directive NIS2 ;
- Formation sur la remédiation (après une attaque cyber) ;
- Formation à la gestion de crise ;
- Initiation à la cryptographie post-quantique ;
- Formation sur le Cloud Sécurisé ;

Ces parcours et modules supplémentaires devront être intégrés au sein de la plateforme de formation en ligne. Ces parcours et modules pourront être intégrés au fur et à mesure de leur création, pendant toute la durée de maintenance de la plateforme. Par ailleurs, ces parcours et modules pourront être dédiés à des publics relativement variés.

Pour chacun de ces modules et parcours, les prestations demandées seront les suivantes :

- **La production d'un parcours ou d'un module de formation sur un thème bien défini**, en lien avec la cybersécurité, et traitant d'une problématique d'actualité majeure. Dans le cas d'un parcours de formation, celui-ci pourra être décliné en différents niveaux de difficulté, tels que, par exemple :

- « Parcours formation thématique », niveau débutant
- « Parcours formation thématique », niveau intermédiaire
- « Parcours formation thématique », niveau avancé

Un plan détaillé des contenus de ces différents parcours, sera fourni par les experts de l'ANSSI à la date de notification du bon de commande. Ces experts seront les référents techniques de ces parcours de formation pour le pouvoir adjudicateur. Ils travailleront de concert avec le titulaire, afin d'affiner le détail des contenus ;

- **L'ingénierie pédagogique** : la scénarisation des contenus, l'adaptation au numérique des documents, la création des activités pédagogiques, des exercices et de l'évaluation finale seront réalisées par le titulaire ;
- **La production multimédia** : la réalisation des vidéos, le cadrage, le montage, la production et la postproduction seront réalisés par le titulaire ; il lui appartient de fournir le matériel et les locaux permettant leur réalisation ;
- **L'accessibilité numérique** : La production multimédia devra prendre en compte les problématiques d'accessibilité numérique des contenus pour les personnes en situation de handicap (cf. article 4.5 du présent CCTP) ;

- **Les tests** : la qualité des contenus pédagogiques devra être testée par le titulaire pour en déceler les éventuels défauts et pour juger de leur adéquation avec les attentes du public. Il mettra en place un accès restreint qui permettra également au pouvoir adjudicateur de réaliser ses propres tests ;
- **La mise en ligne** des parcours obtenus sur la plateforme.

#### 4.3 Structure des différents parcours de formation à la cybersécurité

Un parcours de formation à la cybersécurité sera composé de différents modules dont le nombre pourra varier en fonction de la difficulté du parcours, et selon le profil de l'apprenant et de ses attentes en termes de formation.

Les modules, quant à eux, seront tous construits de la même manière, et seront équilibrés en taille, en nombre d'animations, de vidéos ou d'exercices, afin de répondre aux besoins des différents apprenants.

- Chaque module sera constitué d'un nombre d'unités compris entre 3 et 5 ;
- Une unité correspondra à une durée de formation supérieure à 20 minutes et strictement inférieure à 1h.

Une unité comprend :

- de l'écrit structuré (cours),
- des animations (gifs animés, etc.),
- des vidéos d'une durée maximum de cinq minutes, avec possibilité de lecture en accès direct ou séquentiel,
- des exercices permettant aux apprenants de faire le point sur leurs connaissances. Chaque unité doit contenir au moins une ressource de type graphique (image, schéma, infographie, etc.). La présence et la nature de la ressource seront dictées par un impératif pédagogique : choisir le type de ressource le plus approprié pour mettre en valeur le contenu et retenir l'attention de l'apprenant.

L'utilisation des ressources graphiques (images, schémas, infographies, etc.) doit être pensée pour pouvoir être imprimée pour consultation sans perte d'information.

Les modules pourront également contenir des ressources complémentaires utiles pour approfondir les notions abordées (textes de lois, liens vers des sites Internet, rapports d'étude sur le sujet, documents ppt ou pdf, etc.).

De manière générale, tout type de ressources pourra être inclus, documents bureautiques (PDF, Word, PowerPoint, Excel, Open Office, etc.), animations, fichiers vidéo et/ou audio.

Les contenus finaux devront avoir été pensés en termes d'accessibilité numérique. Ainsi ils devront pouvoir être accessibles aux personnes en situation de handicap (voir article 4.5 du présent CCTP).

Le pouvoir adjudicateur transmettra pour application au titulaire la charte éditoriale de l'ANSSI dès la signature de l'accord-cadre.

#### 4.4 Réalisation du « design d'animation »

Les vidéos de « design d'animation » (*design motion* en anglais) seront réalisées par le titulaire de l'accord-cadre. Dans le cas où des interventions d'acteurs internes de l'ANSSI seraient envisagées (une seule intervention par module d'une durée de trois minutes maximum), le titulaire devra prendre en charge leur préparation avant le tournage.

Le titulaire réalisera également un design d'animation, présentant le parcours de formation (*teaser*), d'une durée maximum de trois minutes.

Les vidéos de « design d'animation » pourront également utiliser le doublage des paroles des acteurs, dès lors qu'ils respecteront le référentiel général de l'amélioration de l'accessibilité (RGAA).

#### 4.5 Accessibilité numérique de la plateforme

Suite au décret numéro 2019-768 du 24 juillet 2019, relatif à l'accessibilité, aux personnes handicapées, des services de communication au public en ligne, la plateforme de formations créée dans le cadre de cet accord-cadre, ainsi que les parcours qu'elle propose devront respecter le RGAA « Référentiel général d'amélioration de l'accessibilité ».

Pour information, l'accessibilité numérique consiste à rendre les services de communication au public en ligne accessibles aux personnes handicapées, c'est-à-dire :

- **perceptibles** : par exemple, faciliter la perception visuelle et auditive du contenu par l'utilisateur ; proposer des équivalents textuels à tout contenu non textuel ; créer un contenu qui puisse être présenté de différentes manières sans perte d'information ni de structure (par exemple avec une mise en page simplifiée) ;
- **utilisables** : par exemple, fournir à l'utilisateur des éléments d'orientation pour naviguer, trouver le contenu ; rendre toutes les fonctionnalités accessibles au clavier ; laisser à l'utilisateur suffisamment de temps pour lire et utiliser le contenu ; ne pas concevoir de contenu susceptible de provoquer des crises d'épilepsie ;
- **compréhensibles** : par exemple, faire en sorte que les pages fonctionnent de manière prévisible ; aider l'utilisateur à corriger les erreurs de saisie.
- **robustes** : par exemple, optimiser la compatibilité avec les utilisations actuelles et futures, y compris avec les technologies d'assistance.

#### 4.6 Propriété des contenus

Le pouvoir adjudicateur sera lui-même titulaire des droits de propriété intellectuelle. En aucun cas, les contenus réalisés ne seront soumis à des droits de propriété intellectuelle tiers.

Les parcours de formation à la sécurité des systèmes d'information auront vocation à être diffusés gratuitement et très largement. Il est donc très important que les modules réalisés puissent être exploités sans aucune limitation technique ou juridique. A cette fin, le pouvoir adjudicateur disposera de l'ensemble des droits permettant d'utiliser, d'exploiter, de diffuser ou de modifier les modules, ceci incluant notamment le droit de les publier en tant que documents publics sous une licence libre permettant l'exploitation par des acteurs publics ou privés, en l'occurrence la licence ouverte Etalab 2.0 (voir [Licence Ouverte Version 2.0](#)).

Par ailleurs, l'ensemble des images et des illustrations utilisées dans le déploiement des modules de formations dans le cadre de cet accord-cadre, devra être libre de droit. Cela signifie, en particulier, qu'elles pourront être réutilisées, par tous, sans contrainte particulière.

Les contenus des modules seront exportables dans un format utilisable par toute plateforme d'enseignement à distance : sous un format standard récent (SCORM ou équivalent). En conséquence, ceux-ci ne doivent pas faire appel à des techniques spécifiques, à un type de matériel ou à un fournisseur, entraînant par la suite le paiement de droits de licences ou d'auteurs ou d'utilisation de brevet.

Le titulaire présentera les formats d'échange des contenus des modules qu'il propose au pouvoir adjudicateur. De plus, le pouvoir adjudicateur devra pouvoir disposer de :

- l'ensemble des animations en motion design,
- l'ensemble des projets de montage et des projets d'effets spéciaux.

Le titulaire proposera des solutions techniques afin de signer numériquement les contenus diffusés (vidéos, pdf, etc.).

Pour information, il est demandé que le CCAP prévoie une clause de propriété intellectuelle permettant à l'ANSSI de disposer de l'ensemble des droits d'utilisation sur les résultats de l'accord-cadre. À ce titre, une proposition de clause d'utilisation des droits rédigée par l'Agence du patrimoine immatériel de l'État (APIE) se trouve en pièce jointe.

#### **4.7 Tests d'évaluation**

La forme privilégiée d'évaluation pourra être le questionnaire à choix multiples (QCM). Cependant, le titulaire pourra proposer au pouvoir adjudicateur, s'il juge cela pertinent, d'autres modalités d'évaluation des apprenants. De manière générale, il conviendra de tirer parti des possibilités les plus pertinentes des supports dynamiques : affichage des résultats des questionnaires à choix multiples, question par question ou consolidés, renvoi des solutions d'exercice à la fin ou affichage par un bouton dynamique, etc.

Il pourra également être proposé des exercices autocorrectifs, pour lesquels une solution complexe est donnée sous forme textuelle, et/ou proposé un renvoi précis à une section du module pour trouver les explications.

## **Article 5 - Exigences techniques**

### **5.1 Plateforme d'enseignement à distance**

La plateforme d'enseignement à distance distribuée par le titulaire regroupera les fonctionnalités nécessaires aux formateurs, aux apprenants et aux administrateurs, permettant de consulter à distance les contenus pédagogiques et l'individualisation de l'apprentissage.

La plateforme proposera un ensemble de fonctionnalités comprenant un serveur de diffusion de contenu et de gestion des profils des apprenants, et un accès au suivi des parcours des apprenants avec mémorisation des résultats obtenus et des progrès.



Plus spécifiquement, elle permettra au service bénéficiaire (notamment au centre de formation) :

- de communiquer par courrier électronique avec les groupes d'apprenants ;
- de consulter des statistiques de fréquentation et de réussite aux exercices ;

Le titulaire devra :

- communiquer, au moyen d'une rubrique éventuellement dédiée sur la plateforme, auprès des apprenants, sur la sortie/mise à disposition de nouveaux modules ou parcours de formation sur la plateforme. Le contenu des messages d'actualités sera établi et validé avec le service communication du bénéficiaire ;
- tester le discours porté sur la plateforme auprès d'un public non-averti pour lequel l'informatique n'est qu'un outil ;
- veiller à la cohérence et à l'homogénéité des parcours ;
- proposer un système d'évaluation des modules et des parcours de formation à la sécurité des systèmes d'information par les apprenants.

## 5.2 Contraintes techniques

La conception et la réalisation des modules doivent être pensées dans une approche de publication multi supports, de consultation multi-contextes, prenant en compte le transfert et l'autonomisation, la réutilisation et la maintenance.

**Transfert et autonomie** : l'accord-cadre comprend le transfert des fichiers sources des modules à l'ANSSI. Ces modules doivent avoir été conçus dans un format accessible et modifiable par le titulaire dans un environnement logiciel que peut prendre en main une compétence informatique standard. Le titulaire respectera la norme SCORM ou proposera une norme reconnue à préciser et à argumenter.

**Réutilisation et maintenance** : de manière à ce que les modules puissent être mis à jour en totalité ou en partie, ou certaines ressources remplacées, et/ou utilisées dans différents modules, il faut faire en sorte que les contenus et les ressources soient isolables en tant que tels (modifier une image ou une animation ou changer une section ne doit pas demander de refaire tout le parcours).

**Multi-navigateur** : les modules doivent être conçus suivant les standards les plus répandus de façon à pouvoir être visualisés par les principaux navigateurs (compatibilité au minimum avec une version stable de Firefox, Internet Explorer, Chrome et Edge) ; les modules de formation à la sécurité des systèmes d'information pourront également être suivis par le biais d'une application utilisable sur ordiphone ou tablette, sous les principaux systèmes d'exploitation (iOS, Android). Aucun plugin ne doit être requis pour accéder à la plateforme et l'utiliser.

## 5.3 Contraintes de sécurité

Les exigences de sécurité concernant la réalisation des prestations sont définies dans l'annexe au présent CCTP « Exigences de sécurité ».

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité. En cas d'évolution, le titulaire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du donneur d'ordres, avant validation par ce dernier.

#### **5.4 Garantie d'accès**

L'accès aux différents parcours de formations à la sécurité des systèmes d'information sera gratuit pour les apprenants s'inscrivant sur la plateforme.

L'inscription se fera par le biais d'une authentification par identifiant et mot de passe. Pour des raisons de statistiques d'analyses des résultats obtenus, il pourra également être demandé, à l'apprenant, de donner le ministère d'origine auquel il est rattaché, tout en respectant les contraintes RGPD (voir Section 9.4 du présent CCTP). En lien avec la protection des données des utilisateurs, le titulaire devra donner aux utilisateurs, s'ils souhaitent ne plus être enregistrés sur la plateforme et qu'ils ne veulent plus poursuivre leur parcours de formation, la possibilité d'effacer eux-mêmes leurs données personnelles.

La plateforme devra permettre un accès simultané de tous les apprenants sans limitation et disposer d'un débit suffisant pour garantir une connexion optimale aux cours.

#### **5.5 Traçabilité des données utilisateurs**

Le titulaire s'engage à fournir au pouvoir adjudicateur les informations de suivi des activités des utilisateurs de la plateforme utile à la vérification de la bonne adéquation de celle-ci au besoin. Le pouvoir adjudicateur recevra à ce titre les informations fournies par les utilisateurs lors de leur inscription (notamment concernant leur activité professionnelle : fonction publique/PME, etc.). D'autre part, le titulaire fournira les données utiles (et non nominatives) de navigation des utilisateurs, permettant par exemple de détecter qu'une portion significative des apprenants ratent un même exercice ou abandonnent au même chapitre, permettant ainsi au pouvoir adjudicateur de pouvoir modifier une portion des contenus qui ne serait pas en adéquation avec les besoins des apprenants.

#### **5.6 Garantie de disponibilité du service**

Le système sera disponible au moins à 99%.

Le titulaire s'engage à mettre en œuvre tous les moyens nécessaires pour rendre accessible le serveur sur sa plateforme d'hébergement 24 heures sur 24, tous les jours de l'année. Toutefois, le titulaire disposera d'un créneau de 4 heures de maintenance par mois sur la plateforme. En cas de nécessité, le titulaire pourra interrompre l'accès au service pour procéder à une intervention technique de maintenance et/ou d'amélioration afin d'assurer le bon fonctionnement du service. Le titulaire fera dans ce cas en sorte d'informer le pouvoir adjudicateur de l'existence et de la durée de l'intervention. Le titulaire procèdera aux opérations de maintenance aux heures où le service est le moins utilisé par les apprenants, sauf dans le cadre d'une maintenance corrective urgente.

#### **5.7 Garantie de temps de rétablissement de l'infrastructure**

La garantie de temps de rétablissement de l'infrastructure est un engagement de réactivité du titulaire qui définit un délai maximum entre la détection d'un dysfonctionnement sur l'infrastructure de la solution et sa remise en service. Ce délai maximum est de quatre heures.

## 5.8 Pénalités en cas de non-respect du temps de rétablissement de l'infrastructure

En cas de non-respect de l'engagement du temps de rétablissement de l'infrastructure de quatre heures, le titulaire sera redevable des indemnités définies ci-après.

Dépassement du délai d'intervention garanti (4h)	Montant des pénalités
De 0 à 2 h de retard	25 % de l'abonnement mensuel du pouvoir adjudicateur
De 2 à 4 h de retard	50 % de l'abonnement mensuel du pouvoir adjudicateur
De 4 à 6 h de retard	75 % de l'abonnement mensuel du pouvoir adjudicateur
Au-delà de 6 h de retard	100 % de l'abonnement mensuel du pouvoir adjudicateur

## 5.9 Licence illimitée en nombre d'utilisateurs

Aucune limitation en nombre d'apprenants ne sera imposée par le titulaire.

## 5.10 Navigation et orientation

La navigation dans un parcours de formation ou dans un module peut être séquentielle (boutons précédent/suivant/retour au début du parcours et/ou du module) ou non-linéaire (pour aller directement à l'une des parties ou l'une des sections ; accès par une table des matières interactive, par exemple).

Un mode d'emploi succinct du parcours (ou du module) doit être accessible par un bouton d'aide.

Chaque page doit comprendre une jauge de défilement de l'animation permettant de connaître, à chaque instant, la durée restante et en particulier de signaler quand celle-ci est terminée.

À chaque instant, l'apprenant doit pouvoir se localiser aisément dans le module et dans son parcours sans être perdu ou désorienté. La multiplication des fenêtres de navigation est à éviter.

## 5.11 Utilisation des résultats de l'accord-cadre et cession des droits

Les modalités d'utilisation des résultats de l'accord-cadre et de cession des droits sont définies à l'annexe du cahier des clauses administratives particulières n° 2025-06 du 26/03/2025.

## 5.12 Charte graphique

La charte graphique gouvernementale pour l'ensemble des pages accessibles en consultation par les usagers du site doit être appliquée. La charte graphique de l'ANSSI devra également être déclinée.

### 5.13 Marque blanche

Le titulaire proposera l'exploitation des modules de formation à la sécurité des systèmes d'information en marque blanche. Il n'apparaîtra pas en tant que titulaire à l'origine de l'information transmise. Seules les références (telles que logos, déclinaison de la charte graphique, etc.) de l'ANSSI seront visibles. Le pouvoir adjudicateur transmettra au titulaire la charte graphique de l'ANSSI ainsi que les outils lui permettant de la décliner sur tous les modules. Le serveur dédié à l'hébergement des contenus devra être lié à une URL de l'ANSSI liée au nom de domaine [cyber.gouv.fr](http://cyber.gouv.fr), ou à une marque qui sera communiquée au titulaire ultérieurement.

### 5.14 Allotissement, cotraitance et sous-traitance

Les différents postes étant liés les uns aux autres (la création de parcours de formations ou de modules se fait en fonction des caractéristiques d'une plateforme donnée), le pouvoir adjudicateur n'est pas en mesure d'allotir l'accord-cadre correspondant à la création des modules de formation à la sécurité des systèmes d'information.

Le titulaire est autorisé à travailler en cotraitance et en sous-traitance. Dans ce cas :

- les cotraitants seront solidaires, et proposeront l'entité représentant le groupement devant le pouvoir adjudicateur, en fonction des compétences de chacun ;
- les curriculum vitae des personnes amenées à travailler sur le projet en sous-traitance seront au préalable présentés au pouvoir adjudicateur afin d'assurer la bonne marche du projet.

## Article 6 - Organisation des prestations du poste n° 1

### 6.1 Création de trois parcours sur la formation « Sensibilisation à la Cybersécurité »

La première formation proposée sur la plateforme aura pour thématique « Sensibilisation à la Cybersécurité ». Cette formation sera composée de l'ensemble des contenus présents sur le MOOC actuel de l'ANSSI, auxquels auront été apportées quelques mises à jour (ajouts, suppressions, correctifs, évolutions, etc.).

La structure globale de cette formation se compose de la manière suivante : (les titres des parties et des sous-parties sont donnés ici à titre indicatif et pourront évoluer).

#### **FORMATION « SENSIBILISATION A LA CYBERSECURITE »**

- Module 1 : Panorama de la SSI
  - Unité 1 Un monde numérique hyper connecté
  - Unité 2 Un monde à hauts risques
  - Unité 3 Les acteurs de la cybersécurité
  - Unité 4. Les règles d'or de la sécurité
  - Unité 5. Mon rôle dans la sécurité numérique

- Module 2 : Sécurité de l'authentification
  - Unité 1. Principes de l'authentification
  - Unité 2. Attaques sur les mots de passe
  - Unité 3. Sécuriser ses mots de passe
  - Unité 4. Gérer ses mots de passe.
  - Unité 5. Pour aller plus loin, notions de cryptographie
- Module 3 : Utilisation du World Wide Web et du Cloud
  - Unité 1. Internet, le Cloud ? De quoi s'agit-il ?
  - Unité 2. Les fichiers en provenance d'Internet
  - Unité 3. La navigation web
  - Unité 4. La messagerie électronique
  - Unité 5. L'envers du décor d'une connexion web
- Module 4 : Sécurité des équipements et nomadisme
  - Unité 1. Applications et mises à jour
  - Unité 2. Options de configuration de base
  - Unité 3. Configurations complémentaires
  - Unité 4. Sécurité des périphériques amovibles
  - Unité 5. Séparation des usages

Les prestations du poste n° 1 comprennent la création des trois parcours de formations suivants :

- « Sensibilisation à la cybersécurité », parcours de niveau 1
- « Sensibilisation à la cybersécurité », parcours de niveau 2
- « Sensibilisation à la cybersécurité », parcours de niveau 3

Ces trois parcours de formation seront construits à partir de la formation « Sensibilisation à la Cybersécurité ». À titre indicatif, voici un exemple de ce à quoi pourraient ressembler les trois parcours de formation en question. Il est à noter, comme précédemment, que les noms des sections et des sous-sections sont donnés ici à titre indicatif et qu'ils pourront être modifiés. Par ailleurs, la structure de chacun de ces parcours pourra être légèrement différente du modèle fourni ici. Le découpage présenté ci-dessous ne constitue qu'un exemple de parcours possibles.

<u>Parcours formation</u>	<u>Parcours formation</u>	<u>Parcours formation</u>
<i>Niveau 1</i>	<i>Niveau 2</i>	<i>Niveau 3</i>
<ul style="list-style-type: none"> <li>- Module 1 <ul style="list-style-type: none"> <li>• Unité 1</li> <li>• Unité 2</li> <li>• Unité 3</li> <li>• Unité 4</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- Module 1 <ul style="list-style-type: none"> <li>• Unité 3</li> <li>• Unité 4</li> </ul> </li> <li>- Module 2 <ul style="list-style-type: none"> <li>• Unité 1</li> <li>• Unité 3</li> </ul> </li> <li>- Module 3 <ul style="list-style-type: none"> <li>• Unité 1</li> <li>• Unité 3</li> <li>• Unité 4</li> </ul> </li> <li>- Module 4 <ul style="list-style-type: none"> <li>• Unité 1</li> <li>• Unité 2</li> <li>• Unité 5</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- Module 1 <ul style="list-style-type: none"> <li>• Unité 3</li> <li>• Unité 4</li> <li>• Unité 5</li> </ul> </li> <li>- Module 2 <ul style="list-style-type: none"> <li>• Unité 2</li> <li>• Unité 4</li> <li>• Unité 5</li> </ul> </li> <li>- Module 3 <ul style="list-style-type: none"> <li>• Unité 1</li> <li>• Unité 2</li> <li>• Unité 5</li> </ul> </li> <li>- Module 4 <ul style="list-style-type: none"> <li>• Unité 2</li> <li>• Unité 3</li> <li>• Unité 4</li> </ul> </li> </ul>

Le plan détaillé final du contenu de ces trois parcours, sera communiqué au titulaire, par les experts de l'ANSSI à la date de notification de l'accord-cadre T<sub>0</sub>. Ces experts seront les référents techniques pour le pouvoir adjudicateur. Ils travailleront de concert avec le titulaire, afin d'affiner le détail des contenus.

L'ANSSI fournira au titulaire l'ensemble des sources du MOOC actuel qu'elle aura à disposition (notamment les fichiers scorm). Le titulaire pourra réutiliser tout ce qui lui est utile (contenus écrits, vidéos, etc.) pour réaliser ces trois parcours de formation dans les meilleures conditions. Par ailleurs, à titre de source d'information complémentaire, l'ANSSI fournira au titulaire en début de prestation, différents documents pertinents en sa possession (supports de cours utilisés au centre de formation à la sécurité des systèmes d'information, guides et notes techniques, etc.).

Le titulaire pourra également consulter et exploiter les documents proposés par l'ANSSI sur les différentes thématiques de la cybersécurité, et notamment ceux disponibles aux adresses suivantes :

- [Guide des bonnes pratiques de l'informatique | ANSSI](#)
- [Se former à la cybersécurité | ANSSI](#)

## 6.2 Date de livraison des trois parcours de formations

Ces trois parcours devront être réalisés en parallèle sur une période qui s'échelonnera entre 6 et 9 mois, à partir de la date de notification de l'accord-cadre T<sub>0</sub>. La date maximale de livraison de ces trois parcours sera fixée à début janvier 2026, afin qu'il n'y ait pas d'interruption entre la fin du marché actuel du MOOC de l'ANSSI et la sortie officielle de cette nouvelle plateforme de formation.

Pour information, les délais de réalisation des parcours de formation mentionnés ici ne tiennent pas compte du temps de vérification des contenus par le pouvoir adjudicateur. La vérification de ces contenus pourra être effectuée tout au long de la prestation, afin de réduire les délais de validation en fin de prestation.

## 6.3 Procédure de validation

Les opérations de vérification nécessaires à la réception des prestations porteront sur leur qualité technique et documentaire.

Chaque parcours de formation sera évalué, tant pour son contenu technique que pour ses qualités pédagogiques, par les experts de l'ANSSI. À l'issue de cette procédure, le parcours pourra être :

- validé en l'état : il est alors déclaré « bon pour le service » et mis en exploitation sur la plateforme du titulaire ;
- validé moyennant un certain nombre de modifications : les modifications devront être effectuées et validées par le pouvoir adjudicateur avant sa mise en exploitation sur la plateforme du titulaire ;
- non validé : le parcours ne sera pas retenu pour être mis en ligne.

Le délai maximum imparti au pouvoir adjudicateur pour procéder aux opérations de vérification des prestations d'un parcours sera compris entre **un mois et un mois et demi** à partir de la date de livraison du parcours, selon la taille de celui-ci.

## 6.4 Suivi du projet

Le titulaire s'engage à informer régulièrement et efficacement l'ANSSI de l'avancée des travaux, et de tout événement susceptible d'avoir un impact sur ces travaux.

### 6.4.1 Réunion de lancement

Une réunion de lancement est fixée pour le démarrage de l'accord-cadre.

Les représentants techniques et administratifs du pouvoir adjudicateur ainsi que les représentants du titulaire, assisteront à cette réunion.

La réunion permettra notamment de préciser le programme et le planning des différentes phases du projet, les étapes intermédiaires, et les modalités de suivi dont, en particulier, le calendrier prévisionnel des réunions d'avancement. Ces précisions ne pourront remettre en cause les documents contractuels de l'accord-cadre.

#### 6.4.2 Réunions d'avancement

Des réunions d'avancement des prestations auront lieu entre le titulaire et le représentant du pouvoir adjudicateur selon le calendrier défini lors de la réunion de lancement. Notamment, une réunion spécifique se tiendra pour le lancement de chaque parcours.

Dans le respect des décisions prises lors de la réunion de lancement, ces réunions s'attacheront à suivre le déroulement de l'exécution des prestations en ce qui concerne notamment :

- l'orientation générale du travail,
- l'avancement de la prestation et le respect des étapes prévues,
- la définition, et le cas échéant, l'ajustement des objectifs à court terme dans le cadre de l'objectif final de l'accord-cadre.

Une réunion mensuelle d'une durée estimée d'une demi-journée pour chacune, permettra de faire un point technique mais aussi de traiter les questions administratives.

Ces réunions se tiendront à Paris, dans les locaux de l'ANSSI. À l'exception de la réunion de conclusion, elles donneront systématiquement lieu à un compte-rendu rédigé sous une semaine par le titulaire et soumis à l'approbation du représentant technique du pouvoir adjudicateur.

#### 6.4.3 Compte rendu de l'exécution des prestations du poste n° 1

Un compte rendu final sur l'exécution des prestations du poste n° 1 de l'accord-cadre sera remis par le titulaire à l'attention du pouvoir adjudicateur sous forme de fichier informatique.

#### 6.4.4 Point sécurité sur l'exécution de l'accord-cadre

Un point trimestriel sera effectué afin de vérifier l'avancement sur la prise en compte de la SSI dans le cycle de vie du projet.

## Article 7 - Organisation des prestations du poste n° 2

### 7.1 Exigences relatives à l'hébergement

L'accord-cadre comprend l'hébergement des parcours de formations à la sécurité des systèmes d'information et de leurs modules ainsi que la maintenance corrective et évolutive des contenus et de la plateforme, pendant la période allant de la date de mise en ligne des prestations du poste n° 1 jusqu'à la date de fin de validité de l'accord-cadre.

Le portail et l'ensemble des informations qu'il contient sera hébergé par un prestataire détenteur d'une qualification SecNumCloud (ou certification équivalente au sens du règlement UE 2019/881).

### 7.2 Suivi du projet

Le titulaire s'engage à rester en contact avec l'ANSSI sur toute la durée de validité de l'accord-cadre. Un point annuel sur l'exécution de l'accord-cadre sera remis par le titulaire à l'attention du pouvoir adjudicateur sous forme de fichier informatique.



### 7.3 Réunions de suivi

Le pouvoir adjudicateur pourra demander jusqu'à quatre réunions annuelles.

Ces réunions de suivi de prestation auront lieu entre le titulaire et le représentant du pouvoir adjudicateur.

Elles s'attacheront à suivre le bon déroulement de l'exécution des prestations en ce qui concerne notamment :

- le bon fonctionnement de la plateforme,
- le bon déroulement de l'exécution des parcours de formation à la sécurité des systèmes d'information,
- l'absence de dysfonctionnements techniques, et le cas échéant, les méthodes qui seront utilisées pour y remédier,
- l'avancement de la prise en compte de la SSI dans le cycle de vie du projet.

Ces réunions se tiendront à Paris, dans les locaux de l'ANSSI, et elles donneront systématiquement lieu à un compte-rendu rédigé sous une semaine par le titulaire et soumis à l'approbation du représentant technique du pouvoir adjudicateur.

## Article 8 - Organisation des prestations du poste n° 3

### 8.1 Création de parcours et de modules de formation supplémentaires

Les prestations du poste n° 3 comprennent la création par voie de bons de commande de différents modules ou parcours de formations en cybersécurité, touchant des thématiques d'importance majeure telles que, par exemple, l'application de la directive NIS2, la cryptographie post-quantique, la remédiation, la gestion de crise, etc.

Ces parcours de formations ou modules seront intégrés au sein de la plateforme de formation en ligne au fur et à mesure de leur création, pendant toute la durée de maintenance de la plateforme. Par ailleurs, ces parcours pourront être de technicité différente et dédiés à des publics relativement variés.

Chaque parcours pourrait être décliné pour différents niveaux de difficulté, tels que, par exemple :

- « Formation thématique 1 », parcours niveau débutant
- « Formation thématique 1 », parcours niveau intermédiaire
- « Formation thématique 1 », parcours niveau avancé

Une des premières thématiques envisagées pour la création d'une nouvelle formation serait : « La directive NIS2 et ses impacts ». Une structuration possible de cette formation serait la suivante. Comme précédemment, il est important de noter que cette structure peut évoluer, à la marge, et que les titres des sections et sous-sections peuvent également être différents. Tous les éléments donnés ici le sont à titre informatif.

## **FORMATION « LA DIRECTIVE NIS2 ET SES IMPACTS »**

- Module 1 : NIS 2, une nouvelle réglementation européenne.
  - Unité 1 : Évolution du contexte européen réglementaire
  - Unité 2 : Qui est impacté par cette nouvelle directive ?
  - Unité 3 : Comment catégoriser votre entité ?
- Module 2 : Les obligations liées à NIS2
  - Unité 1 : Obligations administratives (enregistrement, déclaration d'incidents, sanctions possibles, etc.)
  - Unité 2 : Incidents en cybersécurité : de quoi s'agit-il ? comment les identifier ?
  - Unité 3 : 20 Objectifs de sécurité à mettre en œuvre
- Module 3 : En pratique, comment bien sécuriser son organisation ?
  - Unité 1 : Guide pour une bonne « déclaration d'incidents ».
  - Unité 2 : Guide pour une bonne application des objectifs de sécurité
  - Unité 3 : Besoin d'aide : vers qui se tourner ?

Pour le moment, il n'a pas encore été défini de niveaux de difficulté distincts pour cette formation. Il est fort probable qu'un unique parcours soit créé, de niveau « intermédiaire ». Cependant, il est possible que des discussions ultérieures sur ce sujet montrent qu'il est nécessaire de créer deux (ou plusieurs) parcours sur ce sujet, selon les entités ciblées.

### **8.2 Modalités d'établissement des prestations du poste n° 3**

Les prestations fournies par le titulaire au titre du poste n° 3 s'exécutent par l'émission de bons de commande émis par le représentant légal du pouvoir adjudicateur

Le mécanisme d'établissement des bons de commande est défini à partir des prix unitaires indiqués par le titulaire dans l'annexe n° 1 à l'acte d'engagement de l'accord-cadre selon les modalités précisées au présent article.

#### ***8.2.1 Demande du pouvoir adjudicateur***

Le besoin à satisfaire par une commande sera d'abord défini par une expression de besoin fonctionnel du pouvoir adjudicateur, spécifiant la nature et l'étendue des prestations à réaliser, avec notamment un plan détaillé des contenus du parcours de formation à réaliser, qui sera fourni par les experts de l'ANSSI, éventuellement la date limite d'achèvement ou le délai d'exécution impératif ou souhaité ainsi que le délai de production du devis estimatif.

### 8.2.2 Devis estimatif

Sur la base de la demande du pouvoir adjudicateur, le titulaire propose un devis estimatif dans le délai précisé par la demande définie ci-dessus ou, à défaut, dans un délai de vingt jours calendaires, comprenant :

- l'évaluation, à partir des prix unitaires définis à l'annexe n° 1 à l'acte d'engagement de l'accord-cadre, du montant global forfaitaire hors taxes des prestations et sa décomposition,
- le délai de réalisation des prestations exprimé en forfait de nombre de jours de travail / homme.

Le défaut de réponse du titulaire à la demande du pouvoir adjudicateur dans le délai imparti pourra entraîner l'application de pénalités de retard conformément à l'article 3.8 du CCAP.

### 8.2.3 Exécution des prestations

Aucun commencement d'exécution ne pourra avoir lieu avant l'envoi au titulaire d'un bon de commande acceptant le devis par tout moyen permettant de déterminer de façon certaine la date de sa réception.

La réception du bon de commande par le titulaire vaut date de notification et ordre d'exécution des prestations demandées.

## 8.3 Date de livraison de ces différents parcours de formations

Ces parcours de formation seront réalisés, au fil de l'eau, pendant toute la durée de validité de l'accord-cadre. Une nouvelle date de notification sera fixée à chaque nouveau bon de commande lancé. La durée de réalisation d'un (ou plusieurs) parcours associés à une formation donnée, sera fixée entre 6 et 9 mois, à partir de la date de notification du bon de commande concerné.

Pour information, les délais de réalisation des parcours de formation mentionnés ici ne tiennent pas compte du temps de vérification des contenus par le pouvoir adjudicateur.

## 8.4 Procédure de validation

Les opérations de vérification nécessaires à la réception des prestations porteront sur leur qualité technique et documentaire.

Chaque parcours de formation sera évalué, tant pour son contenu technique que pour ses qualités pédagogiques, par les experts de l'ANSSI. À l'issue de cette procédure, le parcours pourra être :

- validé en l'état : il est alors déclaré « bon pour le service » et mis en exploitation sur la plateforme du titulaire ;
- validé moyennant un certain nombre de modifications : les modifications devront être effectuées et validées par le pouvoir adjudicateur avant sa mise en exploitation sur la plateforme du titulaire ;
- non validé : le parcours ne sera pas retenu pour être mis en ligne.

Le délai maximum imparti au pouvoir adjudicateur pour procéder aux opérations de vérification des prestations d'un parcours sera compris entre **un mois et un mois et demi** à partir de la date de livraison du parcours, selon la taille de celui-ci.

## 8.5 Suivi du projet

Le titulaire s'engage à informer régulièrement et efficacement l'ANSSI de l'avancée des travaux, et de tout événement susceptible d'avoir un impact sur ces travaux.

### 8.5.1 Réunion de lancement

Une réunion de lancement est fixée pour le démarrage de chaque nouvelle thématique de formation.

Les représentants techniques et administratifs du pouvoir adjudicateur ainsi que les représentants du titulaire, assisteront à cette réunion.

La réunion permettra notamment de préciser le programme et le planning des différentes phases du projet, les étapes intermédiaires, et les modalités de suivi dont, en particulier, le calendrier prévisionnel des réunions d'avancement. Ces précisions ne pourront remettre en cause les documents contractuels de l'accord-cadre.

### 8.5.2 Réunions d'avancement

Des réunions d'avancement des prestations auront lieu entre le titulaire et le représentant du pouvoir adjudicateur selon le calendrier défini lors de la réunion de lancement. Notamment, une réunion spécifique se tiendra pour le lancement de chaque nouveau module ou nouveau parcours de formation.

Dans le respect des décisions prises lors de la réunion de lancement, ces réunions s'attacheront à suivre le déroulement de l'exécution des prestations en ce qui concerne notamment :

- l'orientation générale du travail,
- l'avancement de la prestation et le respect des étapes prévues,
- la définition, et le cas échéant, l'ajustement des objectifs à court terme dans le cadre de l'objectif final de l'accord-cadre.

Une réunion mensuelle d'une durée estimée d'une demi-journée pour chacune, permettra de faire un point technique mais aussi de traiter les questions administratives.

Ces réunions se tiendront à Paris, dans les locaux de l'ANSSI. À l'exception de la réunion de conclusion, elles donneront systématiquement lieu à un compte-rendu rédigé sous une semaine par le titulaire et soumis à l'approbation du représentant technique du pouvoir adjudicateur.

### 8.5.3 Compte rendu de l'exécution des prestations du poste n° 3

Un compte rendu final sur l'exécution de chacune des prestations du poste n° 3 sera remis par le titulaire à l'attention du pouvoir adjudicateur sous forme de fichier informatique.

### 8.5.4 Point sécurité sur l'exécution de l'accord-cadre

Un point trimestriel sera effectué afin de vérifier l'avancement sur la prise en compte de la SSI dans le cycle de vie du projet.

## Article 9 - Référentiels applicables

La plateforme devra respecter les référentiels généraux obligatoires suivants.

### 9.1 Le Référentiel Général d'Accessibilité pour les Administrations (RGAA)

La loi n° 2005-102 du 11 février 2005 "pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées" instaure au titre de l'article 47, l'obligation pour les services de communication publique en ligne des services de l'État, des collectivités territoriales et des établissements publics qui en dépendent d'être accessibles aux personnes handicapées. Le décret d'application de l'article 47 a été actualisé en 2019. Il permet d'introduire le Référentiel Général d'Accessibilité pour les Administrations (RGAA) pour les modalités techniques de mise en œuvre. L'arrêté relatif au référentiel général d'accessibilité pour les administrations est disponible ici : <https://www.legifrance.gouv.fr/loda/id/LEGIARTI000030541284/2015-05-03#LEGIARTI000030541284>

Ces obligations valent tant pour les publics, que pour la communication interne vers les agents. En conséquence, la conception et la réalisation d'applications web à destination des publics ou des agents de l'État doivent impérativement valider au minimum l'ensemble des tests ayant un niveau WCAG déduit A et AA, ceci afin de répondre aux exigences de conformité définies par le RGAA lors de leur ouverture au public.

Le titulaire s'engage à ce que chacun de ses livrables respecte strictement tous les critères du RGAA, consultable à l'adresse suivante : <https://accessibilite.numerique.gouv.fr/>.

Le titulaire met en œuvre les processus et moyens pour s'assurer de la conformité du code.

### 9.2 Le Design Système de l'État (DSFR)

Le DSFR est le volet numérique de la marque de l'État. Il permet d'avoir une cohérence graphique et une meilleure expérience à travers l'ensemble des sites de l'État. Le Système de Design de l'État regroupe un ensemble de composants réutilisables, répondant à des standards et à une gouvernance, pouvant être assemblés pour créer des sites Internet accessibles et ergonomiques.

Le DSFR vise à :

- concrétiser un ensemble de règles ergonomiques et accessibles en transposant ce qui est possible en éléments prêts à l'emploi pour les designers et développeurs ;
- harmoniser la présence numérique de l'Etat et l'expérience des citoyens.

Le titulaire sera amené à respecter le cadre du DSFR : <https://www.systeme-de-design.gouv.fr/>, notamment pour la page d'accueil de la plateforme de formations.

### 9.3 Le Référentiel Général de Sécurité (RGS)

Le Référentiel Général de Sécurité (RGS) est pris en application du décret n° 2010-112 du 2 février 2010 pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

Dans le cadre du développement des téléservices et des échanges électroniques entre l'administration et les usagers, les autorités administratives doivent garantir la sécurité de leurs systèmes d'information en charge de la mise en œuvre de ces services.

Le RGS s'impose spécifiquement aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et dans leurs relations avec les usagers.

Indirectement, le RGS s'adresse à l'ensemble des prestataires de services qui assistent les autorités administratives dans la sécurisation des échanges électroniques qu'elles mettent en œuvre, ainsi qu'aux industriels dont l'activité est de proposer des produits de sécurité.

- Il est demandé au titulaire de se conformer aux règles et recommandations tirées du RGS <https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs>
- <https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents>

Si le titulaire est informé de l'existence d'une nouvelle vulnérabilité de sécurité, il convient qu'il en informe dans les délais les plus brefs ses équipes techniques ainsi que les équipes techniques du bénéficiaire, incluant les responsables de la sécurité des systèmes d'information (RSSI).

Le titulaire est tenu à une obligation permanente de conseil et de mise en garde du point de vue de la sécurité des systèmes d'information, relative aux logiciels et prestations fournies au bénéficiaire. Dans ce cadre, le titulaire notifie au bénéficiaire toute information permettant d'améliorer le niveau de sécurité du système d'information et signaler les difficultés et risques que certains choix peuvent entraîner.

En termes de développement, le titulaire doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière. Toutefois, il doit respecter les exigences suivantes pour les services Web et de messagerie :

- les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc.) ou une technologie en particulier ;
- les mécanismes cryptographiques TLS (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications; l'utilisation de la technologie HSTS est fortement recommandée ;
- les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
- une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer- Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;

- les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés ;
- si les services de courriels sont mis en œuvre, les mécanismes de chiffrement TLS sont requis pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc.) et l'utilisation des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs SPF, signature numérique par DKIM, politique de sécurité liant le tout par DMARC).

#### **9.4 Le Règlement Général de Protection des Données (RGPD)**

Le Règlement Général de Protection des Données (RGPD) est en vigueur depuis le 25 mai 2018. À ce titre, le titulaire s'engage dès à présent, à respecter les prérogatives imposées par ce nouveau cadre. <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

Le titulaire doit intégrer a minima :

- la gestion des droits utilisateurs en fonction de leur profil,
- la gestion des cycles de vie des données (archivage, anonymisation des données, purge automatique),
- la garantie de la sécurité du flux d'information : méthode de chiffrement, l'hébergement, la portabilité des données,
- une proposition relative aux mentions obligatoires sur le Web,
- les méthodes de développement ne devront pas faire appel à des ressources externes (Javascripts, fonts, images...). Si des ressources sont nécessaires, que cela soit par des développements spécifiques ou des extensions, elles devront être embarquées dans le site web directement.

# Annexe n°1 au CCTP n° 2025-06 du 25 mars 2025

## Exigences particulières de sécurité

### Article 1 - Exigences de sécurité

#### 1.1 Maîtrise des risques de l'hébergement des parcours de formation à la sécurité des systèmes d'information

La solution proposée fera l'objet d'une homologation de sécurité avant sa mise en production. Celle-ci pourra être réalisée avec [MonServiceSécurisé](#). La solution devra respecter, à minima, les recommandations du guide d'hygiène informatique de l'ANSSI et le référentiel général de sécurité (RGS).

La solution proposée devra être conforme aux recommandations de l'ANSSI en termes de sécurité, notamment sur la gestion des mots de passe, l'hébergement, le renforcement de la sécurité des serveurs, le guide de développement des applications, les mesures contre les dénis de services, etc.

La version 2.0 du référentiel général de sécurité prévu à l'article 2 du décret du 2 février 2010 ([Le référentiel général de sécurité \(RGS\) | ANSSI](#)) est applicable aux prestations de l'accord-cadre.

De plus, la plateforme devra être sécurisée selon les bonnes pratiques décrites par les règles de l'Open Web Application Security Project (OWASP) ou par tout autre référentiel dont l'équivalence aura été démontrée par le titulaire.

#### 1.2 Le titulaire mettra en œuvre les moyens prévus dans le cadre du processus d'amélioration continue de la sécurité de ses infrastructures d'hébergement définis dans l'annexe n° 2 à l'acte d'engagement. Mises à jour, correctifs de sécurité

Le titulaire doit assurer une veille technologique de sécurité à travers une analyse des vulnérabilités identifiées sur les applications et infrastructures mises à disposition et si nécessaire la mise en place de solutions de correction ou de contournement. Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles sur tous les matériels dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERT-FR), le correctif doit être appliqué dans un délai de 24 heures sur les infrastructures hébergeant le système du pouvoir adjudicateur (serveurs, pare-feux, routeurs ouverts vers l'extérieur). Lorsqu'aucun correctif n'est disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERT-FR dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenances hebdomadaires ou mensuelles. Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de pré production.

Un « tableau de bord de veille technologique de sécurité » est établi mensuellement par le titulaire. Il synthétise les avis, alertes et incidents de sécurité identifiés et traités avec



le descriptif de leur qualification et les dates de mise en œuvre des différentes actions en cours et prévues. Ceci permet au pouvoir adjudicateur de suivre l'avancement des actions de veille technologique de sécurité.

La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du titulaire et le pouvoir adjudicateur.

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques, le titulaire sera notifié par téléphone et courrier électronique avant toute opération. La décision de l'action ne pourra être prise que par des personnels du pouvoir adjudicateur. En particulier, le responsable sécurité du pouvoir adjudicateur sera le correspondant privilégié pour le suivi des opérations.

Le titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (H24, heures ouvrables, etc.) permettant au pouvoir adjudicateur de suivre le traitement d'une alerte.

En cas d'annonce de fin de support d'un composant de la solution par un des éditeurs ou constructeurs, le titulaire devra proposer une solution de remplacement par une version supportée ou un produit à fonctionnalités équivalentes. La solution de remplacement sera soumise à la validation du pouvoir adjudicateur. Le délai de mise à disposition de la solution proposée par le titulaire sera défini en accord avec le pouvoir adjudicateur et ne pourra excéder 6 mois à compter de la date de fin de support du composant.

### **1.3 Sauvegardes et restauration**

Le titulaire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Les opérations de sauvegardes donnent lieu à un compte-rendu par messagerie avec indicateur de réussite ou d'échec.

La fiabilité des sauvegardes sera mise à l'épreuve par des tests de restauration périodiques, dont les rapports seront communiqués dans le mois suivant les tests.

Un double exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du titulaire hébergeant l'application du donneur d'ordres.

Le titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :

- confidentialité des flux lors des opérations de sauvegardes ;
- stockage sécurisé des sauvegardes.

En cas de sauvegarde externalisée, les sauvegardes doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du titulaire et du donneur d'ordres.

Dans le cadre de plans de sécurité gouvernementaux, le pouvoir adjudicateur pourra imposer une augmentation de la fréquence des sauvegardes.

#### 1.4 Continuité d'activité

Le titulaire doit prendre toutes les mesures techniques, organisationnelles et procédurales nécessaires pour assurer la disponibilité du système d'information, conformément aux exigences définies dans la clause relative au niveau de service exigé.

Les procédures de sauvegarde et de secours seront auditées conformément aux modalités identifiées dans la clause relative aux audits de sécurité.

#### 1.5 Authentification

Les accès à la partie publique de l'application se feront via une authentification basée sur « FranceConnect » ([Franceconnect - Accédez simplement aux services publics](#)) et « ProConnect » ([Accueil - ProConnect](#)), les deux moyens seront proposés aux visiteurs.

Pour la partie privée (administration) de la plateforme, l'authentification se fera uniquement par « ProConnect ».

#### 1.6 Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, TLS, IPsec, etc.), garantissant la confidentialité et l'intégrité des données. De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties. Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du référentiel général de sécurité.

#### 1.7 Contrôle et filtrage des flux

Au titre de la défense en profondeur, trois zones seront mises en place au sein du système d'information, chacune étant protégée par un dispositif de filtrage :

- une zone publique regroupant les machines qui hébergent des services ayant vocation à communiquer avec l'extérieur (Reverse Proxy, Serveur Web, FTP, serveur de mail, DNS, etc.) ;
- une zone privée regroupant les machines n'ayant pas vocation à communiquer avec l'extérieur ;
- un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés chez l'hébergeur.

Le trafic réseau en provenance et à destination du système doit faire l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes. Une matrice de flux (inventaire des flux légitimes) sera fournie par le titulaire.

La politique de filtrage est définie à partir de la matrice des flux. Les dispositifs de filtrage sont bloquants par défaut, tout ce qui n'est pas explicitement autorisé étant interdit.

Le service global doit être protégé contre les attaques classiques sur IP et les protocoles associés (filtrage sanitaire) notamment :

- attaque en déni de service (TCP SYN Flood, Ping Flooding, SMURF, Ping of Death, large packet attacks, etc.) ;
- IP options (*source routing*, etc.).

Les interfaces d'administration des machines ou des équipements du système ne doivent pas être accessibles depuis l'extérieur. Les services correspondants seront donc configurés pour ne pas accepter de connexions sur les interfaces publiques.

Seuls les services utiles au bon fonctionnement de l'application doivent être activés. Les autres services doivent être désactivés et si possible désinstallés.

### **1.8 Imputabilité, traçabilité**

Les informations suivantes devront être enregistrées et journalisées :

- entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ;
- actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :
  - date, heure, identité de l'utilisateur, nom de l'objet ;
  - type de la tentative d'accès, réussite ou échec de la tentative ;
  - création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
  - actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

### **1.9 Marquage des supports de données et équipements sensibles**

Le titulaire devra préciser les mesures mises en œuvre pour assurer le recensement, la classification et le suivi des supports de données et équipements sensibles (boîtiers de chiffrement, pare-feux, etc.).

Le marquage des supports de stockage de données est obligatoire (disque dur, bandes de sauvegardes, etc.).

### **1.10 Stockage sécurisé des informations**

Le titulaire devra préciser les mesures techniques mises en œuvre pour assurer le chiffrement intégral des données sensibles (par exemple les données des comptes utilisateurs) stockées au profit du pouvoir adjudicateur.

## **Article 2 - Sécurité et gestion des évolutions**

### **2.1 Audits de sécurité**

Le pouvoir adjudicateur doit pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le titulaire. Un modèle de convention d'audit de sécurité est fourni à la fin du présent document. Les audits pourront être réalisés par le pouvoir adjudicateur, ou délégués à un tiers. Le contrôle s'effectuera selon des modalités contractuelles définies (visite des locaux du titulaire avec interviews individuelles des membres des équipes du titulaire, accès aux machines mises à la disposition du titulaire). Cette visite sera notifiée au titulaire selon un délai de 15 jours qui permettra à l'hébergeur de s'organiser (rassembler la documentation, s'assurer de la disponibilité des personnes concernées).

### **2.2 Réversibilité**

En raison des investissements importants qu'il nécessite, l'accord-cadre avec le titulaire est destiné à s'inscrire dans la durée. Néanmoins, cette clause de réversibilité permettra au pouvoir adjudicateur de reprendre la gestion des parcours de formation à la sécurité des systèmes d'information, soit pour l'exploiter directement, soit pour en confier l'exploitation à un tiers de son choix. Cette clause pourra être activée à tout moment en respectant le délai légal, et ce, sans justification particulière. Le titulaire s'engage à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des données, et la reprise de leur exploitation par le pouvoir adjudicateur, ou par un autre prestataire de service. Le titulaire s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations.

À la fin de l'exécution de l'accord-cadre, le titulaire est tenu :

- de transférer à l'équipe du futur titulaire les informations sur le contexte fonctionnel et technique de l'ensemble applicatif ainsi que sur les aspects de suivi du projet ;
- de préparer un support informatique défini par le donneur d'ordres contenant tous les éléments (documentations, programmes, chaînes de compilation...) gérés par le titulaire actuel et qui seront, à l'issue de cette prestation, placés sous la responsabilité du futur titulaire (cette mise à disposition devra être faite sous un format pouvant permettre au futur titulaire d'installer, le cas échéant, l'ensemble de ces éléments sur une plateforme de son choix pour examen approfondi par celui-ci) ;
- d'assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) aux personnels du futur titulaire, avec travaux pratiques sur poste de travail, en présence de représentants du donneur d'ordres.

### **2.3 Résiliation**

Dans le cadre d'un manquement grave par le titulaire à l'une des obligations de sécurité mises à sa charge dans l'accord-cadre, le pouvoir adjudicateur pourra le mettre en demeure de réparer ce manquement dans un délai donné. À l'issue de ce délai, si le manquement n'est pas réparé, le pouvoir adjudicateur pourra résilier de plein droit l'accord-cadre. De façon générale, tout manquement aux clauses entraînera des pénalités ou la résiliation.

## **2.4 Correspondant sécurité**

Le titulaire fournira le point de contact du responsable de la sécurité des systèmes d'information (RSSI) en charge de la plateforme. Ce dernier sera l'interlocuteur privilégié du pouvoir adjudicateur pour toutes questions relatives à la sécurité.

## **Article 3 - Bonnes pratiques**

### **3.1 Journaux d'événements et conservation des traces**

Le titulaire est tenu de s'assurer qu'une journalisation des accès et des événements (système, Web, etc.) est activée sur tous les équipements dont il a la charge. Une politique de sauvegarde de ces traces doit exister (deux mois de sauvegarde sont demandés sur les pare-feux et les serveurs Web).

Le pouvoir adjudicateur peut être amené à demander un extrait de ces traces, soit dans le cas d'un incident, soit à des fins de suivi de la (des) ressource(s).

### **3.2 Prévention d'une attaque**

Dans le cadre de l'accord-cadre, l'hébergeur doit prévoir le cas d'éventuelles attaques informatiques. La réactivité en cas d'incident étant extrêmement importante, il conviendra de fournir au pouvoir adjudicateur dans le cadre de l'exécution de l'accord-cadre les points suivants :

- l'identification d'un contact technique (ou plusieurs) clairement identifié chez l'hébergeur ainsi que chez le pouvoir adjudicateur, joignable 24/24, 7/7, tous les jours de l'année,
- l'identification d'un contact décisionnel (ou plusieurs) clairement identifié chez l'hébergeur ainsi que chez le pouvoir adjudicateur, joignable 24/24, 7/7, tous les jours de l'année,
- la garantie d'information immédiate : le pouvoir adjudicateur doit être tenu informé sans délai en cas d'attaque afin de déclencher le circuit de réaction adéquat,
- la définition des procédures de remontée d'incident,
- la définition claire et exhaustive avec l'hébergeur de ce que l'on entend par incident (défiguration, temps d'indisponibilité, etc.).

## **Article 4 - Protocole d'audit des sites du titulaire et de ses sous-traitants impliqués dans les projets du SGDSN**

**Objet** : ce protocole d'audit définit les modalités pratiques suivant lesquelles les audits se dérouleront.

### **4.1 Modalités générales pour l'exécution de l'audit**

Les auditeurs du SGDSN seront accompagnés en permanence par un personnel du titulaire ou sous-traitant, ils auront un badge visiteur pour la durée de l'audit.

Les déplacements dans les locaux sont limités aux zones autorisées dans le cadre de ce protocole, toute autre demande de visite devra être validée par le pilotage de l'audit du titulaire.

Un débriefing rapide « à chaud » de la journée se tiendra en fin d'audit entre les auditeurs et le pilotage de l'audit pour le titulaire constitué de personnes présentes au catalogue des emplois.

### **4.2 Principes généraux pour l'exécution de l'audit**

Le périmètre de l'audit porte sur les infrastructures dédiées au contexte du système audité ou qui permettent d'en assurer directement le bon fonctionnement et la sécurité.

La connexion logique des intervenants du SGDSN sur les infrastructures n'est pas possible à priori.

Les sorties d'informations des sites d'exploitation pourront être réalisées, autant que possible, par les intervenants du titulaire et seront soumises à l'avis de l'Officier de Sécurité du site.

L'entrée de matériel appartenant au SGDSN dans les locaux du titulaire sera soumise à l'accord de l'Officier de Sécurité du site concerné.

L'audit technique ne doit pas engendrer d'indisponibilité du service rendu par le système audité. Le titulaire se donne le droit de ne pas exécuter des commandes système demandées par le SGDSN si le titulaire estime que ces dernières peuvent impacter le bon fonctionnement du service dû par le titulaire au SGDSN.

1. Les audits portent sur toutes les informations et fonctions, au sens EBIOS, affectant le système audité, notamment celles définies dans l'étude EBIOS globale du système, et sur lesquelles portent les exigences de sécurité et les hypothèses de la cible de sécurité. Cela comprend pour le système audité : la sécurité physique des locaux, la sécurité logique des systèmes dédiés, la vérification de l'habilitation/accréditation des personnels et le bon respect des procédures établies et les réglementations en vigueur.

Note : Dans le cas où les locaux font l'objet d'une aptitude physique de l'autorité de tutelle, le SGDSN ne pourra pas exiger de quelconques travaux supplémentaires.

2. Les sites du titulaire ou de ses sous-traitants impliqués directement dans la mise en place ou dans l'exploitation du système audité peuvent être audités par le SGDSN. Pour ces sites, le titulaire ou le sous-traitant concerné autorise aux personnes impliquées dans l'audit l'accès aux locaux et aux informations des systèmes affectant directement le système audité. Conformément à la cible de sécurité, le SGDSN prévient le titulaire de sa venue sur un site au moins quatorze jours auparavant.
3. Les contraintes spécifiques des sites audités sont communiquées par le titulaire au SGDSN au moins cinq jours ouvrés avant la tenue des audits, afin que le groupe d'audit puisse en prendre connaissance avant sa venue sur les sites concernés et puisse vérifier leur compatibilité avec les exigences de l'audit dans la limite des ressources opérationnelles disponibles.
4. Le périmètre global de l'audit (présenté aux paragraphes 1 et 2) est défini entre les parties deux semaines avant la tenue de chaque audit. Sont définis en particulier les domaines exclus du champ de l'audit. Le titulaire ou son sous-traitant mettent à disposition des auditeurs les moyens nécessaires au bon déroulement de l'audit.
5. Les auditeurs peuvent accéder aux sites du titulaire ou de ses sous-traitants avec les matériels informatiques nécessaires à leur audit, tels qu'ordinateurs portables, clés USB, appareils photos numériques, etc., et sont autorisés à s'en servir avec l'autorisation et sous le contrôle de l'Officier de Sécurité du site ou de son représentant dans la mesure où :
  - leur usage n'est pas susceptible d'interférer avec les systèmes d'information sous la responsabilité du titulaire ;
  - aucune donnée à caractère personnel n'est recueillie, et à fortiori utilisée.

La liste exhaustive des matériels et logiciels nécessaires pour l'audit sera envoyé par le SGDSN au titulaire au moins trois jours ouvrés avant la tenue de chaque audit.

Dans le cas d'un recueil d'informations nécessitant une interconnexion avec les réseaux sous la responsabilité du titulaire, les auditeurs du SGDSN pourront :

- en premier choix, utiliser des moyens mis à leur disposition par le titulaire si leurs fonctionnalités sont suffisantes ;
- ou à défaut utiliser des moyens propres après en avoir exposé les fonctions utilisées et avoir obtenu l'accord de l'Officier de Sécurité du site.

Toute sortie d'informations (papier, électronique, résultat des commandes, documentation) doit faire l'objet d'une demande auprès de l'Officier de Sécurité du site et d'une validation de sa part,

Toutes les données recueillies par les auditeurs sont confidentielles et à usage exclusif du SGDSN sauf accord express et préalable du titulaire ou du sous-traitant concerné. L'officier de Sécurité pourra demander copie de toutes données recueillies dans le cadre de l'audit.

6. Les auditeurs peuvent contacter autant que de besoin durant les jours et heures prévus pour l'audit, les personnels du site concerné ou sur des domaines affectant le système audité. Le cas échéant, dans la mesure où cela n'entrave pas le bon fonctionnement des systèmes, et avec l'accord de la personne interviewée et de son responsable hiérarchique, ces entrevues peuvent se dérouler en l'absence du responsable hiérarchique ou de l'Officier de Sécurité du site (ou de son représentant). A cette fin, des locaux adéquats doivent être prévus par le titulaire ou son sous-traitant (salle de réunion isolée, etc.). Le SGDSN peut poser toutes questions ayant trait à la sécurité du système audité. Les points ne concernant pas directement ou indirectement le système audité sont exclus. Tout ou partie du contenu de ces entrevues pourra, en fonction de sa sensibilité, être communiqué au titulaire ou ses sous-traitants par le SGDSN.
7. Les auditeurs du SGDSN peuvent demander aux opérateurs d'exécuter des commandes sur tous les équipements dédiés au système audité. Si l'opérateur juge que les commandes sont susceptibles d'altérer le bon fonctionnement du système, il doit l'indiquer aux auditeurs et peut en faire part à son responsable hiérarchique et à son Officier de Sécurité. Des tests alternatifs de qualification peuvent, le cas échéant, être proposés par le titulaire.
8. Le groupe d'audit du SGDSN est composé de personnels du SGDSN, comprenant entre 1 et 6 personnes. Le SGDSN communique au titulaire les noms des auditeurs une semaine avant leur venue et le site concerné par l'audit deux semaines avant la date d'exécution. La délégation est conduite par le responsable sécurité ou le chef de projet du système audité. Le responsable du groupe d'audit du SGDSN communique à l'Officier de Sécurité du site concerné un facsimilé d'un exemplaire dûment complété de la fiche en annexe 1, au moins deux jours avant l'audit. L'Officier de Sécurité du site concerné communique alors au responsable du groupe d'audit du SGDSN un facsimilé d'un exemplaire dûment complété de la fiche en annexe 2, au moins un jour avant l'audit. Le jour de l'audit des exemplaires originaux de ces documents sont échangés.
9. Sauf accord particulier préalable entre le SGDSN et le titulaire, le titulaire mettra en œuvre les moyens humains et techniques nécessaires pour que les audits puissent se dérouler de 09h00 à 18h00, avec une pause d'une heure entre 12h00 et 14h00.
10. En fonction du programme d'audit défini entre le SGDSN et le titulaire, l'audit peut être planifié sur plus d'une journée. Autant que faire se peut cette information de durée estimée de l'audit est communiquée à J-14 dès l'avis initial d'audit. La durée finale de l'audit est calée à J-3 lors de la définition du périmètre précis de ce dernier.



Le tableau ci-dessous récapitule les différentes étapes marquantes définies par le protocole jusqu'au moment du déroulement de l'audit :

<b>Moment de l'événement</b>	<b>Action à mener</b>
J-14	Le SGDSN notifie au titulaire le site à auditer. Définition du périmètre global de l'audit entre le titulaire et le SGDSN.
J-7	Le SGDSN transmet au titulaire la liste des intervenants qui participeront à l'audit et la liste des matériels/logiciels prévues pour l'audit
J-5	Le titulaire transmet au SGDSN les contraintes spécifiques concernant le site ou les personnes auditées.
J-3	Définition des moyens qui seront utilisés par le SGDSN lors de l'audit (appareil photo, clé usb, etc.)
J-2	Le modèle de fiche 1 de la présente annexe est transmis par le SGDSN au titulaire.
J-1	Le modèle de fiche 2 de la présente annexe est transmis par le titulaire au SGDSN.
Jour J	Déroulement de l'audit suivant les modalités définies et échange des fiches 1 et 2 originales entre le titulaire et le SGDSN.

### **Modèle fiche 1**

Je soussigné .....  
déclare piloter l'audit du système .....  
.....  
devant se dérouler du ..... au .....  
sur le site .....  
..... ,  
suivant les modalités prévues au protocole d'audit établi entre le SGDSN et le titulaire. La  
composition du groupe d'audit est la suivante :

<b>Nom</b>	<b>Prénom</b>	<b>Fonction (chef de projet, responsable sécurité, autre)</b>

Fait à ..... le ..... en deux (2) exemplaires, dont un remis à chacune des parties.

Signature

## Modèle fiche 2

Je soussigné ..... ,

Officier de Sécurité responsable du site.....

..... ,

et

Je soussigné ..... ,

responsable du système audité à .....

déclarent avoir autorisé l'audit par le SGDSN du ..... au.....

de tous les éléments sous notre responsabilité et affectant directement le système mentionné ci-dessus, suivant les modalités prévues au protocole d'audit de l'accord-cadre établi entre le SGDSN et le titulaire.

Nous reconnaissons par ailleurs avoir pris connaissance de la composition suivante du groupe d'audit :

Nom	Prénom	Fonction (chef de projet, responsable sécurité, autre)

Fait à ..... le ..... en deux (2) exemplaires, dont un remis à chacune des parties.

Signature