Digital113
Cluster numérique Sud de France

Cahier des charges

Sélection d'un prestataire pour la formation
Le Cyber Résilience Act (CRA)

1. Contexte

1.1 Le cluster Digital 113

Digital 113 est une association d'entreprises du numérique sur le territoire régional d'Occitanie, qui fédère tous les acteurs de l'économie et de l'innovation, et fait bénéficier à ses adhérents d'une plus grande proximité avec les laboratoires de recherche, les grands groupes, les pôles de compétitivité, les structures de formation et les universités, ainsi que les institutionnels, les médias, les investisseurs, …

Situé au cœur de l'écosystème numérique, Digital 113 favorise les synergies et développe la coopération entre les entreprises. Le cluster permet le rayonnement des expertises numériques des entreprises et les secteurs d'excellence de la Région Occitanie, en France et à l'international.

1.2 Positionnement de Digital 113 sur le sujet de la cybersécurité

Dans le domaine de la cybersécurité, Digital 113 s'engage activement à jouer un rôle de catalyseur en favorisant la sensibilisation, le partage des bonnes pratiques et le renforcement des compétences au sein de ses adhérents. Le cluster considère la cybersécurité comme un enjeu majeur pour les entreprises du numérique et s'efforce de positionner ses actions en accord avec les évolutions réglementaires et les meilleures pratiques du secteur.

Aujourd'hui, la cybermenace s'industrialise. Ces attaques visent de plus en plus la chaîne de valeur. On compte 500 à 550 atteintes par an contre la défense et la recherche françaises, dont 80 % visent les PME. En 2025, l'ANSSI a traité 1 366 incidents, et les exfiltrations de données ont bondi de 51 %.

À cette menace d'État s'ajoute une cybercriminalité qui n'est plus l'affaire de quelques attaquants isolés et très qualifiés. Elle s'est structurée en une économie décentralisée, où des services prêts à l'emploi permettent de louer un rançongiciel, d'acheter des identifiants volés, de négocier une rançon ou de se former, et où l'IA aide à repérer les failles et à attaquer des milliers de systèmes à la fois. Beaucoup se croient pourtant trop petites pour intéresser un attaquant et négligent les règles élémentaires d'hygiène informatique, alors que les TPE et PME représentent plus de 99 % des entreprises françaises. La cybersécurité est moins une question de taille que d'exposition et de préparation. L'ANSSI anticipe une augmentation massive des attaques hybrides d'ici 2030. Les entreprises de la filière, à commencer par les PME, déjà les plus visées, doivent s'y préparer dès maintenant. Les entreprises de la filière du numérique doivent elles aussi continuer de s'y préparer, plus sérieusement que jamais.

Pour plus d'informations et de détails sur le positionnement de Digital 113 sur les enjeux de cybersécurité, nous vous invitons à consulter la Note de Résilience parue en novembre 2026.

1.3 Contexte et enjeux

Le Cyber Resilience Act (CRA), ou règlement européen sur la cyber résilience (règlement UE 2024/2847), est entré en vigueur le 10 décembre 2024. Son application est progressive :

- 11 septembre 2026 : entrée en application des obligations de **signalement des vulnérabilités** activement exploitées et des **incidents graves affectant la sécurité** des produits numériques.
- 11 décembre 2027 : application générale du règlement, notamment **des exigences de cybersécurité** applicables aux produits mis sur le marché.

Quel est son objectif ?

Le CRA établit un cadre européen horizontal imposant des exigences de cybersécurité **aux produits** comportant des éléments numériques, tout au long de leur cycle de vie.

Il complète ainsi les réglementations qui portent davantage sur la cybersécurité des organisations, comme NIS 2, en ciblant directement les produits matériels et logiciels commercialisés sur le marché européen.

Il ne s'agit donc pas simplement de sécuriser l'entreprise qui développe un produit, mais aussi de garantir un niveau minimal de sécurité du produit lui-même, de sa conception à la fin de sa période de support.

Quels produits et quels acteurs sont concernés ?

Champ d'application : Tout produit comportant des éléments numériques mis sur le marché de l'UE, matériel ou logiciel dès lors qu'il se connecte directement ou indirectement à un réseau ou à un appareil.

Cela peut notamment concerner :

- Les objets connectés, équipements réseau et appareils intelligents.
- **Les systèmes d'exploitation, logiciels applicatifs et outils de développement commercialisés en tant que produits**.
- Les composants matériels et logiciels mis séparément sur le marché.
- Les produits intégrant des bibliothèques, dépendances ou composants open source.

Les principaux acteurs concernés sont les fabricants, importateurs et distributeurs, avec des obligations qui varient selon leur rôle.

La durée de support des produits doit être d'au moins cinq ans en principe, sauf si leur durée d'utilisation prévisible est inférieure. Le fabricant doit assurer le traitement des vulnérabilités et la mise à disposition des mises à jour de sécurité pendant toute cette période.

Particularités de l'open source :

Le CRA prévoit des dispositions spécifiques pour les logiciels open source : si un fabricant intègre des composants open source dans un produit commercialisé, il reste responsable de la conformité du produit final. Les entités qui assurent le soutien durable de logiciels open source (open source software stewards) sont, quant à elles, soumises à des obligations adaptées.

Quelles sont les principales obligations ?

- Sécurité dès la conception (security by design) : *le produit doit respecter les exigences essentielles de cybersécurité de l'annexe I du règlement*
- Un inventaire des composants logiciels (SBOM) *: le fabricant doit identifier et documenter les composants du produit, notamment au moyen d'une Software Bill of Materials (SBOM), dans un format communément utilisé et lisible par machine.*
- Une période de support et des mises à jour de sécurité *: le fabricant doit définir une période de support correspondant à la durée d'utilisation attendue du produit et assurer le traitement des vulnérabilités pendant cette période.*
- Le signalement des vulnérabilités et des incidents graves au CSIRT et à l'ENISA *: depuis le 11 septembre 2026, les fabricants doivent signaler les vulnérabilités activement exploitées et les incidents graves ayant un impact sur la sécurité des produits comportant des éléments numériques*
- L'évaluation de conformité et le marquage CE *: À partir du 11 décembre 2027, les produits concernés devront respecter les exigences de conformité du CRA pour être mis sur le marché européen.*

Comment le CRA s'inscrit-il dans un renforcement plus global de la responsabilité des fabricants de produits numériques ?

Cette évolution du cadre réglementaire européen s'accompagne également d'un renforcement des exigences en matière de responsabilité des fabricants. La directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux, dont les dispositions s'appliqueront aux produits mis sur le marché à compter du 9 décembre 2026, modernise les règles de responsabilité pour intégrer explicitement les logiciels dans la définition des produits concernés, qu'ils soient commercialisés de manière autonome, intégrés à un équipement ou proposés sous forme de service.

Elle prévoit ainsi que les fabricants de logiciels puissent être tenus responsables des dommages causés par un produit défectueux, notamment lorsque ceux-ci résultent de vulnérabilités de cybersécurité qui n'auraient pas été corrigées par les mises à jour nécessaires.

Ces deux textes s'inscrivent ainsi dans une même dynamique de renforcement de la sécurité des produits numériques : là où le Cyber Resilience Act définit les exigences de cybersécurité que les

fabricants doivent respecter, la directive sur la responsabilité du fait des produits défectueux vient renforcer les conséquences juridiques d'un défaut de sécurité. **Leur articulation place donc la maîtrise des risques cyber et le maintien en condition de sécurité des produits au cœur des responsabilités des entreprises du numérique.**

1.4 Finalité de la formation

Pour les entreprises du numérique, et en particulier les éditeurs de logiciels, ce règlement implique **de nouvelles exigences en matière de conception, de développement, de maintenance et de commercialisation des produits**.

Ces exigences soulèvent des enjeux à la fois **réglementaires, techniques et organisationnels**. Elles interrogent les pratiques de développement logiciel, les processus de gestion des vulnérabilités, la répartition des responsabilités entre les acteurs et la capacité des entreprises à démontrer la conformité de leurs produits.

Elles nécessitent également une coordination entre plusieurs fonctions de l'entreprise : direction, équipes de développement, responsables techniques, RSSI, équipes qualité, responsables produits et, selon les organisations, fonctions juridiques et commerciales.

Dans ce contexte, Digital 113 souhaite proposer à ses adhérents une formation permettant de **comprendre les exigences du CRA, d'évaluer leurs impacts sur leur activité et d'identifier les actions concrètes à engager pour anticiper leur mise en conformité**.

2. Formation

2.1 Présentation des attendus de la formation au Cyber Résilience Act

La formation "Cyber Résilience Act" ne doit pas être trop théorique, ni exclusivement juridique. Les compétences attendues sont les suivantes :

- Maîtrise réglementaire
- Expertise technique
- Approche opérationnelle

La formation "Cyber Résilience Act" doit être conçue pour être dispensée en format collectif, réunissant différentes entreprises.

2.2 Objectif de la Formation

La formation "Cyber Resilience Act" est une formation-action **sur une durée adaptée** à un public de TPE-PME.

Elle devra permettre aux participants de :

- Comprendre le périmètre du CRA et déterminer si leurs produits et activités sont susceptibles d'être concernés.

- Identifier les principales obligations applicables à leur entreprise et les responsabilités associées à leur rôle.
- Comprendre les impacts du règlement sur leurs pratiques de conception, de développement, de maintenance et de commercialisation.
- Identifier les processus, outils et documents à mettre en place ou à faire évoluer.
- Évaluer les premières actions à engager et prioriser les chantiers de mise en conformité.
- Identifier les points nécessitant un accompagnement complémentaire, notamment pour les démarches techniques ou réglementaires spécifiques à leurs produits.

L'objectif est de permettre aux participants de repartir avec une vision claire des enjeux et des premières étapes à engager, sans prétendre que la formation constitue à elle seule une démarche complète de mise en conformité.

La modalité de formation-action permettra la mise en application concrète en entreprise, et devra favoriser le partage de bonnes pratiques et l'échange d'expériences entre les participants, pour une montée en compétences accélérée sur le sujet.

2.3 Intervenants

Il est attendu que l'équipe pédagogique proposée puisse couvrir l'ensemble des objectifs requis, à la fois le volet juridique et le volet technique.

2.4 Périmètre

L'implantation des sièges sociaux ou établissements secondaires des entreprises bénéficiaires est en Occitanie.

Des déplacements sont à prévoir sur Montpellier et Toulouse, et parfois plus occasionnellement dans les territoires de la Région Occitanie.

3. Réponse Attendue

Digital 113 sera l'organisme porteur de cette démarche d'accompagnement, et attend que les prestataires puissent proposer une réponse complète sur l'ensemble de la consultation (seul ou en consortium).

L'objectif étant d'accompagner principalement les PME et TPE, le dispositif devra être adapté dans sa durée, pour permettre une mobilisation suffisante des individus concernés tout en étant acceptable sur la charge de travail. Cela sous-entend des modules articulés avec des séances collectives de travail et des intersessions le cas échéant pour que chacun travaille sur sa conformité au règlement.

Il est attendu du prestataire qu'il conçoive les contenus et supports de formation pour les journées de formation-action.

Digital 113 attend de la part des prestataires :

- Une réponse détaillée, précisant les publics cibles, les contenus traités et les modalités pédagogiques. Il est attendu que les prestataires puissent détailler comment ils comptent aborder les impacts du CRA de façon concrète (la formation doit être orientée sur les aspects opérationnels de la mise en conformité).
- Une proposition sur l'architecture de la formation, avec articulation entre les différents modules de formation le cas échéant, ou les différentes phases de formation
- Les outils/livrables avec lesquels les participants repartiront après la formation
- Les CV des intervenants (avec mention de l'expérience de formateur), leurs méthodes d'actualisation des compétences sur le sujet concerné, et un historique de l'expérience de formateur.
- Les villes d'intervention en présentiel
- La disponibilité pour démarrer des actions de formation et le volume possible
- Une proposition tarifaire adaptée : le prestataire sera sous-traitant de Digital 113, et doit proposer son coût journalier d'intervention, indépendamment du nombre d'apprenants dans les sessions.

Il appartiendra à Digital 113 de commercialiser le dispositif et d'organiser les sessions de formation, dans le respect de ses process Qualiopi. Le prestataire pourra être sollicité en « avant-vente » en cas de besoin.

Le prestataire ne pourra pas intervenir dans la définition du modèle économique appliqué par Digital 113 sur l'offre de formation.

Sauf aléas, les formations collectives auront lieu dans les locaux de Digital 113.

Critères du prestataire :

Il est attendu que le prestataire propose une réponse adaptée au cahier des charges.

Il est attendu que le prestataire soit formé à l'animation de formation et dispose d'une expérience terrain en cybersécurité des produits et en développement sécurisé : la connaissance du règlement est importante, mais savoir traduire ses exigences en actions concrètes l'est tout autant !

Il devra disposer d'un numéro de déclaration d'activité de formation. La certification Qualiopi n'est pas nécessaire.

À proposition égale, la priorité sera donnée aux prestataires ayant leur siège social ou un établissement secondaire sur le territoire d'Occitanie, et adhérant à Digital 113.

Il est attendu du prestataire qu'il conçoive les contenus et supports de formation pour les journées de formation. Si des frais d'ingénierie et de conception s'appliquent, il est important de les détailler de façon explicite dans l'offre tarifaire.

Ces éléments permettront une première sélection des prestataires, et constituent une base de travail solide pour finaliser le dispositif avec Digital 113 avant mise à disposition auprès des entreprises du numérique en région Occitanie.

Les prestataires sont appelés à se manifester au plus tard le **23 décembre 2026 à 17h00** par un dossier de candidature, à l'adresse formation@digital113.fr

Les candidats qui souhaitent échanger sur le présent cahier des charges pourront poser leurs questions à Digital 113, en demandant Mathilde Alarçon au 07 86 06 95 29, **exclusivement sur les périodes ci-dessous :**

- Jeudi 19 novembre de 9h à 11h
- Mardi 24 novembre de 14h à 16h
- Vendredi 4 décembre de 10h à 12h
- Mercredi 9 décembre de 15h à 17h
- Jeudi 17 décembre de 14h à 16h

Pour des questions d'organisation, en dehors de ces périodes, aucune réponse concernant ce cahier des charges ne sera apportée.