

Expert en conception et cybersécurité d'infrastructures IT/OT durables

RNCP42822 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	200, 326, 326n
Formacode(s)	31034, 24231, 31006, 31009, 31045
Code(s) ROME	M1802, M1801, M1806, H1209, M1803
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2031

Certificateur(s)

AFORP FORMATION (CFAI) · SIRET : 77572845400205

Partenaires habilités

6 organismes habilités, d'après la liste publiée par France compétences : 6 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION DES NETICIENS	87927861200012	Former et organiser l'évaluation
CFAI ALSACE	38855948600070	Former et organiser l'évaluation
CFAI DE CHAMPAGNE ARDENNE	40120610700062	Former et organiser l'évaluation
CFAI DIAFOR	39048242000028	Former et organiser l'évaluation
LASER ASSOCIATION	34025508200034	Former et organiser l'évaluation
MASTERSCHOOL FRANCE	94150264300013	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification d'Expert en conception et cybersécurité d'infrastructures IT/OT durables vise à former des professionnels capables de concevoir, déployer, sécuriser et maintenir des infrastructures IT et OT complexes, dans des environnements soumis à de fortes exigences de performance, de cybersécurité, de conformité réglementaire et de durabilité.

Dans un contexte marqué par la convergence des systèmes d'information (IT) et des systèmes industriels (OT), l'augmentation significative des cybermenaces ciblant les infrastructures critiques, la généralisation des architectures hybrides, virtualisées et cloud, le renforcement des cadres réglementaires et normatifs (RGPD, LPM, RGS, ANSSI, ISO 27001/27005, IEC 62443), et la nécessité d'intégrer des enjeux de sobriété numérique et de performance énergétique, les organisations publiques et privées ont un besoin croissant d'experts capables de piloter l'ingénierie technique globale des infrastructures, de la phase d'audit et de conception jusqu'à l'exploitation sécurisée et l'amélioration continue.

Cette certification répond à ces besoins en validant des compétences permettant au titulaire d'analyser et auditer des infrastructures IT/OT existantes, en évaluant les risques, la conformité, la performance et la durabilité, de concevoir

des architectures réseaux, systèmes et cloud sécurisées et résilientes, intégrant dès l'origine les exigences de cybersécurité et d'optimisation énergétique, de déployer et d'automatiser des infrastructures IT/OT, en garantissant leur mise en production sécurisée, et d'assurer le maintien en conditions opérationnelles et de sécurité, la supervision, la gestion d'incidents et la continuité d'activité.

Positionnée à un niveau d'expertise, la certification atteste de la capacité du titulaire à intervenir sur des projets complexes, à dialoguer avec des interlocuteurs techniques et décisionnels, à produire une documentation professionnelle en français et en anglais, et à accompagner les organisations dans la transformation et la sécurisation de leurs infrastructures numériques.

ACTIVITÉS VISÉES

L'Expert en conception et cybersécurité d'infrastructures IT/OT durables exerce ses activités dans des environnements complexes intégrant des infrastructures informatiques (IT) et industrielles (OT). Il intervient tout au long du cycle de vie des infrastructures, depuis l'analyse initiale jusqu'à l'exploitation sécurisée et l'amélioration continue, en intégrant les exigences de cybersécurité, de conformité réglementaire, de performance et de durabilité.

Ses principales activités consistent à : Analyser l'existant IT/OT ; Analyser les risques et les vulnérabilités IT/OT ; Évaluer la conformité réglementaire et normative ; Évaluer la performance, la résilience et la disponibilité ; Évaluer la durabilité et l'efficacité énergétique des infrastructures ; Formaliser, restituer et communiquer les résultats de l'analyse ; Concevoir des architectures IT/OT ; Définir les choix technologiques et architecturaux ; Intégrer la cybersécurité et la conformité dès la conception ; Formaliser et valider l'architecture cible ; Déployer et intégrer les infrastructures IT/OT ; Sécuriser les infrastructures IT/OT ; Tester, valider et documenter les déploiements ; Maintenir les infrastructures IT/OT en conditions opérationnelles ; Superviser la performance, la disponibilité et la sécurité ; Gérer la sécurité opérationnelle et la conformité continue ; Améliorer en continu les infrastructures IT/OT.

COMPÉTENCES ATTESTÉES

Réaliser et formaliser un audit global d'une infrastructure IT/OT hybride, en analysant les architectures réseaux, systèmes, cloud et industrielles, en modélisant les flux et les interconnexions, afin d'établir un diagnostic structuré de l'existant et d'identifier les vulnérabilités et points critiques.

Identifier, analyser et hiérarchiser les risques IT/OT, en mettant en œuvre une méthode d'analyse adaptée (EBIOS RM, ISO 27005), afin de formaliser des scénarios de risques cyber, opérationnels et industriels exploitables pour la prise de décision.

Évaluer et formaliser le niveau de conformité réglementaire et normative d'une infrastructure IT/OT, en analysant l'application des exigences applicables (ANSSI, RGS, LPM, RGPD, ISO 27001/27002, IEC 62443), afin d'identifier, hiérarchiser et documenter les écarts de conformité exploitables pour la mise en conformité.

Évaluer et formaliser le niveau de performance, de résilience et de disponibilité des infrastructures IT/OT, en analysant les capacités, les charges, les mécanismes de continuité et les risques d'interruption de service, afin d'objectiver la robustesse de l'infrastructure et d'orienter les décisions d'amélioration.

Évaluer et formaliser le niveau de durabilité et d'efficacité énergétique d'une infrastructure IT/OT, en analysant la consommation énergétique, l'empreinte environnementale et les pratiques Green IT, afin d'objectiver les impacts environnementaux et de proposer des leviers d'optimisation et de sobriété numérique.

Formaliser, argumenter et communiquer les résultats d'une analyse IT/OT, en produisant des rapports structurés et des recommandations hiérarchisées, et en adaptant la restitution aux parties prenantes techniques et décisionnelles, en français et en anglais, afin d'éclairer la prise de décision.

Concevoir et formaliser une architecture IT/OT cible, en intégrant les exigences de performance, de résilience, de cybersécurité, d'interopérabilité et de durabilité, et en arbitrant entre différentes solutions technologiques, afin de répondre aux besoins métiers et aux contraintes opérationnelles et réglementaires.

Définir, comparer et arbitrer les choix technologiques et architecturaux d'une infrastructure IT/OT, en analysant leurs impacts en matière de sécurité, de performance, de résilience, de durabilité et de coûts, afin de garantir une solution interopérable et pérenne.

Intégrer et formaliser la cybersécurité et la conformité réglementaire dès la phase de conception d'une architecture IT/OT, en appliquant les principes de Security by Design et de segmentation des zones et flux, afin de réduire les risques cyber et de garantir la conformité réglementaire.

Formaliser, documenter et faire valider l'architecture IT/OT cible, en produisant des schémas et un dossier d'architecture structuré, et en argumentant les choix auprès des parties prenantes techniques et décisionnelles, afin d'assurer sa compréhension, son exploitation et son évolutivité.

Déployer et intégrer une infrastructure IT/OT en mettant en œuvre l'architecture définie, en pilotant les configurations et l'interopérabilité des composants, afin d'assurer un fonctionnement opérationnel conforme aux exigences de

sécurité, de performance et de continuité d'activité.

Sécuriser une infrastructure IT/OT déployée, en mettant en œuvre et en adaptant les mesures de sécurité et de segmentation prévues, en contrôlant leur efficacité, afin de réduire les risques cyber et opérationnels et de garantir la continuité d'activité.

Tester, valider et documenter une infrastructure IT/OT déployée, en structurant les vérifications fonctionnelles, techniques et de sécurité, en analysant les écarts éventuels et en formalisant les résultats, afin de garantir sa conformité, sa sécurité et son exploitabilité.

Maintenir et piloter une infrastructure IT/OT en conditions opérationnelles et de sécurité, en assurant l'exploitation, la gestion structurée des incidents et des changements, en analysant les causes et en priorisant les actions, afin de garantir la continuité de service et la maîtrise des risques techniques.

Superviser et analyser une infrastructure IT/OT en exploitant les outils de monitoring et de détection, en interprétant les indicateurs et en anticipant les dérives, afin d'assurer durablement la performance, la disponibilité et la sécurité.

Assurer et piloter la sécurité opérationnelle et la conformité continue d'une infrastructure IT/OT, en priorisant la gestion des vulnérabilités et des correctifs selon leur criticité, en évaluant les impacts des mises à jour, afin de maîtriser les risques cyber et réglementaires dans la durée.

Piloter l'amélioration continue d'une infrastructure IT/OT, en analysant les retours d'exploitation et les incidents, en priorisant les actions correctives et évolutives, afin d'optimiser durablement la performance, la résilience, la sécurité et la durabilité.

Blocs de compétences

RNCP42822BC01 — Analyser les infrastructures IT/OT et évaluer leur conformité, leurs risques et leur durabilité

LISTE DE COMPÉTENCES

Réaliser et formaliser un audit global d'une infrastructure IT/OT hybride, en analysant les architectures réseaux, systèmes, cloud et industrielles, en modélisant les flux et les interconnexions, afin d'établir un diagnostic structuré de l'existant et d'identifier les vulnérabilités et points critiques.

Identifier, analyser et hiérarchiser les risques IT/OT, en mettant en œuvre une méthode d'analyse adaptée (EBIOS RM, ISO 27005), afin de formaliser des scénarios de risques cyber, opérationnels et industriels exploitables pour la prise de décision.

Évaluer et formaliser le niveau de conformité réglementaire et normative d'une infrastructure IT/OT, en analysant l'application des exigences applicables (ANSSI, RGS, LPM, RGPD, ISO 27001/27002, IEC 62443), afin d'identifier, hiérarchiser et documenter les écarts de conformité exploitables pour la mise en conformité.

Évaluer et formaliser le niveau de performance, de résilience et de disponibilité des infrastructures IT/OT, en analysant les capacités, les charges, les mécanismes de continuité et les risques d'interruption de service, afin d'objectiver la robustesse de l'infrastructure et d'orienter les décisions d'amélioration.

Évaluer et formaliser le niveau de durabilité et d'efficacité énergétique d'une infrastructure IT/OT, en analysant la consommation énergétique, l'empreinte environnementale et les pratiques Green IT, afin d'objectiver les impacts environnementaux et de proposer des leviers d'optimisation et de sobriété numérique.

Formaliser, argumenter et communiquer les résultats d'une analyse IT/OT, en produisant des rapports structurés et des recommandations hiérarchisées, et en adaptant la restitution aux parties prenantes techniques et décisionnelles, en français et en anglais, afin d'éclairer la prise de décision.

MODALITÉS D'ÉVALUATION

L'évaluation du bloc repose sur une mise en situation professionnelle individuelle, réalisée à partir d'une infrastructure IT/OT réelle ou reconstituée comprenant : Une architecture IT et OT (réseaux, systèmes, environnements industriels), des flux et interconnexions documentés, des éléments de configuration et d'exploitation, un contexte réglementaire et normatif applicable, et des données relatives aux performances, à la continuité d'activité et à la consommation énergétique

Le candidat doit : Analyser l'environnement IT/OT existant et produire une cartographie structurée des architectures et des flux ; Mettre en œuvre une méthode d'analyse des risques adaptée (EBIOS RM, ISO 27005 ou équivalent) ; Évaluer la conformité réglementaire et normative applicable ; Évaluer la performance, la résilience et la disponibilité de l'infrastructure ; Analyser la durabilité et l'efficacité énergétique de l'environnement IT/OT ; Formaliser un diagnostic global hiérarchisé ; Formuler des recommandations prioritaires ; Restituer les résultats à des parties prenantes techniques et décisionnelles.

Les livrables attendus comprennent : Une cartographie des architectures et des flux IT/OT ; Une analyse de risques structurée et hiérarchisée ; Une évaluation de conformité réglementaire et normative ; Une analyse de performance et de résilience ; Une analyse de durabilité et d'efficacité énergétique ; Un rapport de diagnostic global incluant recommandations et priorisation

Une soutenance orale permet d'évaluer : La cohérence et la rigueur méthodologique des analyses réalisées ; La pertinence et la hiérarchisation des recommandations ; La capacité à argumenter les choix et à répondre aux questions ; La capacité à adapter la communication à un public technique et décisionnel ; La qualité de la communication professionnelle en français et en anglais

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

RNCP42822BC02 — Concevoir des architectures IT/OT durables, performantes et sécurisées

LISTE DE COMPÉTENCES

Concevoir et formaliser une architecture IT/OT cible, en intégrant les exigences de performance, de résilience, de cybersécurité, d'interopérabilité et de durabilité, et en arbitrant entre différentes solutions technologiques, afin de répondre aux besoins métiers et aux contraintes opérationnelles et réglementaires.

Définir, comparer et arbitrer les choix technologiques et architecturaux d'une infrastructure IT/OT, en analysant leurs impacts en matière de sécurité, de performance, de résilience, de durabilité et de coûts, afin de garantir une solution interopérable et pérenne.

Intégrer et formaliser la cybersécurité et la conformité réglementaire dès la phase de conception d'une architecture IT/OT, en appliquant les principes de Security by Design et de segmentation des zones et flux, afin de réduire les risques cyber et de garantir la conformité réglementaire.

Formaliser, documenter et faire valider l'architecture IT/OT cible, en produisant des schémas et un dossier d'architecture structuré, et en argumentant les choix auprès des parties prenantes techniques et décisionnelles, afin d'assurer sa compréhension, son exploitation et son évolutivité.

MODALITÉS D'ÉVALUATION

L'évaluation du bloc repose sur une mise en situation professionnelle individuelle, réalisée à partir d'un cas réel ou reconstitué de conception ou de refonte d'une architecture IT/OT dans un contexte à forts enjeux techniques, sécuritaires, réglementaires et environnementaux.

L'environnement fourni comprend notamment : Un contexte organisationnel et stratégique ; Une expression des besoins métiers et techniques ; Une architecture existante ou des hypothèses d'évolution ; Des contraintes réglementaires, normatives et budgétaires ; Des exigences de performance, de résilience, de cybersécurité et de durabilité.

Le candidat doit : Analyser les besoins métiers, techniques et opérationnels ; Définir une architecture IT/OT cible intégrant IT, OT et interconnexions hybrides ; Intégrer les principes de cybersécurité dès la conception (Security by Design) ; Prendre en compte les exigences de performance, de disponibilité et de résilience ; Assurer l'interopérabilité entre environnements IT et OT ; Intégrer les principes de durabilité et de sobriété numérique ; Argumenter les choix technologiques retenus.

Les livrables attendus comprennent : Des schémas d'architecture logique et physique ; La description des zones, flux et mécanismes de segmentation ; La formalisation des mécanismes de sécurité intégrés ; Une justification argumentée des choix technologiques ; Une analyse des impacts en matière de sécurité, performance, résilience, interopérabilité et durabilité ; Une synthèse destinée à des décideurs.

Une soutenance orale permet d'évaluer : La cohérence globale de l'architecture proposée ; La capacité d'arbitrage technologique argumenté ; La prise en compte des contraintes réglementaires et de sécurité ; L'intégration effective des enjeux de durabilité ; La capacité à défendre les choix structurants face à un questionnement technique.

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

RNCP42822BC03 — Déployer, intégrer et sécuriser des infrastructures IT/OT

LISTE DE COMPÉTENCES

Déployer et intégrer une infrastructure IT/OT en mettant en œuvre l'architecture définie, en pilotant les configurations et l'interopérabilité des composants, afin d'assurer un fonctionnement opérationnel conforme aux exigences de sécurité, de performance et de continuité d'activité.

Sécuriser une infrastructure IT/OT déployée, en mettant en œuvre et en adaptant les mesures de sécurité et de segmentation prévues, en contrôlant leur efficacité, afin de réduire les risques cyber et opérationnels et de garantir la continuité d'activité.

Tester, valider et documenter une infrastructure IT/OT déployée, en structurant les vérifications fonctionnelles,

techniques et de sécurité, en analysant les écarts éventuels et en formalisant les résultats, afin de garantir sa conformité, sa sécurité et son exploitabilité.

MODALITÉS D'ÉVALUATION

L'évaluation du bloc repose sur une mise en situation professionnelle individuelle, réalisée à partir d'un projet réel ou reconstitué de déploiement et d'intégration d'une infrastructure IT/OT, dans un contexte comportant des contraintes opérationnelles, sécuritaires et de continuité d'activité.

L'environnement fourni comprend notamment : Une architecture IT/OT cible validée ; Des composants réseaux, systèmes, virtualisés ou industriels à déployer ou configurer ; Des exigences de sécurité et de conformité ; Des contraintes d'exploitation et de continuité de service ; Des scénarios d'incidents ou d'aléas techniques.

Le candidat doit : Mettre en œuvre l'architecture IT/OT définie ; Intégrer les composants IT et OT en assurant leur interopérabilité ; Configurer les mécanismes de segmentation et de sécurité ; Déployer les dispositifs de cybersécurité adaptés ; Réaliser les tests fonctionnels, techniques et de sécurité ; Identifier et traiter les risques techniques rencontrés ; Documenter les configurations et procédures d'exploitation ; Justifier les choix techniques réalisés.

Les livrables attendus comprennent : Les configurations mises en œuvre et documentées ; Les preuves de fonctionnement et de tests réalisés ; Les mécanismes de segmentation et de sécurisation opérationnels ; Un plan de tests et ses résultats ; Un rapport de gestion des risques techniques ; Une documentation d'exploitation initiale..

Une soutenance orale permet d'évaluer : La cohérence entre l'architecture cible et le déploiement réalisé ; La maîtrise des mécanismes de sécurisation ; La capacité à gérer des aléas techniques ; La justification des choix techniques ; La capacité à expliquer les impacts sur la sécurité, la performance et la continuité d'activité..

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

RNCP42822BC04 — Maintenir, superviser et améliorer des infrastructures IT/OT en conditions opérationnelles et de sécurité

LISTE DE COMPÉTENCES

Maintenir et piloter une infrastructure IT/OT en conditions opérationnelles et de sécurité, en assurant l'exploitation, la gestion structurée des incidents et des changements, en analysant les causes et en priorisant les actions, afin de garantir la continuité de service et la maîtrise des risques techniques.

Superviser et analyser une infrastructure IT/OT en exploitant les outils de monitoring et de détection, en interprétant les indicateurs et en anticipant les dérives, afin d'assurer durablement la performance, la disponibilité et la sécurité.

Assurer et piloter la sécurité opérationnelle et la conformité continue d'une infrastructure IT/OT, en priorisant la gestion des vulnérabilités et des correctifs selon leur criticité, en évaluant les impacts des mises à jour, afin de maîtriser les risques cyber et réglementaires dans la durée.

Piloter l'amélioration continue d'une infrastructure IT/OT, en analysant les retours d'exploitation et les incidents, en priorisant les actions correctives et évolutives, afin d'optimiser durablement la performance, la résilience, la sécurité et la durabilité.

MODALITÉS D'ÉVALUATION

L'évaluation du bloc repose sur une mise en situation professionnelle individuelle, réalisée à partir d'un environnement IT/OT réel ou reconstitué en conditions opérationnelles, comportant des contraintes de disponibilité, de sécurité, de conformité et de continuité d'activité.

L'environnement fourni comprend notamment : Une infrastructure IT/OT en production ; Des outils de supervision et de journalisation ; Des indicateurs de performance et de sécurité ; Des alertes, incidents ou dérives simulés ; Des exigences de conformité et de maintien en conditions de sécurité.

Le candidat doit : Superviser l'infrastructure IT/OT et analyser les indicateurs techniques et de sécurité ; Identifier et qualifier les incidents, anomalies ou dérives ; Mettre en œuvre des actions correctives adaptées ; Assurer le maintien en conditions opérationnelles et de sécurité ; Vérifier le respect des exigences de conformité et de continuité d'activité ; Proposer des actions d'amélioration technique et organisationnelle ; Documenter les interventions et mettre à jour les procédures d'exploitation.

Les livrables attendus comprennent : Un rapport d'analyse des incidents ou anomalies détectés ; Les actions correctives mises en œuvre et leurs justifications ; Les preuves de rétablissement du niveau de service attendu ; Une mise à jour documentée des procédures ou configurations ; Des propositions d'amélioration continue argumentées.

Une soutenance orale permet d'évaluer : La capacité à diagnostiquer des situations complexes en environnement IT/OT ; La pertinence des actions correctives et préventives proposées ; La maîtrise des enjeux de sécurité et de continuité d'activité ; La capacité à anticiper les risques futurs ; La posture d'expert en maintien en conditions opérationnelles et de sécurité.

L'évaluation s'appuie sur une grille critériée permettant de statuer sur l'acquisition des compétences du bloc.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les titulaires de la certification Expert en conception et cybersécurité d'infrastructures IT/OT durables exercent leurs activités dans des organisations publiques ou privées, de toutes tailles, disposant d'infrastructures informatiques et/ou industrielles critiques, intégrant des environnements IT et OT.

Les principaux secteurs d'activités concernés sont notamment : Industrie (manufacturière, process, énergie, chimie, agroalimentaire, pharmaceutique). Infrastructures critiques et opérateurs d'importance vitale (énergie, eau, transport, télécommunications). Services numériques et sociétés de services (ESN, cabinets de conseil, intégrateurs IT/OT, cybersécurité). Éditeurs de solutions logicielles et fournisseurs d'équipements IT/OT. Secteur public et parapublic (administrations, collectivités, établissements publics, hôpitaux). Transport et logistique (ferroviaire, aérien, maritime, plateformes logistiques). Bâtiments et infrastructures intelligentes (smart buildings, smart grids, smart cities). Data centers et services cloud.

Les activités peuvent s'exercer en contexte national ou international, dans des environnements soumis à de fortes exigences de cybersécurité, de conformité réglementaire, de continuité de service et de durabilité.

TYPE D'EMPLOIS ACCESSIBLES

La certification Expert en conception et cybersécurité d'infrastructures IT/OT durables permet d'accéder à des fonctions à forte responsabilité technique et organisationnelle, centrées sur la conception, la sécurisation, le déploiement et l'exploitation d'infrastructures informatiques et industrielles complexes.

Les principaux types d'emplois accessibles sont notamment : Expert en conception d'infrastructures IT/OT, Architecte infrastructures IT/OT, Architecte cybersécurité IT/OT, Consultant en cybersécurité des infrastructures IT/OT, Consultant en architecture et sécurité des systèmes industriels, Ingénieur infrastructures systèmes, réseaux et cloud, Ingénieur cybersécurité des infrastructures, Responsable de la sécurité des infrastructures IT/OT, Responsable architecture et résilience des infrastructures, Expert en sécurisation des systèmes industriels et critiques.

Selon la taille et l'organisation de la structure, ces fonctions peuvent également recouvrir des intitulés tels que : Lead architecte infrastructures IT/OT, Expert sécurité des systèmes d'information et industriels, Référent cybersécurité IT/OT.

Ces emplois s'exercent généralement avec un haut niveau d'autonomie et de responsabilité, en interaction avec des équipes techniques, des directions métiers, des responsables de la sécurité et des décideurs, dans des contextes à fortes contraintes de performance, de continuité de service, de conformité réglementaire et de durabilité.

RÉGLEMENTATIONS D'ACTIVITÉ

Les activités exercées par les titulaires de la certification Expert en conception et cybersécurité d'infrastructures IT/OT durables s'inscrivent dans un cadre juridique et réglementaire exigeant, lié à la cybersécurité, à la protection des données, à la sécurité des systèmes d'information et des systèmes industriels, ainsi qu'à la continuité et à la durabilité des infrastructures. Les principales références juridiques et réglementaires applicables sont notamment :

Réglementations et cadres juridiques nationaux et européens : Règlement (UE) 2016/679 – RGPD relatif à la protection des données à caractère personnel. Directive (UE) 2022/2555 – NIS 2, relative à la sécurité des réseaux et des systèmes d'information. Code du travail (obligations de sécurité, santé et prévention des risques). Loi n° 2018-133 du 26 février 2018 transposant la directive NIS. Loi de programmation militaire (LPM) – dispositions relatives à la cybersécurité des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE). Code de la défense – protection des systèmes d'information d'importance vitale.

Référentiels et exigences de sécurité : Référentiels de l'ANSSI (règles de sécurité, guides, recommandations, PSSI). Référentiel Général de Sécurité (RGS) pour les systèmes d'information des administrations. ISO/IEC 27001 et ISO/IEC 27002 – management et mesures de sécurité de l'information. ISO/IEC 27005 – gestion des risques liés à la sécurité de l'information. EBIOS Risk Manager – méthode d'analyse et de gestion des risques.

Réglementations et normes spécifiques aux environnements industriels et OT : IEC 62443 – sécurité des systèmes d'automatisation et de contrôle industriels. ISO 22301 – management de la continuité d'activité. ISO 50001 – management de l'énergie (selon contexte).

Cadres liés à la durabilité et à la sobriété numérique : Loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique. Référentiel général d'écoconception des services numériques (RGESN). Recommandations Green IT et sobriété numérique (référentiels et bonnes pratiques reconnus).

Ces références constituent le cadre de conformité dans lequel s'exercent les activités professionnelles couvertes par la certification. Elles sont mobilisées de manière proportionnée selon le secteur d'activité, la nature des infrastructures IT/OT concernées et le périmètre de responsabilité du titulaire.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 947 €
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée) N0X70 — Techniciens d'étude, recherche et développement · tension 5/5 (Très élevée) N1X90 — Ingénieurs et cadres d'étude, recherche et développement (industrie) · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	31 794
Jugés difficiles à recruter	46 %
Emplois saisonniers	3 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X91 — Chefs de projet et directeurs de service informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information N0X70 — Techniciens d'étude, recherche et développement N1X90 — Ingénieurs et cadres d'étude, recherche et développement (industrie)

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Justifier d'un niveau 6 (ou équivalent) dans les domaines de l'informatique, des réseaux, des systèmes, de la cybersécurité, de l'électronique ou de l'informatique industrielle, ou d'une expérience professionnelle significative dans les domaines des infrastructures IT, des systèmes, des réseaux, de la cybersécurité et/ou des environnements industriels (OT).

Les candidats doivent disposer de connaissances solides en informatique, notamment dans les domaines suivants : Administration des systèmes d'exploitation (Linux et/ou Windows), réseaux informatiques (adressage IP, protocoles réseau, services d'infrastructure), virtualisation et infrastructures informatiques, et principes de base de la cybersécurité. (gestion des accès, sécurisation des systèmes et des réseaux).

Une appétence pour l'architecture des infrastructures, la cybersécurité et les environnements techniques complexes est attendue.

Les prérequis sont évalués lors de l'admission par l'analyse du dossier de candidature (diplômes, expériences, certifications), un entretien de positionnement, et, le cas échéant, des tests ou exercices de positionnement technique. Des parcours individualisés ou des modules de mise à niveau peuvent être proposés afin de sécuriser l'entrée en formation.

PRÉREQUIS À LA VALIDATION

Valider l'ensemble des blocs de compétences constitutifs de la certification,

et participer aux évaluations certificatives, le tout dans le respect des modalités définies par le règlement de certification.

Aucun autre prérequis spécifique n'est exigé pour la validation de la certification.

COMPOSITION DU JURY — FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

Le jury de certification est composé de cinq membres : un président et quatre membres décisionnaires. Le président est désigné par les membres du jury parmi eux, préalablement à l'ouverture des délibérations. L'ensemble des membres du jury est constitué de professionnels experts du domaine des systèmes, réseaux et cybersécurité. Ils sont tous extérieurs à l'AFORP : ils n'interviennent ni dans la formation, ni dans l'accompagnement pédagogique, et n'encadrent aucun candidat préparant la certification.

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	30/09/2031
Date de dernière délivrance possible	30/09/2035

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	106	0	92 %	—
2024	17	0	83 %	77 %
2023	41	0	96 %	96 %
2022	63	2	100 %	94 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP38105

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Formation alternance Expert en conception et cybersécurité d'infrastructures IT/OT durables - AFORP

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42822/>