

Manager cybersécurité et résilience numérique

RNCP42858 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31006, 31045, 31038
Code(s) ROME	M1802, M1803, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	30/09/2026
Date d'échéance	30/09/2029

Certificateur(s)

OPENCLASSROOMS · SIRET : 49386136300098

Résumé de la certification

OBJECTIFS ET CONTEXTE

Dans un contexte de transformation numérique massive, l'interconnexion croissante des systèmes d'information et l'essor de technologies comme le cloud et l'intelligence artificielle exposent l'ensemble des organisations à des risques cyber systémiques. Cette réalité est aggravée par une pression réglementaire inédite (notamment NIS2 et DORA) qui fait de la sécurité non plus une simple composante technique, mais un enjeu stratégique majeur pour la pérennité économique et la confiance numérique. Le secteur fait face à une pénurie structurelle de talents et à un besoin accru de professionnels capables de combler un skills gap en matière de pilotage et de gouvernance.

Dans ce contexte, la certification professionnelle Manager cybersécurité et résilience numérique (MCRN) atteste de la capacité à se positionner comme un cadre stratégique et opérationnel. Elle certifie un profil hybride capable de naviguer entre l'expertise technique et la prise de décision stratégique. Elle s'adresse aux professionnels disposant d'un socle technique préalable et cible des fonctions à haute responsabilité et de coordination, se positionnant à l'interface des équipes techniques et des directions métiers.

Les débouchés professionnels principaux incluent des rôles cadres tels que Responsable de la sécurité des systèmes d'information (RSSI), Consultant GRC (Gouvernance, Risques et Conformité), ou Auditeur de sécurité (en particulier sur les dimensions d'évaluation et d'audit).

ACTIVITÉS VISÉES

Élaborer la stratégie de cybersécurité du SI (diagnostic, évaluation des risques et orientations).

Définir, valider et piloter la mise en œuvre des mesures de sécurité, notamment de l'architecture.

Piloter la posture de sécurité, la conformité et la résilience.

Management stratégique de la sécurité dans les activités de l'entreprise.

COMPÉTENCES ATTESTÉES

Définir le périmètre du diagnostic via l'analyse des actifs et des enjeux organisationnels pour valider ses objectifs décisionnels.

Cartographier les flux critiques par des référentiels adaptés pour garantir une analyse d'impact centrée sur le métier.

Évaluer la maturité de sécurité par l'audit de preuves organisationnelles afin d'identifier tous les écarts procéduraux.

Superviser les audits techniques via la coordination d'experts pour évaluer la criticité et éclairer les arbitrages de sécurité.

Traduire les constats d'audit en risques métiers par une synthèse factuelle pour objectiver l'exposition aux décideurs.

Cadrer l'analyse des risques cybersécurité via une méthode adaptée afin d'établir un socle de préparation à

l'évaluation métier.

Traduire les vulnérabilités en scénarios de risques via une méthode éprouvée pour évaluer la gravité métier par processus.

Définir les options de traitement des risques via l'évaluation des mesures pour formaliser le plan d'action de direction.

Formaliser la stratégie de sécurité cible en intégrant les contraintes globales pour constituer le référentiel opposable.

Construire la feuille de route SSI pluriannuelle via des indicateurs dédiés afin d'assurer son pilotage et son arbitrage.

Argumenter la stratégie SSI aux instances via des dossiers formels afin d'obtenir et tracer les décisions de ressources.

Décliner les objectifs de la PSSI en exigences mesurables par le durcissement afin de sécuriser l'ingénierie des projets.

Cadrer l'architecture de sécurité par des critères dédiés afin de garantir la résilience et minimiser l'empreinte SI.

Piloter la sécurité des acquisitions via le CCTP pour éclairer les choix des solutions selon les risques inhérents et l'écologie.

Valider les architectures via l'analyse des preuves MOE afin de garantir un déploiement sécurisé et accessible.

Arbitrer les risques résiduels en formalisant les dérogations pour assurer la traçabilité continue de la posture sécurité.

Définir les conditions de mise en service via la validation d'exploitabilité pour garantir le maintien de la sécurité RUN.

Assurer la veille réglementaire par l'analyse des évolutions afin d'éclairer les mises en conformité de l'organisation.

Hiérarchiser les exigences normatives via une matrice dédiée afin d'établir un dispositif SSI contrôlable et accessible.

Piloter le contrôle interne SSI par des indicateurs continus afin de fournir une vision consolidée de la posture cybersécurité.

Orchestrer l'amélioration continue via la définition des options de traitement des écarts pour garantir la traçabilité des décisions de sécurité.

Évaluer le risque tiers par l'analyse des dépendances pour qualifier l'exposition cyber et contractualiser des exigences de sécurité et d'audit rigoureuses.

Piloter le cycle de vie des prestataires par des contrôles récurrents afin de maintenir une posture de sécurité pérenne.

Prescrire les exigences de résilience via des procédures d'escalade pour garantir la continuité des activités critiques.

Définir des scénarios de crise cyber par des simulations inclusives pour formaliser le plan d'actions post-exercice attendu.

Coordonner la réponse aux crises via la cellule décisionnelle afin de préserver les équipes et tracer les arbitrages.

Piloter la reprise sécurisée par des critères de remise en service pour clôturer la crise avec un plan d'actions suivi.

Cadrer l'intégration SSI projet via la définition de jalons afin d'ancrer les critères d'acceptation au planning global.

Suivre l'avancement budgétaire par l'anticipation des dérives pour assurer la clôture SSI et le transfert sécurisé RUN.

Spécifier les exigences SSI par la déclinaison des normes pour adapter les critères d'acceptation aux risques du projet.

Vérifier la conformité des livrables par des preuves tangibles afin d'émettre un avis motivé avant la mise en service.

Mobiliser les acteurs internes via la gouvernance projet afin d'aligner les enjeux SSI et tracer les arbitrages globaux.

Accompagner l'adoption des mesures via des actions ciblées afin de piloter les ajustements selon les irritants métiers.

Déployer le changement SSI par des formations profilées afin d'assurer l'adoption durable des nouveaux dispositifs cyber.

Sécuriser la transition RUN par le suivi des indicateurs pour garantir l'adoption durable des nouvelles pratiques cyber.

Blocs de compétences

RNCP42858BC01 — Élaborer la stratégie de cybersécurité du SI (diagnostic, évaluation des risques et orientations)

LISTE DE COMPÉTENCES

Analyser l'écosystème et les enjeux de l'organisation, afin de définir le périmètre fonctionnel et technique du diagnostic en identifiant les actifs et les profils utilisateurs diversifiés, les sites et environnements concernés afin de circonscrire l'intervention, puis qualifier les contraintes et le contexte d'intervention afin de valider avec la Direction des objectifs de diagnostic explicites (audit vs conseil).

Réaliser une cartographie macro, orientée impact métier, des flux d'information critiques et des dépendances techniques ou externes, en sélectionnant le cadre méthodologique d'évaluation adapté aux objectifs et à la maturité de l'organisation (référentiels, normes telles qu'ISO, NIS2 ou ANSSI), afin de garantir une analyse d'impact centrée sur les processus essentiels.

Conduire un audit organisationnel de la sécurité : évaluer, sur la base de preuves objectivées (échantillonnage, traçabilité), la maturité de la gouvernance ainsi que des processus et pratiques de sécurité en s'appuyant sur des référentiels et méthodes d'audit reconnus (ex. ISO 27001/27002, etc.) et sur des techniques d'entretien et de revue documentaire, afin d'identifier et de qualifier les écarts procéduraux.

Superviser et piloter des audits techniques de cybersécurité (revues d'architecture, de configuration, de code, audits offensifs) en cadrant le périmètre et les objectifs, en coordonnant les experts internes ou tiers et en garantissant la qualité des preuves collectées, afin de consolider et interpréter les résultats, d'en évaluer la criticité au regard du risque métier et d'éclairer les décisions et arbitrages de sécurité.

Exploiter les résultats des audits organisationnels et techniques, analyser les rapports afin d'identifier les vulnérabilités exploitables, puis traduire les résultats en risques métiers et produire une synthèse exécutive des constats de sécurité fondée sur des preuves factuelles, afin d'objectiver le niveau de risque auprès des décideurs.

Cadrer la démarche d'analyse des risques cybersécurité : sélectionner la méthode d'analyse appropriée (ex. EBIOS RM/ISO 27005), définir le périmètre de l'étude en identifiant les biens essentiels, leurs dépendances et les exigences de continuité d'activité, puis établir une lecture du socle de sécurité existant afin de préparer l'analyse des risques.

Élaborer des scénarios de risques de cybersécurité (ex. EBIOS RM) en traduisant les vulnérabilités et les contextes en événements redoutés et impacts métiers, puis évaluer pour chaque processus critique la gravité, la vraisemblance et le niveau de risque brut, en documentant les hypothèses et le niveau de confiance.

Évaluer l'efficacité des mesures existantes pour établir le niveau de risque résiduel, définir et justifier les options de traitement (réduction/acceptation/transfert/refus), désigner les propriétaires de risque, préciser les mesures compensatoires et les modalités de revue, puis formaliser un plan d'action et des fiches d'arbitrage à destination de la Direction.

Définir les orientations stratégiques SSI et le niveau de sécurité cible en intégrant les contraintes budgétaires, les objectifs de sobriété numérique, et les priorités de la Direction. Puis formaliser la politique de sécurité (PSSI/directives) et les directives et procédures associées pour constituer le référentiel normatif opposable de l'organisation.

Construire la feuille de route SSI pluriannuelle et le budget associé (ex. CAPEX/OPEX) : prioriser une trajectoire soutenable, puis structurer les modalités de pilotage de la feuille de route à l'aide d'indicateurs de suivi (KPI/KRI) et de dispositif de gouvernance afin d'assurer le suivi et l'arbitrage dans la durée.

Argumenter la stratégie SSI auprès des instances de gouvernance afin d'obtenir des décisions formalisées relatives aux arbitrages, au budget et aux ressources, d'en acter les acceptations, et d'en assurer la traçabilité dans les dispositifs de gouvernance.

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP42858BC02 — Définir, valider et piloter la mise en œuvre des mesures de sécurité, notamment de l'architecture

LISTE DE COMPÉTENCES

Décliner les objectifs de la PSSI en exigences de sécurité mesurables (techniques et organisationnelles) en intégrant les principes de Security by Design et de durcissement : Produire des exigences priorisées (must/should), assorties de critères de preuve et de jalons de validation afin de guider et de sécuriser l'ingénierie des projets.

Cadrer l'architecture de sécurité cible, définir les principes de segmentation, de Zero Trust et de gestion des identités, en formalisant les principes, les contraintes et les critères d'acceptation, afin de réduire les surfaces d'exposition et de garantir la résilience structurelle du système d'information. Puis veiller à ce que l'architecture minimise l'empreinte environnementale du SI.

Piloter le volet sécurité des acquisitions de solutions, définir et formaliser les exigences de sécurité et de durabilité dans les cahiers des charges (CCTP), évaluer les offres au regard des risques et des exigences de sécurité et de leur empreinte environnementale, puis éclairer le choix final en lien avec les fonctions Achats.

Valider la conformité des architectures et solutions : analyser les dossiers d'architecture, définir les critères d'acceptation puis vérifier les preuves fournies par la MOE (tests, scans, etc.) avant mise en production : Décliner les principes de conception universelle dans les spécifications de sécurité des systèmes, en assurant une accessibilité de niveau requis (ex.RGAA/WCAG niveau AA).

Arbitrer les risques résiduels et les dérogations lors des phases de projet : analyser les écarts entre exigences et mise en œuvre, statuer sur les dérogations, puis formaliser les décisions, l'autorité d'acceptation, les mesures compensatoires, la durée de validité et les modalités de revue afin d'assurer la traçabilité de la posture de sécurité.

Définir les conditions de mise en service sécurisée et organiser la transition vers l'exploitation (RUN) en validant les

exigences d'exploitabilité (supervision, journalisation) et en transférant les responsabilités documentées pour garantir le maintien de la posture de sécurité post-déploiement

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP42858BC03 — Piloter la posture de sécurité, la conformité et la résilience

LISTE DE COMPÉTENCES

Assurer la veille réglementaire et normative en cybersécurité en analysant les impacts des évolutions légales (NIS2, DORA, etc.) sur le dispositif de sécurité de l'organisation, et structurer la diffusion et la communication internes des informations pertinentes afin d'éclairer les décisions et les mises en conformité.

Cadrer la conformité SSI : hiérarchiser les exigences réglementaires et normatives applicables (NIS2, ISO 27001, RGPD, etc.) en les corrélant aux risques majeurs de l'organisation, et traduire ces obligations externes en règles internes de sécurité (PSSI, Directives) pour établir et maintenir un dispositif SSI opérationnel, priorisé et contrôlable : Établir une matrice d'applicabilité pour chaque exigence, le périmètre, le propriétaire, les contrôles attendus. Cartographier les exigences, les registres de risques et les mécanismes de scoring (criticité, exposition, effort). Intégrer les exigences d'accessibilité numérique (RGAA/WCAG).

Structurer le dispositif de contrôle interne SSI en définissant les référentiels, la périodicité des campagnes et les modalités de gestion des preuves et les mécanismes de contrôle continu. Puis, Piloter la performance SSI via des indicateurs (KPI/KRI) en analysant les tendances et les dérives, en intégrant si pertinent, les enjeux de sobriété numérique, pour fournir une vision consolidée de la posture de sécurité.

Orchestrer l'amélioration continue du dispositif en qualifiant les écarts de sécurité selon leur criticité ((bloquant, majeur, mineur) et en définissant les plans de remédiation ou les options de traitement des risques avec les mesures compensatoires, les échéances associées. Puis, consolider l'état de conformité et préparer les dossiers d'arbitrage à destination des instances, enfin suivre la mise en œuvre et la clôture des décisions pour garantir la traçabilité des décisions de sécurité.

Évaluer et encadrer le risque lié aux tiers (fournisseurs, SaaS) en analysant les dépendances, critères EBIOS, les accès accordés et les chaînes de sous-traitance, y compris en cascade, afin de qualifier l'exposition cyber de l'organisation (TPRM) et en évaluant l'efficacité des actions correctives post-audit. Puis, définir et valider les exigences de sécurité contractuelles, incluant les clauses de protection, de réversibilité et de droit d'audit, afin d'encadrer la relation.

Piloter le cycle de vie de la sécurité des prestataires, superviser les processus d'embarquement, organiser les contrôles récurrents (basés sur des preuves et indicateurs) et la gestion des accès, et encadrer la réversibilité et la sortie sécurisée afin d'assurer ou de maintenir une posture de sécurité maîtrisée dans le temps.

Définir les exigences de résilience opérationnelle (BIA/PCA/PRA, RTO/RPO) en coordination avec les métiers pour garantir la continuité des activités critiques : Définir le cadre organisationnel de réponse aux incidents en structurant les procédures d'escalade, le RACI et les contrats de support spécialisés. Prescrire les exigences de résilience opérationnelle (RTO, RPO, scénarios de continuité) en coordination avec les métiers.

Définir des scénarios de simulation alignés sur des objectifs mesurables et des critères de réussite, préparer les dispositifs de communication de crise inclusifs (accessible aux PSH), y compris hors des systèmes d'information potentiellement compromis, mobiliser et entraîner les parties prenantes, puis formaliser un plan d'actions post-exercice précisant les axes d'amélioration, les propriétaires et les échéances.

Coordonner la réponse stratégique en situation de crise cybersécurité, structurer et piloter l'animation de la cellule de crise SSI (ex en cellule décisionnelle et technique), organiser la production et la mise à jour des éléments de situation (main courante, SITREP), préparer les arbitrages décisionnels sous contrainte tout en veillant à la prévention des RPS et à la sécurité des équipes engagées (préservation des effectifs, rotation) et en assurer la traçabilité, en appui du dispositif global de gestion de crise.

Piloter la sortie de crise et la reprise sécurisée : définir et valider les critères de remise en service (go / no-go), encadrer les opérations de restauration dans un état de confiance (environnements sains, rotation des secrets et des identités), organiser les contrôles de régression de sécurité, puis formaliser la clôture de crise à travers un retour d'expérience structuré et un plan d'actions suivi.

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP42858BC04 — Management stratégique de la sécurité dans les activités de l'entreprise

LISTE DE COMPÉTENCES

Cadrer et structurer la contribution SSI au sein des projets, définir les jalons et gates de sécurité incluant les critères d'acceptation, les livrables de sécurité, les dépendances avec les autres lots, les responsabilités associées (RACI), ainsi que les points de décision (go / no-go), puis intégrer ces éléments au pilotage et au planning global.

Suivre l'avancement des activités et les consommations budgétaires (CAPEX/OPEX), anticiper les dérives afin de préparer les arbitrages budgétaires ou calendaires, puis assurer la clôture SSI des projets et organiser le transfert vers l'exploitation (RUN).

Spécifier les exigences SSI propres à chaque projet en déclinant la PSSI, les standards et les principes d'architecture en exigences (NFR) mesurables et vérifiables, adaptées aux enjeux métiers/techniques et au profil de risque du projet, et assorties de critères d'acceptation : Analyser le contexte, le périmètre et les enjeux du projet. Co-construire avec les métiers à partir des processus et des usages, les fonctions de sécurité nécessaires. Adapter les exigences SSI applicables.

Vérifier, sur la base de preuves, la conformité des livrables aux jalons décisionnels ; qualifier les écarts et piloter leur traitement (remédiation ou dérogation compensée) ; puis émettre un avis motivé (go / no-go) en traçant le risque résiduel et les décisions d'acceptation avant la mise en service.

Coordonner et mobiliser les acteurs internes (métiers, DSI, juridique, RUN) au sein de la gouvernance projet en construisant une coalition sponsor + relais ; aligner les enjeux SSI avec les objectifs business et IT ; gérer les dépendances et les résistances ; préparer les arbitrages afin d'assurer la traçabilité des décisions et des engagements.

Accompagner l'adoption des mesures de sécurité en analysant les impacts et les irritants utilisateurs et les besoins spécifiques de compensation (accessibilité, etc.), orchestrer les actions ciblées avec les relais internes, puis mesurer l'adoption réelle afin de piloter les ajustements nécessaires.

Déployer le plan d'accompagnement au changement SSI en définissant et en pilotant des actions de formation et de sensibilisation adaptées par profils, en mobilisant les relais internes (RH/Com/management), et en mesurant leur efficacité afin d'assurer l'adoption des nouveaux dispositifs.

Sécuriser la transition vers l'exploitation (RUN) et mesurer l'adoption des mesures de sécurité : suivre les indicateurs d'usage, ancrer les nouvelles pratiques de sécurité dans les rituels d'exploitation, et s'assurer de la montée en compétence des équipes afin de garantir l'adoption réelle et durable.

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le manager en cybersécurité et résilience numérique intervient dans de nombreux secteurs (IT, conseil, finance, industrie, secteur public) où les systèmes d'information sont essentiels. Il évolue dans des environnements complexes marqués par l'augmentation des cybermenaces, l'usage du cloud et des systèmes distribués, ainsi que des exigences réglementaires accrues.

Son rôle répond à des enjeux majeurs : protection des données, continuité d'activité, conformité et gestion des risques. Il peut exercer dans des structures variées, de petites entreprises spécialisées à de grandes organisations disposant d'infrastructures et d'équipes dédiées.

TYPE D'EMPLOIS ACCESSIBLES

Fonctions de conseil, d'audit et de pilotage et management GRC : Consultant cybersécurité (gouvernance & risques, audit, prescripteur d'architecture sécurisée) - Auditeur sécurité des systèmes d'information

Fonctions de management et d'encadrement : Responsable sécurité SI - Responsable risques et sécurité informatique - Manager sécurité et risques de l'information

Fonctions d'ingénierie cybersécurité appliquées à la GRC : Ingénieur conformité SSI - Ingénieur cybersécurité (orientation gouvernance / risque / architecture)

RÈGLEMENTATIONS D'ACTIVITÉ

L'activité de Manager cybersécurité et résilience numérique n'est pas une profession réglementée en droit français (non soumise à ordre professionnel, autorisation administrative ou certification d'État obligatoire). Cependant, elle s'exerce dans un environnement fortement encadré par des normes et des réglementations, telles que :

Textes européens et nationaux : Directive NIS2, DORA (Digital Operational Resilience Act), CRA (Cyber Resilience Act), RGPD, Loi Godfrain, Loi de programmation militaire (LPM).

Autres cadres européens : DSA (Digital Services Act) et DMA (Digital Markets Act).

Normes et cadres méthodologiques internationaux : Référentiels COBIT, recommandations de l'ANSSI (méthode EBIOS Risk Manager et référentiel PASSI), normes ISO/IEC 27000, ISO 22301 (continuité d'activité) et ISO

Les professionnels doivent donc piloter la conformité, évaluer les risques et coordonner les dispositifs de sécurité selon ces cadres réglementaires et normatifs.

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 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 913 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % des actifs en emploi)
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) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	14 615
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 M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'une certification professionnelle de niveau 6 (ou équivalent) en informatique - systèmes d'information et numérique ; Ou être titulaire d'une certification professionnelle de niveau 5 (ou équivalent) avec une expérience professionnelle d'au moins trois ans, dans le domaine de l'informatique - systèmes d'information et numérique.

Tout autre profil relève d'une procédure dérogatoire.

PRÉREQUIS À LA VALIDATION

Pour bénéficier de la certification professionnelle complète, le candidat doit valider les quatre blocs de compétences.

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

Le jury de délivrance de la certification est composé du responsable pédagogique de la filière et deux professionnels du métier visé extérieurs à l'organisme.

Base légale

Date de décision	30/09/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	30/09/2029
Date de dernière délivrance possible	30/09/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	48	0	82 %	71 %
2024	38	0	91 %	81 %
2023	53	0	92 %	82 %

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42858/>