

Expert en sécurité, stratégie et conformité blockchain

RNCP42467 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326m, 326n
Formacode(s)	31006, 31056, 31036, 31004
Code(s) ROME	M1805, M1802, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	26/06/2026
Date d'échéance	26/06/2029

Certificateur(s)

TALIS COMPETENCES & CERTIFICATIONS · SIRET : 34959731000086

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASTON INSTITUT	49868549400029	Former et organiser l'évaluation
ASTON INSTITUT	49868549400060	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification « Expert en sécurité, stratégie et conformité Blockchain » s'inscrit dans un contexte de déploiement croissant des technologies blockchain dans des environnements professionnels critiques, conjugué à un renforcement des exigences de sécurité, de conformité et de gouvernance des systèmes numériques.

Les organisations publiques et privées recourent de plus en plus à des architectures décentralisées pour la gestion de transactions, d'actifs numériques, de données sensibles ou de processus automatisés. Cette évolution s'accompagne d'une exposition accrue aux risques techniques, économiques et réglementaires, nécessitant des compétences expertes en sécurisation des infrastructures blockchain, en audit de smart contracts et en gestion des incidents.

L'objectif de la certification est de répondre à ce besoin en formant des professionnels capables de concevoir, d'évaluer et de sécuriser des systèmes blockchain complexes, dans des contextes non standardisés et à forts enjeux. Elle vise à attester de la capacité des titulaires à analyser les risques, à définir des stratégies de sécurité adaptées, à assurer la conformité réglementaire et à accompagner les organisations dans le pilotage de projets blockchain sécurisés.

La certification s'adresse à des professionnels appelés à exercer des fonctions d'expertise, d'architecture, d'audit ou de conseil, impliquant un haut niveau d'autonomie, de responsabilité et de prise de décision, maîtrisant des savoirs hautement spécialisés, des capacités à concevoir des solutions innovantes et à intervenir sur des situations professionnelles complexes et évolutives.

ACTIVITÉS VISÉES

Conception et déploiement d'architecture blockchain sécurisée

Continuité de service, optimisation et formation

Audit de sécurité des smart contracts
Sécurisation des protocoles DeFi
Développement et documentation
Analyse de données blockchain on-chain
Intelligence des menaces et veille proactive
Pilotage de projets blockchain
Gestion des risques techniques et opérationnels et gestion budgétaires
Communication, RSE et amélioration continue
Conformité aux cadres réglementaires blockchain et Mise en œuvre des processus KYC/AML
Conseil stratégique et analyse d'impact RSE
Représentation lors d'audits et formation conformité

COMPÉTENCES ATTESTÉES

Concevoir l'architecture de sécurité globale des systèmes blockchain en évaluant les options techniques (publique/privée/consortium, consensus PoS/PoW/PBFT, architecture réseau, scalabilité Layer 2), en arbitrant entre sécurité/performance/décentralisation, en définissant les standards de sécurité et politiques organisationnelles, en déployant les infrastructures sur cloud (AWS/Azure/GCP) avec services managés adaptés, en automatisant le déploiement avec Infrastructure-as-Code (Terraform, Docker, Ansible, Kubernetes), en configurant la haute disponibilité multi-zones et load balancing, en implémentant la segmentation réseau stricte et le durcissement selon bonnes pratiques CIS, afin d'établir une architecture sécurisée, scalable, résiliente et opérationnelle.

Automatiser le déploiement et la gestion des infrastructures en utilisant Infrastructure-as-Code (Terraform, Docker, Ansible, Kubernetes, Helm), en créant des pipelines CI/CD avec tests intégrés, en versionnant les configurations dans Git avec code review obligatoire, en implémentant des tests automatisés de sécurité (scanning, vulnerability assessment), en développant des API REST pour exposition des services d'infrastructure, en configurant des systèmes de monitoring complets (Prometheus, Grafana, CloudWatch/Azure Monitor, stack ELK), en définissant les métriques et KPIs critiques, en créant des dashboards temps réel accessibles (RGAA 4.1 niveau AA), en configurant des alertes automatiques avec escalation, en analysant les logs pour détecter comportements suspects, afin d'assurer reproductibilité, traçabilité, qualité continue, disponibilité 24/7 et détection rapide d'incidents.

Gérer de manière sécurisée les clés cryptographiques en concevant une politique complète couvrant le cycle de vie (génération, stockage, rotation, révocation, destruction), en déployant des HSM on-premise ou KMS cloud, en implémentant multi-signature et threshold signatures pour opérations critiques, en définissant les procédures de backup/recovery avec tests réguliers, en auditant les accès avec traçabilité complète, afin de protéger les actifs contre vol ou compromission.

Assurer la résilience et continuité de service en définissant une stratégie de sauvegarde avec objectifs RPO/RTO selon criticité métier, en mettant en place des backups automatisés avec géo-réplication, en concevant des plans de disaster recovery avec procédures de basculement testées, en réalisant des tests réguliers de restauration et exercices de crise, en documentant les procédures d'escalade avec rôles clairs, afin de garantir récupération rapide en cas d'incident majeur.

Optimiser les coûts et performances des infrastructures cloud en appliquant les principes FinOps (analyse continue, rightsizing, instances spot/reserved), en monitorant les coûts par service avec alertes sur dépassements, en identifiant les opportunités d'optimisation (ressources inutilisées, dimensionnement approprié, caching), en équilibrant performance et coût selon exigences métier, en documentant les décisions avec analyse coût/bénéfice, afin de maximiser l'efficacité économique.

Former et documenter pour assurer le transfert de compétences en créant une documentation technique complète et à jour (architectures, procédures d'exploitation, runbooks d'incidents), en formant les équipes d'exploitation aux technologies blockchain et aux procédures de sécurité, en créant des supports pédagogiques adaptés aux différents niveaux, en accompagnant la montée en compétences avec mentorat et coaching, afin d'assurer l'autonomie opérationnelle des équipes et la pérennité des solutions.

Auditer la sécurité des smart contracts multi-langages en effectuant une revue manuelle ligne par ligne du code source Solidity, Rust (pour Solana, Polkadot, Substrate) et Move (pour Aptos, Sui), en recherchant systématiquement les patterns de vulnérabilités (reentrancy, integer overflow/underflow, access control, front-running, oracle manipulation, flashloan attacks), en vérifiant la conformité aux spécifications fonctionnelles, en créant des preuves de concept d'exploitation pour les vulnérabilités critiques, afin d'identifier exhaustivement les failles de sécurité avant déploiement en production.

Effectuer des tests automatisés de sécurité en utilisant prioritairement Foundry (framework Rust-based pour tests

rapides et fuzzing) ou Hardhat (framework JavaScript complet), en implémentant des tests unitaires couvrant toutes les fonctions critiques, en réalisant du fuzzing pour tests basés sur propriétés, en utilisant des analyseurs statiques complémentaires (Slither, Mythril), en intégrant ces tests dans les pipelines CI/CD pour vérification automatique à chaque commit, afin de détecter systématiquement les failles de sécurité avant déploiement.

Sécuriser les protocoles DeFi complexes en analysant les mécanismes économiques (Automated Market Makers, protocoles de lending, yield aggregators, produits dérivés), en identifiant les risques de manipulation (manipulation d'oracle, sandwich attacks, extraction MEV, attaques de gouvernance), en testant la robustesse des oracles avec simulation de scénarios extrêmes, en analysant les risques de composabilité entre protocoles interconnectés, en proposant des contre-mesures techniques et économiques, afin de prévenir les pertes financières majeures.

Analyser les risques économiques et de gouvernance en évaluant les mécanismes de tokenomics (distribution, vesting, inflation), en identifiant les vecteurs d'attaque économique (manipulations de vote, accumulation de pouvoir, attaques de gouvernance), en analysant la résilience face aux chocs économiques et variations de liquidité, en évaluant les risques systémiques de contagion entre protocoles, en proposant des ajustements de paramètres économiques pour améliorer la sécurité, afin de garantir la stabilité économique du protocole.

Documenter les audits de sécurité en rédigeant des rapports détaillés incluant (1) description technique précise de chaque vulnérabilité avec extraits de code, (2) scénario d'exploitation par un attaquant, (3) estimation de l'impact financier potentiel, (4) classification de criticité (Critical/High/Medium/Low) selon CVSS, (5) recommandations de correction avec suggestions de code, (6) résumé exécutif pour dirigeants non techniques, afin de communiquer efficacement les findings à toutes les parties prenantes.

Développer des interfaces et intégrations en créant des interfaces Web3 avec web3.js ou ethers.js pour interagir avec les smart contracts, en développant des API REST pour exposer les fonctionnalités blockchain aux applications externes, en implémentant des tests d'intégration end-to-end couvrant l'ensemble de la stack, en documentant les endpoints API avec spécifications OpenAPI/Swagger, en assurant la sécurité des intégrations avec authentification et gestion des erreurs, afin de faciliter l'adoption et l'intégration des protocoles blockchain.

Maintenir une veille technologique et sécuritaire continue en suivant les publications de sécurité (audits publics, post-mortems d'incidents, recherches académiques), en analysant les exploits récents pour identifier les patterns d'attaque émergents, en participant activement aux communautés de sécurité blockchain (Discord, forums spécialisés), en expérimentant avec les nouvelles techniques d'attaque et de défense, en se formant aux nouvelles technologies blockchain (L2, zkEVMs, nouvelles chaînes), en participant aux programmes de bug bounty en analysant le code de protocoles pour identifier des vulnérabilités inédites, en documentant les findings selon les standards des plateformes (Immunefi, HackerOne, Code4rena) et en collaborant avec les équipes projets pour la vérification des corrections, afin de rester à jour sur les menaces émergentes et de contribuer à l'amélioration de la sécurité de l'écosystème.

Analyser les données blockchain on-chain en collectant et indexant les données via nodes full et API (Etherscan, The Graph, Dune Analytics), en analysant les patterns transactionnels pour identifier comportements suspects (wash trading, pump and dump, money laundering), en effectuant du clustering d'adresses et traçage des flux de fonds avec outils spécialisés (Chainalysis, Elliptic), en développant des systèmes de détection d'anomalies par machine learning (isolation forests, autoencoders, LSTM) avec feature engineering pertinent, entraînement sur données historiques, évaluation des performances (précision/rappel/F1, ROC) et déploiement en production avec monitoring continu, afin de détecter automatiquement les transactions suspectes en temps réel.

Réaliser des investigations forensiques post-incident en collectant et préservant les preuves numériques selon les standards forensiques, en reconstituant la chronologie complète de l'incident avec timeline précise des événements, en traçant les flux de fonds volés à travers échanges centralisés et décentralisés, mixers (Tornado Cash) et chain hopping avec outils Chainalysis et Elliptic, en identifiant les acteurs malveillants via OSINT, corrélation d'adresses et analyse comportementale, en documentant l'investigation avec chaîne de traçabilité des preuves, afin de supporter les actions légales et récupérations d'actifs.

Corréler les événements de sécurité en collectant des données de multiples sources (logs blockchain, SIEM, threat intelligence feeds, dark web monitoring), en normalisant et enrichissant les événements pour analyse unifiée, en implémentant des règles de corrélation pour détecter les attaques multi-étapes, en identifiant les chaînes d'attaque complexes (kill chains) avec reconstruction des TTPs, en priorisant les alertes selon la criticité et l'impact potentiel, afin de détecter les attaques sophistiquées nécessitant coordination de multiples actions.

Produire de l'intelligence des menaces en collectant des renseignements depuis des sources OSINT, threat intelligence feeds commerciales et dark web monitoring, en analysant les TTPs des groupes d'attaquants selon le framework MITRE ATT&CK adapté à la blockchain, en créant et maintenant des indicateurs de compromission (IoC) réutilisables (adresses malveillantes, patterns de transactions, signatures d'attaque), en contextualisant les menaces selon les actifs et profil de risque de l'organisation, en produisant des rapports d'intelligence stratégique et tactique,

afin d'anticiper proactivement les risques émergents.

Développer des règles de détection, API et tableaux de bord en créant des règles SIEM optimisées pour attaques blockchain spécifiques, en définissant des KPIs de sécurité pertinents (taux d'attaques, temps de détection, impact financier), en développant des dashboards interactifs conformes RGAA 4.1 niveau AA avec visualisations temps réel, en créant des API REST documentées (OpenAPI/Swagger) pour exposer les fonctionnalités d'analyse, en automatisant les réponses aux incidents courants avec playbooks SOAR, en communiquant les résultats d'analyse via rapports techniques détaillés avec méthodologie et preuves, résumés exécutifs synthétiques pour la direction avec focus impact business, et visualisations impactantes (infographies, graphes, heat maps), afin d'améliorer l'efficacité du SOC blockchain et d'assurer l'appropriation des recommandations par tous les niveaux.

Maintenir et améliorer les capacités d'analyse en effectuant des retours d'expérience post-incident pour améliorer les processus, en développant et maintenant des scripts d'analyse réutilisables et automatisés, en créant une base de connaissances des techniques d'attaque et d'investigation, en formant les équipes SOC aux techniques d'analyse blockchain, en participant à la recherche et développement de nouvelles techniques de détection, afin d'améliorer continuellement l'efficacité du centre d'opérations de sécurité.

Piloter des projets blockchain complexes en définissant la roadmap technique alignée avec les objectifs business et les contraintes de sécurité, en planifiant les sprints avec estimation de la charge et allocation des ressources, en coordonnant des équipes multidisciplinaires avec respect de la diversité et promotion de l'inclusion, en assurant des conditions de travail sûres et saines conformes aux principes SST, en suivant l'avancement avec métriques quantitatives (vélocité, burndown, taux de complétion), en créant des dashboards de pilotage accessibles RGAA 4.1 niveau AA, en gérant les risques projet avec identification proactive et plans de mitigation, afin de livrer les projets dans les délais, budget et qualité attendus.

Manager des équipes techniques multidisciplinaires en recrutant et intégrant les talents avec processus inclusif valorisant la diversité, en définissant clairement les rôles et responsabilités de chacun, en animant les cérémonies agiles avec participation active de tous, en favorisant le développement des compétences par formation et mentorat, en gérant les situations conflictuelles avec médiation et communication non-violente, en assurant le bien-être au travail avec prévention des risques psychosociaux, en promouvant la responsabilité sociétale et environnementale dans les pratiques de l'équipe, afin de construire une équipe performante, soudée et engagée.

Identifier et évaluer les risques en réalisant une cartographie exhaustive des risques techniques (vulnérabilités, obsolescence, dépendances), financiers (dépassements budgétaires, volatilité crypto), opérationnels (disponibilité équipes), réglementaires et de réputation, en évaluant quantitativement chaque risque (probabilité × impact avec métriques financières) et en priorisant selon criticité avec matrice de risques documentée dans un registre maintenu à jour, en élaborant des stratégies de mitigation en définissant pour chaque risque majeur une stratégie appropriée (éviter, réduire, transférer, accepter) avec actions concrètes et responsables identifiés, en créant des plans de contingence détaillés pour scénarios critiques avec procédures de gestion de crise (cellule de crise, escalation, communication), en réalisant des exercices de simulation pour tester les procédures et en documentant les incidents avec analyse des causes racines (5 Why, Ishikawa), afin d'anticiper les problèmes, minimiser l'impact des risques et améliorer continuellement la résilience.

Gérer les budgets et optimiser les coûts en élaborant un budget détaillé par poste (développement, infrastructure cloud, licences, audit, formation) avec justification des estimations, en suivant l'exécution budgétaire avec outils de tracking en temps réel et alertes automatiques sur dépassements (10%), en appliquant les principes FinOps (analyse continue, rightsizing, utilisation d'instances spot/reserved), en négociant avec les fournisseurs pour obtenir les meilleurs tarifs, en produisant des rapports financiers réguliers avec analyse des écarts (budgété vs réel) et forecast actualisé, afin de maximiser le retour sur investissement.

Coordonner avec les équipes de conformité et juridique en intégrant les exigences réglementaires dès la conception du projet (security by design, privacy by design), en collaborant étroitement avec les équipes conformité pour validation des choix techniques, en assurant la traçabilité des décisions avec documentation audit-ready, en anticipant les évolutions réglementaires (MiCA, PSAN, AML/KYC) et leur impact sur le projet, en coordonnant les audits de conformité externes avec préparation de la documentation, afin de garantir la conformité légale continue du projet.

Communiquer efficacement avec les parties prenantes en établissant un plan de communication adapté à chaque audience (direction, équipes techniques, clients, investisseurs), en créant des tableaux de bord exécutifs accessibles RGAA 4.1 niveau AA avec KPIs clés et visualisations impactantes, en rédigeant des rapports d'avancement clairs avec focus sur les décisions requises, en présentant les concepts techniques complexes de manière compréhensible avec analogies et storytelling, en gérant les attentes avec transparence et honnêteté, en facilitant les prises de décision collégiales avec méthodes structurées, afin d'assurer l'alignement et l'engagement de toutes les parties prenantes.

Promouvoir l'amélioration continue et la responsabilité sociétale (RSE) en organisant des rétrospectives régulières avec identification des axes d'amélioration et plans d'action concrets, en mettant en place des indicateurs de performance et d'amélioration continue suivis dans le temps, en intégrant les principes RSE dans les décisions techniques avec évaluation de l'impact environnemental (consommation énergétique des blockchains PoW vs PoS, optimisation ressources) et social (accessibilité, inclusion, bien-être), en sensibilisant l'équipe aux enjeux RSE et aux bonnes pratiques d'éco-conception, en documentant et partageant les bonnes pratiques au sein de l'organisation, afin de contribuer à une démarche d'excellence opérationnelle et de responsabilité globale.

Assurer la conformité au règlement MiCA en identifiant le statut réglementaire des actifs numériques émis (crypto-actifs, jetons référencés actifs, jetons de monnaie électronique), en appliquant les exigences de fonds propres et de gouvernance pour les prestataires CASP, en rédigeant le White Paper conforme avec informations obligatoires sur les risques, en implémentant les procédures de traitement des réclamations et de gestion des conflits d'intérêts, et en assurant la notification et coopération avec les autorités (ACPR, AMF, ESMA), en garantissant la conformité PSAN en France en préparant le dossier d'enregistrement ou d'agrément AMF avec justificatifs des moyens (humains, techniques, financiers), en implémentant les dispositifs LCB-FT avec procédures de vigilance client et déclarations TRACFIN, en assurant la séparation des actifs clients et en mettant en place les procédures de lutte contre la manipulation de marché, afin de garantir la légalité des opérations crypto-actifs en Europe et en France.

Implémenter les processus KYC/AML (Know Your Customer / Anti-Money Laundering) en définissant les niveaux de vigilance requis selon l'approche basée sur les risques (vigilance simplifiée, standard, renforcée), en intégrant des outils de vérification d'identité électronique (eIDAS, solutions biométriques) et de screening contre les listes de sanctions (OFAC, UE, ONU), en classifiant les clients selon leur profil de risque (PEP, pays à haut risque, activités sensibles), en monitorant les transactions avec règles de détection d'activités suspectes (montants atypiques, patterns de smurfing, layering), en rédigeant et transmettant les déclarations de soupçon à TRACFIN selon les délais réglementaires.

Assurer la conformité RGPD (Règlement Général Protection Données) et privacy by design en réalisant des analyses d'impact sur la protection des données (DPIA) pour les traitements à risque élevé, en implémentant les principes de minimisation des données, limitation de la finalité et limitation de la conservation, en garantissant les droits des personnes (accès, rectification, effacement, portabilité) malgré l'immutabilité blockchain via techniques de pseudonymisation et encryption, en assurant la sécurité des données personnelles avec chiffrement at-rest et in-transit, en tenant un registre des traitements et en désignant un DPO (Data Protection Officer) si requis.

Fournir du conseil stratégique aux dirigeants en analysant les opportunités blockchain pour l'organisation (réduction des coûts, nouveaux revenus, amélioration de l'efficacité opérationnelle), en évaluant les risques stratégiques (adoption technologique, risque réglementaire, risque de réputation), en réalisant des analyses coûts-bénéfices et calculs de ROI avec scénarios multiples, en développant des roadmaps stratégiques alignées avec les objectifs business et les contraintes réglementaires, en créant des outils de conseil accessibles RGAA 4.1 niveau AA (dashboards stratégiques, simulateurs) pour faciliter la prise de décision, en présentant les recommandations de manière convaincante avec storytelling et data visualization.

Évaluer l'impact sociétal et RSE des solutions blockchain en analysant l'impact environnemental (consommation énergétique des différents consensus PoW/PoS/DPoS, empreinte carbone, optimisation ressources), en évaluant l'impact social (inclusion financière, accessibilité services, création d'emploi, protection des consommateurs), en identifiant les risques éthiques (vie privée, surveillance, biais algorithmiques, gouvernance décentralisée), en proposant des mesures d'atténuation des impacts négatifs et de maximisation des impacts positifs, en documentant l'analyse RSE avec indicateurs quantitatifs et qualitatifs, en alignant les solutions avec les Objectifs de Développement Durable (ODD) des Nations Unies.

Coordonner les audits réglementaires et représenter l'organisation en préparant la documentation audit-ready avec registres à jour (traitements de données, opérations blockchain, incidents de sécurité), en organisant les entretiens avec les auditeurs et en fournissant les preuves de conformité requises, en répondant aux demandes d'information des régulateurs (ACPR, AMF, CNIL) dans les délais impartis avec précision et exhaustivité, en gérant les non-conformités identifiées avec plans d'action correctifs et suivi de leur implémentation, en représentant l'organisation lors de réunions avec les autorités compétentes avec préparation rigoureuse et communication professionnelle.

Former et sensibiliser les équipes à la conformité blockchain en créant des programmes de formation adaptés aux différents rôles (développeurs, opérations, commercial, direction) couvrant MiCA, PSAN, AML/KYC, RGPD, en développant des supports pédagogiques engageants (e-learning, cas pratiques, quiz) avec formats accessibles, en organisant des sessions de sensibilisation régulières aux évolutions réglementaires, en créant une base de connaissances conformité avec FAQ, procédures, modèles de documents, en instaurant une culture de conformité avec responsabilisation de chacun et processus d'escalation clairs, en mesurant l'efficacité des formations avec

Blocs de compétences

RNCP42467BC01 — Sécuriser et optimiser les infrastructures blockchain

LISTE DE COMPÉTENCES

Concevoir l'architecture de sécurité globale des systèmes blockchain en évaluant les options techniques (publique/privée/consortium, consensus PoS/PoW/PBFT, architecture réseau, scalabilité Layer 2), en arbitrant entre sécurité/performance/décentralisation, en définissant les standards de sécurité et politiques organisationnelles, en déployant les infrastructures sur cloud (AWS/Azure/GCP) avec services managés adaptés, en automatisant le déploiement avec Infrastructure-as-Code (Terraform, Docker, Ansible, Kubernetes), en configurant la haute disponibilité multi-zones et load balancing, en implémentant la segmentation réseau stricte et le durcissement selon bonnes pratiques CIS, afin d'établir une architecture sécurisée, scalable, résiliente et opérationnelle.

Automatiser le déploiement et la gestion des infrastructures en utilisant Infrastructure-as-Code (Terraform, Docker, Ansible, Kubernetes, Helm), en créant des pipelines CI/CD avec tests intégrés, en versionnant les configurations dans Git avec code review obligatoire, en implémentant des tests automatisés de sécurité (scanning, vulnerability assessment), en développant des API REST pour exposition des services d'infrastructure, en configurant des systèmes de monitoring complets (Prometheus, Grafana, CloudWatch/Azure Monitor, stack ELK), en définissant les métriques et KPIs critiques, en créant des dashboards temps réel accessibles (RGAA 4.1 niveau AA), en configurant des alertes automatiques avec escalation, en analysant les logs pour détecter comportements suspects, afin d'assurer reproductibilité, traçabilité, qualité continue, disponibilité 24/7 et détection rapide d'incidents.

Gérer de manière sécurisée les clés cryptographiques en concevant une politique complète couvrant le cycle de vie (génération, stockage, rotation, révocation, destruction), en déployant des HSM on-premise ou KMS cloud, en implémentant multi-signature et threshold signatures pour opérations critiques, en définissant les procédures de backup/recovery avec tests réguliers, en auditant les accès avec traçabilité complète, afin de protéger les actifs contre vol ou compromission.

Assurer la résilience et continuité de service en définissant une stratégie de sauvegarde avec objectifs RPO/RTO selon criticité métier, en mettant en place des backups automatisés avec géo-réplication, en concevant des plans de disaster recovery avec procédures de basculement testées, en réalisant des tests réguliers de restauration et exercices de crise, en documentant les procédures d'escalade avec rôles clairs, afin de garantir récupération rapide en cas d'incident majeur.

Optimiser les coûts et performances des infrastructures cloud en appliquant les principes FinOps (analyse continue, rightsizing, instances spot/reserved), en monitorant les coûts par service avec alertes sur dépassements, en identifiant les opportunités d'optimisation (ressources inutilisées, dimensionnement approprié, caching), en équilibrant performance et coût selon exigences métier, en documentant les décisions avec analyse coût/bénéfice, afin de maximiser l'efficacité économique.

Former et documenter pour assurer le transfert de compétences en créant une documentation technique complète et à jour (architectures, procédures d'exploitation, runbooks d'incidents) sous formats numérique et papier adaptables aux situations de handicap (alternatives textuelles, contraste suffisant, navigation clavier pour les supports numériques), en formant les équipes d'exploitation aux technologies blockchain et aux procédures de sécurité, en créant des supports pédagogiques adaptés aux différents niveaux et adaptables aux besoins spécifiques des personnes en situation de handicap, en accompagnant la montée en compétences avec mentorat et coaching, afin d'assurer l'autonomie opérationnelle des équipes et la pérennité des solutions.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle Réelle/ Reconstituée -

Travail individuel -

À partir d'un cas d'entreprise, le candidat conçoit et déploie une infrastructure blockchain sécurisée complète.

Livrables à produire :

Dossier d'architecture de sécurité blockchain avec choix techniques justifiés, threat modeling, infrastructure déployée en Infrastructure-as-Code, pipeline CI/CD et monitoring temps réel avec dashboards accessibles RGAA 4.1 niveau AA

Politique de gestion des clés cryptographiques avec couverture du cycle de vie complet, , mécanismes multi-signature et threshold signatures et procédures de backup/recovery testées

Plan de continuité de service avec stratégie de sauvegarde, géo-réplication multi-zones, plan de disaster recovery

détaillé, procédures d'escalade et tests de restauration documentés

Analyse FinOps d'optimisation des coûts avec estimation budgétaire par service, opportunités d'optimisation chiffrées, arbitrages coût/performance documentés et plan d'amélioration continue

Plan de transfert de compétences avec documentation technique complète, supports de formation adaptables aux situations de handicap et plan de mentorat structuré

Déroulement de la soutenance :

Phase 1 – Présentation par le candidat - Le candidat présente son projet en s'appuyant sur ses livrables : architecture de sécurité conçue avec justification des choix techniques (blockchain type, consensus, cloud provider), démonstration de l'infrastructure déployée fonctionnelle, présentation du système de monitoring et des dashboards, explication de la stratégie de gestion des clés et des procédures de continuité de service.

Phase 2 – Échanges collectifs avec le jury - Le jury pose des questions collectives pour approfondir : justification des arbitrages sécurité/performance/coût réalisés, analyse des choix d'architecture et des alternatives envisagées, pertinence des mécanismes de scalabilité et de résilience mis en œuvre.

Phase 3 – Entretien technique approfondi - Questions techniques individuelles des membres du jury pour évaluer la maîtrise : capacité à résoudre des incidents complexes sur l'infrastructure, compréhension approfondie des mécanismes cryptographiques et de sécurité, analyse de scénarios de menaces et propositions de contre-mesures, évaluation de la vision stratégique et du recul sur les technologies blockchain.

Phase 4 – Délibération du jury hors présence du candidat, le jury évalue les livrables selon les critères définis, attribue la note finale et prépare le retour au candidat.

Jury de soutenance (3 personnes minimum) : Professionnel en

architecture blockchain sécurisée (3+ ans d'expérience) - Professionnel en infrastructures cloud sécurisées (certifications AWS/Azure/GCP) - Représentant de l'organisme certificateur (président). Au moins 2 membres externes, aucun formateur du candidat.

RNCP42467BC02 — Auditer la sécurité des smart contracts avant leur déploiement et sécuriser leur environnement

LISTE DE COMPÉTENCES

Auditer la sécurité des smart contracts multi-langages en effectuant une revue manuelle ligne par ligne du code source Solidity, Rust (pour Solana, Polkadot, Substrate) et Move (pour Aptos, Sui), en recherchant systématiquement les patterns de vulnérabilités (reentrancy, integer overflow/underflow, access control, front-running, oracle manipulation, flashloan attacks), en vérifiant la conformité aux spécifications fonctionnelles, en créant des preuves de concept d'exploitation pour les vulnérabilités critiques, afin d'identifier exhaustivement les failles de sécurité avant déploiement en production.

Effectuer des tests automatisés de sécurité en utilisant prioritairement Foundry (framework Rust-based pour tests rapides et fuzzing) ou Hardhat (framework JavaScript complet), en implémentant des tests unitaires couvrant toutes les fonctions critiques, en réalisant du fuzzing pour tests basés sur propriétés, en utilisant des analyseurs statiques complémentaires (Slither, Mythril), en intégrant ces tests dans les pipelines CI/CD pour vérification automatique à chaque commit, afin de détecter systématiquement les failles de sécurité avant déploiement.

Sécuriser les protocoles DeFi complexes en analysant les mécanismes économiques (Automated Market Makers, protocoles de lending, yield aggregators, produits dérivés), en identifiant les risques de manipulation (manipulation d'oracle, sandwich attacks, extraction MEV, attaques de gouvernance), en testant la robustesse des oracles avec simulation de scénarios extrêmes, en analysant les risques de composabilité entre protocoles interconnectés, en proposant des contre-mesures techniques et économiques, afin de prévenir les pertes financières majeures.

Analyser les risques économiques et de gouvernance en évaluant les mécanismes de tokenomics (distribution, vesting, inflation), en identifiant les vecteurs d'attaque économique (manipulations de vote, accumulation de pouvoir, attaques de gouvernance), en analysant la résilience face aux chocs économiques et variations de liquidité, en évaluant les risques systémiques de contagion entre protocoles, en proposant des ajustements de paramètres économiques pour améliorer la sécurité, afin de garantir la stabilité économique du protocole.

Documenter les audits de sécurité en rédigeant des rapports détaillés et accessibles incluant (1) description technique précise de chaque vulnérabilité avec extraits de code, (2) scénario d'exploitation par un attaquant, (3) estimation de l'impact financier potentiel, (4) classification de criticité (Critical/High/Medium/Low) selon CVSS, (5) recommandations de correction avec suggestions de code, (6) résumé exécutif pour dirigeants non techniques, en produisant des livrables aux formats numériques accessibles (conformité RGAA 4.1 niveau AA pour les rapports en ligne) et adaptables aux destinataires en situation de handicap, afin de communiquer efficacement les findings à toutes les parties prenantes.

Développer des interfaces et intégrations en créant des interfaces Web3 avec web3.js ou ethers.js pour interagir avec les smart contracts, en développant des API REST pour exposer les fonctionnalités blockchain aux applications externes, en implémentant des tests d'intégration end-to-end couvrant l'ensemble de la stack, en documentant les endpoints API avec spécifications OpenAPI/Swagger, en assurant la sécurité des intégrations avec authentification et gestion des erreurs, afin de faciliter l'adoption et l'intégration des protocoles blockchain.

Maintenir une veille technologique et sécuritaire continue en suivant les publications de sécurité (audits publics, post-mortems d'incidents, recherches académiques), en analysant les exploits récents pour identifier les patterns d'attaque émergents, en participant activement aux communautés de sécurité blockchain (Discord, forums spécialisés), en expérimentant avec les nouvelles techniques d'attaque et de défense, en se formant aux nouvelles technologies blockchain (L2, zkEVMs, nouvelles chaînes), en participant aux programmes de bug bounty en analysant le code de protocoles pour identifier des vulnérabilités inédites, en documentant les findings selon les standards des plateformes (Immunefi, HackerOne, Code4rena) et en collaborant avec les équipes projets pour la vérification des corrections, afin de rester à jour sur les menaces émergentes et de contribuer à l'amélioration de la sécurité de l'écosystème.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle Réelle/ Reconstituée - Travail individuel - À partir de smart contracts DeFi (Solidity et/ou Rust), le candidat réalise un audit de sécurité complet incluant revue manuelle, tests automatisés avec Foundry/Hardhat, création de PoC d'exploitation, développement d'interfaces Web3 et rédaction du rapport d'audit.

Livrables à produire :

Audit de sécurité des smart contracts multi-langages (Solidity, Rust, Move) avec tests automatisés intégrés en pipeline CI/CD (Foundry, Slither, Mythril)

Rapport de sécurité des protocoles DeFi avec analyse économique (AMM, lending, yield aggregators), risques de manipulation (oracle, MEV) et tokenomics (C2.3 + C2.4)

Rapport d'audit accessible RGAA 4.1 niveau AA avec classification CVSS, résumé exécutif et dispositif de veille technologique (bug bounty Immunefi/HackerOne) (C2.5 + C2.7)

Interface Web3 et API REST documentée (web3.js/ethers.js, OpenAPI/Swagger) avec tests d'intégration end-to-end et mécanismes de sécurité (C2.6)

Déroulement de la soutenance :

Phase 1 – Présentation par le candidat - Le candidat présente son audit en s'appuyant sur le rapport : méthodologie d'audit appliquée avec outils utilisés (Foundry, Hardhat, analyseurs statiques), principales vulnérabilités identifiées avec démonstration de PoC critiques, analyse de l'impact financier potentiel des failles, recommandations de correction et priorisation, interface Web3 développée pour tests.

Phase 2 – Échanges collectifs avec le jury

- Questions collectives pour approfondir : justification de la criticité attribuée aux vulnérabilités, pertinence de la méthodologie d'audit choisie, exhaustivité de la couverture des vecteurs d'attaque, qualité et applicabilité des recommandations.

Phase 3 – Entretien technique approfondi - Questions techniques individuelles : capacité à identifier des vulnérabilités complexes non triviales, compréhension approfondie des mécanismes DeFi et attaques spécifiques, maîtrise des frameworks de test (Foundry/Hardhat) et outils d'analyse, analyse de nouveaux vecteurs d'attaque émergents.

Phase 4 – Délibération du jury hors présence du candidat, il évalue les livrables selon critères, attribue la note et prépare le retour.

Jury de soutenance (3 personnes minimum) : Professionnel en audit smart contracts multi-langages (3+ ans d'expérience Solidity/Rust) - Professionnel en sécurité DeFi avec expérience protocoles majeurs - Représentant de l'organisme certificateur (président). Au moins 2 membres externes, aucun formateur du candidat.

RNCP42467BC03 — Capitaliser sur les données blockchain pour renforcer la sécurité

LISTE DE COMPÉTENCES

Analyser les données blockchain on-chain en collectant et indexant les données via nodes full et API (Etherscan, The Graph, Dune Analytics), en analysant les patterns transactionnels pour identifier comportements suspects (wash trading, pump and dump, money laundering), en effectuant du clustering d'adresses et traçage des flux de fonds avec outils spécialisés (Chainalysis, Elliptic), en développant des systèmes de détection d'anomalies par machine learning (isolation forests, autoencoders, LSTM) avec feature engineering pertinent, entraînement sur données historiques, évaluation des performances (précision/rappel/F1, ROC) et déploiement en production avec monitoring continu, afin de détecter automatiquement les transactions suspectes en temps réel.

Réaliser des investigations forensiques post-incident en collectant et préservant les preuves numériques selon les standards forensiques, en reconstituant la chronologie complète de l'incident avec timeline précise des événements,

en traçant les flux de fonds volés à travers échanges centralisés et décentralisés, mixers (Tornado Cash) et chain hopping avec outils Chainalysis et Elliptic, en identifiant les acteurs malveillants via OSINT, corrélation d'adresses et analyse comportementale, en documentant l'investigation avec chaîne de traçabilité des preuves, afin de supporter les actions légales et récupérations d'actifs.

Corréler les événements de sécurité en collectant des données de multiples sources (logs blockchain, SIEM, threat intelligence feeds, dark web monitoring), en normalisant et enrichissant les événements pour analyse unifiée, en implémentant des règles de corrélation pour détecter les attaques multi-étapes, en identifiant les chaînes d'attaque complexes (kill chains) avec reconstruction des TTPs, en priorisant les alertes selon la criticité et l'impact potentiel, afin de détecter les attaques sophistiquées nécessitant coordination de multiples actions.

Produire de l'intelligence des menaces en collectant des renseignements depuis des sources OSINT, threat intelligence feeds commerciales et dark web monitoring, en analysant les TTPs des groupes d'attaquants selon le framework MITRE ATT&CK adapté à la blockchain, en créant et maintenant des indicateurs de compromission (IoC) réutilisables (adresses malveillantes, patterns de transactions, signatures d'attaque), en contextualisant les menaces selon les actifs et profil de risque de l'organisation, en produisant des rapports d'intelligence stratégique et tactique, afin d'anticiper proactivement les risques émergents.

Développer des règles de détection, API et tableaux de bord en créant des règles SIEM optimisées pour attaques blockchain spécifiques, en définissant des KPIs de sécurité pertinents (taux d'attaques, temps de détection, impact financier), en développant des dashboards interactifs conformes RGAA 4.1 niveau AA avec visualisations temps réel, en créant des API REST documentées (OpenAPI/Swagger) pour exposer les fonctionnalités d'analyse, en automatisant les réponses aux incidents courants avec playbooks SOAR, en communiquant les résultats d'analyse via rapports techniques détaillés avec méthodologie et preuves, résumés exécutifs synthétiques pour la direction avec focus impact business, et visualisations impactantes (infographies, graphes, heat maps) accessibles aux destinataires en situation de handicap (alternatives textuelles aux visualisations, contraste 4.5:1, structure de document navigable), afin d'améliorer l'efficacité du SOC blockchain et d'assurer l'appropriation des recommandations par tous les niveaux.

Maintenir et améliorer les capacités d'analyse en effectuant des retours d'expérience post-incident pour améliorer les processus, en développant et maintenant des scripts d'analyse réutilisables et automatisés, en créant une base de connaissances des techniques d'attaque et d'investigation, en formant les équipes SOC aux techniques d'analyse blockchain, en participant à la recherche et développement de nouvelles techniques de détection, afin d'améliorer continuellement l'efficacité du centre d'opérations de sécurité.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle Réelle/ Reconstituée -

Travail individuel -

À partir d'un incident de sécurité (hack, fraude, blanchiment), le candidat réalise une analyse complète des données blockchain, développe un système de détection d'anomalies avec ML, crée des dashboards accessibles RGAA 4.1 et produit un rapport d'investigation forensique avec API REST.

Livrables à produire :

Rapport d'investigation forensique avec chronologie de l'incident, graphes de flux de fonds et identification des acteurs (C3.1, C3.2)

Modèle de détection d'anomalies avec code source, métriques de performance (précision, rappel, F1-score) et rapport d'intelligence des menaces avec analyse des TTPs et recommandations défensives (C3.3, C3.4)

Dashboard d'analyse accessible RGAA 4.1 niveau AA avec visualisations interactives et KPIs de sécurité (C3.5)

Dispositif d'amélioration continue avec un plan de retour d'expérience post-incident formalisé et adapté et un plan de formation adaptable et adapté des équipes SOC à l'analyse blockchain. (C3.6)

Déroulement de la soutenance :

Phase 1 – Présentation par le candidat - Le candidat présente son investigation : méthodologie d'analyse adoptée et outils utilisés (Chainalysis, Elliptic, Dune), reconstitution chronologique de l'incident avec graphes de flux, modèle de détection ML développé avec métriques de performance, dashboards accessibles RGAA 4.1, API REST développée, indicateurs de compromission identifiés et recommandations.

Phase 2 – Échanges collectifs avec le jury - Questions collectives pour approfondir : pertinence de la méthodologie d'investigation choisie, exhaustivité de la traçabilité des fonds et identification des acteurs, efficacité du modèle ML avec taux de détection et faux positifs, conformité RGAA 4.1 des dashboards, applicabilité opérationnelle des recommandations proposées.

Phase 3 – Entretien technique approfondi - Questions techniques individuelles : maîtrise des techniques de clustering

et désanonymisation, compréhension des algorithmes ML et feature engineering, capacité à analyser des scénarios complexes multi-chains, connaissance des techniques d'évasion et contre-mesures, qualité de l'architecture API REST.

Phase 4 – Délibération du jury hors présence du candidat, il évalue les livrables selon critères, attribue la note et prépare le retour.

Jury de soutenance (3 personnes minimum) : Professionnel en data science et machine learning appliqués à la sécurité - Professionnel en forensique blockchain et investigation (Chainalysis/Elliptic/CipherTrace) - Représentant de l'organisme certificateur (président). Au moins 2 membres externes, aucun formateur du candidat.

RNCP42467BC04 — Piloter les projets blockchain et gérer les risques

LISTE DE COMPÉTENCES

Piloter des projets blockchain complexes en définissant la roadmap technique alignée avec les objectifs business et les contraintes de sécurité, en planifiant les sprints avec estimation de la charge et allocation des ressources, en coordonnant des équipes multidisciplinaires avec respect de la diversité et promotion de l'inclusion, en assurant des conditions de travail sûres et saines conformes aux principes SST, en suivant l'avancement avec métriques quantitatives (vélocité, burndown, taux de complétion), en créant des dashboards de pilotage accessibles RGAA 4.1 niveau AA, en gérant les risques projet avec identification proactive et plans de mitigation, afin de livrer les projets dans les délais, budget et qualité attendus.

Manager des équipes techniques multidisciplinaires en recrutant et intégrant les talents avec processus inclusif valorisant la diversité, en définissant clairement les rôles et responsabilités de chacun, en animant les cérémonies agiles avec participation active de tous, en favorisant le développement des compétences par formation et mentorat, en gérant les situations conflictuelles avec médiation et communication non-violente, en assurant le bien-être au travail avec prévention des risques psychosociaux, en promouvant la responsabilité sociétale et environnementale dans les pratiques de l'équipe, afin de construire une équipe performante, soudée et engagée.

Identifier et évaluer les risques en réalisant une cartographie exhaustive des risques techniques (vulnérabilités, obsolescence, dépendances), financiers (dépassements budgétaires, volatilité crypto), opérationnels (disponibilité équipes), réglementaires et de réputation, en évaluant quantitativement chaque risque (probabilité × impact avec métriques financières) et en priorisant selon criticité avec matrice de risques documentée dans un registre maintenu à jour, en élaborant des stratégies de mitigation en définissant pour chaque risque majeur une stratégie appropriée (éviter, réduire, transférer, accepter) avec actions concrètes et responsables identifiés, en créant des plans de contingence détaillés pour scénarios critiques avec procédures de gestion de crise (cellule de crise, escalation, communication), en réalisant des exercices de simulation pour tester les procédures et en documentant les incidents avec analyse des causes racines (5 Why, Ishikawa), afin d'anticiper les problèmes, minimiser l'impact des risques et améliorer continuellement la résilience.

Gérer les budgets et optimiser les coûts en élaborant un budget détaillé par poste (développement, infrastructure cloud, licences, audit, formation) avec justification des estimations, en suivant l'exécution budgétaire avec outils de tracking en temps réel et alertes automatiques sur dépassements (10%), en appliquant les principes FinOps (analyse continue, rightsizing, utilisation d'instances spot/reserved), en négociant avec les fournisseurs pour obtenir les meilleurs tarifs, en produisant des rapports financiers réguliers avec analyse des écarts (budgété vs réel) et forecast actualisé, afin de maximiser le retour sur investissement.

Coordonner avec les équipes de conformité et juridique en intégrant les exigences réglementaires dès la conception du projet (security by design, privacy by design), en collaborant étroitement avec les équipes conformité pour validation des choix techniques en s'adaptant aux besoins de communication de chaque interlocuteur (formats accessibles, modalités d'échange adaptables), en assurant la traçabilité des décisions avec documentation audit-ready et accessible, en anticipant les évolutions réglementaires (MiCA, PSAN, AML/KYC) et leur impact sur le projet, en coordonnant les audits de conformité externes avec préparation de la documentation, afin de garantir la conformité légale continue du projet.

Communiquer efficacement avec les parties prenantes en établissant un plan de communication adapté à chaque audience (direction, équipes techniques, clients, investisseurs), en créant des tableaux de bord exécutifs accessibles RGAA 4.1 niveau AA avec KPIs clés et visualisations impactantes, en rédigeant des rapports d'avancement clairs avec focus sur les décisions requises, en présentant les concepts techniques complexes de manière compréhensible avec analogies et storytelling, en gérant les attentes avec transparence et honnêteté, en facilitant les prises de décision collégiales avec méthodes structurées, afin d'assurer l'alignement et l'engagement de toutes les parties prenantes.

Promouvoir l'amélioration continue et la responsabilité sociétale (RSE) en organisant des rétrospectives régulières

avec identification des axes d'amélioration et plans d'action concrets, en mettant en place des indicateurs de performance et d'amélioration continue suivis dans le temps, en intégrant les principes RSE dans les décisions techniques avec évaluation de l'impact environnemental (consommation énergétique des blockchains PoW vs PoS, optimisation ressources) et social (accessibilité, inclusion, bien-être), en sensibilisant l'équipe aux enjeux RSE et aux bonnes pratiques d'éco-conception, en documentant et partageant les bonnes pratiques au sein de l'organisation, afin de contribuer à une démarche d'excellence opérationnelle et de responsabilité globale.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle Réelle/ Reconstituée -

Travail individuel ou en Binôme -

À partir d'un projet blockchain complexe, le candidat élabore la roadmap, pilote l'équipe avec management inclusif et conditions SST, gère les risques, optimise les coûts, intègre les principes RSE et produit les livrables de pilotage avec dashboards accessibles RGAA 4.1.

Livrables à produire :

Roadmap technique détaillée avec priorisation MoSCoW, estimation des charges, jalons clés, cartographie quantitative des risques, stratégies de mitigation et plans de contingence (C4.1 + C4.3)

Documentation d'organisation d'équipe avec organigramme, matrice RACI, mesures SST, démarche d'inclusion, trame de rétrospectives, indicateurs d'amélioration continue et plan de sensibilisation RSE (C4.2 + C4.7)

Plan budgétaire détaillé avec estimation par poste, suivi des écarts budgétés/réels, analyse FinOps et plan d'optimisation chiffré (C4.4)

Dispositif de coordination conformité avec gap analysis MiCA/PSAN/AML/KYC/RGPD, registre de traçabilité des décisions, veille réglementaire et plan de préparation aux audits externes (C4.5)

Plan de communication parties prenantes avec dashboards de pilotage accessibles RGAA 4.1 niveau AA, modèles de rapports d'avancement et supports de présentation accessibles aux audiences non-techniques (C4.6)

Déroulement de la soutenance :

Phase 1 – Présentation par le candidat - Le candidat présente son pilotage de projet : roadmap technique justifiée avec priorisation explicite, organisation de l'équipe avec méthodes de travail inclusives et respect des principes SST (prévention risques psychosociaux, équilibre vie pro/perso), suivi de l'avancement avec dashboards accessibles RGAA 4.1, gestion des risques et plans de mitigation, optimisation des coûts avec stratégie FinOps, intégration RSE avec évaluation impact environnemental (choix consensus PoS vs PoW) et social.

Phase 2 – Échanges collectifs avec le jury - Questions collectives pour approfondir : pertinence de la roadmap et priorisation des fonctionnalités, efficacité du management d'équipe inclusif avec promotion de la diversité, application concrète des principes SST dans l'organisation du travail, qualité du suivi avec métriques et dashboards accessibles, gestion proactive des risques identifiés, intégration RSE dans les décisions techniques.

Phase 3 – Entretien technique approfondi - Questions individuelles : capacité à gérer des situations de crise et arbitrer sous contraintes, compréhension des enjeux business et alignement stratégique, maîtrise des méthodes agiles et adaptation au contexte, analyse des impacts RSE (environnementaux et sociaux) et démarche d'amélioration continue, gestion du bien-être au travail et prévention des risques psychosociaux.

Phase 4 – Délibération du jury hors présence du candidat, il évalue les livrables selon critères, attribue la note et prépare le retour.

Jury de soutenance (3 personnes minimum) : Professionnel en pilotage de projets blockchain complexes (certification PMP/Prince2 ou équivalent) - Professionnel en management d'équipes techniques et transformation digitale - Représentant de l'organisme certificateur (président). Au moins 2 membres externes, aucun formateur du candidat.

RNCP42467BC05 — Garantir la conformité réglementaire et fournir le conseil stratégique dans le cadre de projets blockchain

LISTE DE COMPÉTENCES

Assurer la conformité au règlement MiCA en identifiant le statut réglementaire des actifs numériques émis (crypto-actifs, jetons référencés actifs, jetons de monnaie électronique), en appliquant les exigences de fonds propres et de gouvernance pour les prestataires CASP, en rédigeant le White Paper conforme avec informations obligatoires sur les risques, en implémentant les procédures de traitement des réclamations et de gestion des conflits d'intérêts, et en assurant la notification et coopération avec les autorités (ACPR, AMF, ESMA), en garantissant la conformité PSAN en France en préparant le dossier d'enregistrement ou d'agrément AMF avec justificatifs des moyens (humains, techniques, financiers), en implémentant les dispositifs LCB-FT avec procédures de vigilance client et déclarations TRACFIN, en assurant la séparation des actifs clients et en mettant en place les procédures de lutte contre la manipulation de marché, afin de garantir la légalité des opérations crypto-actifs en Europe et en France.

Implémenter les processus KYC/AML (Know Your Customer / Anti-Money Laundering) en définissant les niveaux de vigilance requis selon l'approche basée sur les risques (vigilance simplifiée, standard, renforcée), en intégrant des outils de vérification d'identité électronique (eIDAS, solutions biométriques) et de screening contre les listes de sanctions (OFAC, UE, ONU), en classifiant les clients selon leur profil de risque (PEP, pays à haut risque, activités sensibles), en monitorant les transactions avec règles de détection d'activités suspectes (montants atypiques, patterns de smurfing, layering), en rédigeant et transmettant les déclarations de soupçon à TRACFIN selon les délais réglementaires.

Assurer la conformité RGPD (Règlement Général Protection Données) et privacy by design en réalisant des analyses d'impact sur la protection des données (DPIA) pour les traitements à risque élevé, en implémentant les principes de minimisation des données, limitation de la finalité et limitation de la conservation, en garantissant les droits des personnes (accès, rectification, effacement, portabilité) malgré l'immutabilité blockchain via techniques de pseudonymisation et encryption, en assurant la sécurité des données personnelles avec chiffrement at-rest et in-transit, en tenant un registre des traitements et en désignant un DPO (Data Protection Officer) si requis.

Fournir du conseil stratégique aux dirigeants en analysant les opportunités blockchain pour l'organisation (réduction des coûts, nouveaux revenus, amélioration de l'efficacité opérationnelle), en évaluant les risques stratégiques (adoption technologique, risque réglementaire, risque de réputation), en réalisant des analyses coûts-bénéfices et calculs de ROI avec scénarios multiples, en développant des roadmaps stratégiques alignées avec les objectifs business et les contraintes réglementaires, en créant des outils de conseil accessibles RGAA 4.1 niveau AA (dashboards stratégiques, simulateurs) pour faciliter la prise de décision, en présentant les recommandations de manière convaincante avec storytelling et data visualization.

Évaluer l'impact sociétal et RSE des solutions blockchain en analysant l'impact environnemental (consommation énergétique des différents consensus PoW/PoS/DPoS, empreinte carbone, optimisation ressources), en évaluant l'impact social (inclusion financière, accessibilité services, création d'emploi, protection des consommateurs), en identifiant les risques éthiques (vie privée, surveillance, biais algorithmiques, gouvernance décentralisée), en proposant des mesures d'atténuation des impacts négatifs et de maximisation des impacts positifs, en documentant l'analyse RSE avec indicateurs quantitatifs et qualitatifs, en alignant les solutions avec les Objectifs de Développement Durable (ODD) des Nations Unies.

Coordonner les audits réglementaires et représenter l'organisation en préparant la documentation audit-ready avec registres à jour (traitements de données, opérations blockchain, incidents de sécurité), en organisant les entretiens avec les auditeurs et en fournissant les preuves de conformité requises, en répondant aux demandes d'information des régulateurs (ACPR, AMF, CNIL) dans les délais impartis avec précision et exhaustivité, en gérant les non-conformités identifiées avec plans d'action correctifs et suivi de leur implémentation, en représentant l'organisation lors de réunions avec les autorités compétentes avec préparation rigoureuse et communication professionnelle.

Former et sensibiliser les équipes à la conformité blockchain en créant des programmes de formation adaptés aux différents rôles (développeurs, opérations, commercial, direction) couvrant MiCA, PSAN, AML/KYC, RGPD, en développant des supports pédagogiques engageants (e-learning, cas pratiques, quiz) avec formats accessibles, en organisant des sessions de sensibilisation régulières aux évolutions réglementaires, en créant une base de connaissances conformité avec FAQ, procédures, modèles de documents, en instaurant une culture de conformité avec responsabilisation de chacun et processus d'escalation clairs, en mesurant l'efficacité des formations avec évaluations des connaissances et indicateurs de conformité.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle Réelle/ Reconstituée - Travail individuel ou en Binôme - À partir d'un projet blockchain réel, le candidat réalise une évaluation de conformité complète (MiCA, PSAN, AML/KYC, RGPD), élabore le plan de mise en conformité, implémente les processus KYC/AML, réalise une analyse d'impact RSE et produit les livrables réglementaires avec outils accessibles RGAA 4.1.

Livrables à produire :

Rapport de conformité réglementaire avec gap analysis MiCA/PSAN, plan de remédiation priorisé et procédures KYC/AML opérationnelles (vérification d'identité eIDAS, screening sanctions OFAC/UE/ONU, classification des clients PEP, monitoring des transactions et déclarations TRACFIN) (C5.1 + C5.2)

Analyse d'impact RGPD (DPIA) avec mesures de privacy by design, mécanismes de pseudonymisation et chiffrement adaptés à l'immutabilité blockchain, registre des traitements et procédures de respect des droits des personnes (C5.3)

Rapport de conseil stratégique avec analyse des opportunités blockchain, évaluation des risques, calculs ROI/NPV, roadmap stratégique et dashboards de décision accessibles RGAA 4.1 niveau AA (C5.4)

Rapport d'impact RSE avec évaluation environnementale chiffrée (consommation énergétique, empreinte carbone, comparaison PoS/PoW/DPoS), analyse sociale, analyse éthique et alignement avec les ODD (C5.5)

Dispositif de gouvernance opérationnelle de la conformité avec documentation audit-ready, plan de représentation auprès des régulateurs (ACPR/AMF/CNIL), programmes de formation par rôle et base de connaissances conformité (C5.6 + C5.7)

Déroulement de la soutenance :

Phase 1 – Présentation par le candidat - Le candidat présente son travail de conformité : évaluation de conformité réalisée avec gap analysis détaillée (MiCA, PSAN, AML/KYC, RGPD), plan de remédiation priorisé avec actions concrètes et échéancier, processus KYC/AML implémentés avec outils de screening et monitoring, analyse DPIA (Data Protection Impact Assessment) pour le RGPD, conseil stratégique avec analyse coûts-bénéfices et ROI, évaluation d'impact RSE avec mesures environnementales et sociales, outils accessibles RGAA 4.1 développés (dashboards conformité et conseil).

Phase 2 – Échanges collectifs avec le jury - Questions collectives pour approfondir : exhaustivité de l'évaluation de conformité et pertinence du gap analysis, applicabilité du plan de remédiation et réalisme des échéances, efficacité des processus KYC/AML avec pertinence des règles de détection, conformité RGPD avec respect des droits des personnes malgré l'immuabilité blockchain, qualité du conseil stratégique et robustesse de l'analyse RSE.

Phase 3 – Entretien technique approfondi - Questions individuelles : maîtrise approfondie des cadres réglementaires MiCA, PSAN, AML/KYC, RGPD avec capacité à interpréter les textes, compréhension des enjeux de coordination avec les régulateurs (ACPR, AMF, CNIL), expertise sur les techniques de privacy by design et pseudonymisation blockchain, analyse critique de l'impact sociétal et environnemental des solutions blockchain, capacité à représenter l'organisation lors d'audits réglementaires.

Phase 4 – Délibération du jury hors présence du candidat, il évalue les livrables selon critères, attribue la note et prépare le retour.

Jury de soutenance (3 personnes minimum) : Professionnel en conformité réglementaire blockchain et crypto-actifs (expérience MiCA, PSAN) - Juriste spécialisé fintech/blockchain ou Compliance Officer certifié (CAMS/ACAMS) - Représentant de l'organisme certificateur (président). Au moins 2 membres externes, aucun formateur du candidat.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le métier d'Expert en Sécurité, Stratégie et Conformité Blockchain s'exerce principalement dans les secteurs suivants : Services du numérique et conseil (ESN, cabinets de conseil en cybersécurité et blockchain) - Finance, banque, assurance et fintech (crypto-actifs, DeFi, paiements, gestion d'actifs) - Éditeurs et intégrateurs de solutions blockchain / Web3 - Industrie et grands groupes (énergie, logistique, supply chain, industrie 4.0) - Secteur public et parapublic (administrations, collectivités, institutions) - Cabinets d'audit et de cybersécurité - Startups et scale-ups technologiques

TYPE D'EMPLOIS ACCESSIBLES

Expert en Sécurité Blockchain - Architecte Solutions Blockchain et Cloud - Auditeur de solutions Blockchain - Expert Conformité CASP (Prestataire Services Crypto-Actifs) - Consultant Blockchain - Data Analyst Forensique Blockchain - Expert Cryptographie et Sécurité Blockchain - Consultant Innovation Blockchain

RÉGLEMENTATIONS D'ACTIVITÉ

Néant

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)	Très élevée (5/5) 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)	2 942 €

Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	32 216
Jugés difficiles à recruter	51 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

L'accès à la certification est ouvert selon le niveau du candidat, avec des durées de formation adaptées :

Accès avec un niveau 4 - Le candidat titulaire d'un niveau 4 accède à une formation sur 5 ans

Accès avec un niveau 4 + crédits - Le candidat titulaire d'une certification de niveau 4 disposant de crédits supplémentaires accède à une formation sur 4 ans

Accès avec un niveau 5 : Le candidat titulaire d'une certification de niveau 5 en informatique accède à une formation sur 3 ans

Accès avec un niveau 6 : Le candidat titulaire d'une certification de niveau 6 en informatique, développement, cybersécurité ou blockchain accède à une formation sur 2 ans

Accès dérogatoire par expérience professionnelle : les candidats ne disposant pas des niveaux requis peuvent accéder à la formation s'ils justifient d'au moins 3 ans d'expérience professionnelle en développement blockchain, smart contracts ou cybersécurité applicative, d'un dossier de VAPP validé par le certificateur attestant d'une expérience équivalente en développement informatique et/ou cybersécurité. L'admission est prononcée après examen du dossier et entretien individuel. Selon les process des écoles partenaires, des épreuves écrites ou orales peuvent être également organisées. Sont généralement demandés : une lettre de motivation, un test de connaissances techniques (développement, blockchain, cybersécurité), et un entretien professionnel qui permet d'évaluer les aptitudes professionnelles et techniques du candidat pour l'exercice du métier visé par la certification

Dans le cadre de la VAE : aucun prérequis dès lors que la faisabilité est validée et que la recevabilité est transmise au candidat.

S'agissant des candidats souhaitant préparer un ou plusieurs blocs de compétences, les prérequis à la validation des blocs de compétences sont les mêmes que ceux exigés pour la préparation complète du titre.

PRÉREQUIS À LA VALIDATION

Valider l'ensemble des blocs de compétences, ainsi que l'épreuve complémentaire consistant en la soutenance d'un mémoire professionnel.

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

Les membres du jury sont à 80% des professionnels, membres extérieurs à l'autorité délivrant la certification, non intervenants dans l'établissement, choisis et désignés par le certificateur en fonction de leur expérience, domaines de compétences et aptitudes particulières à l'évaluation.

Ils sont au nombre minimum de 5 dont le président(e), professionnel extérieur à l'établissement, désigné par l'ensemble des membres du jury, le responsable de programme concerné, le responsable des programmes certifiés. Ces derniers ou au moins l'un d'entre eux font toujours partie du jury de certification.

Parmi les professionnels est respectée une répartition à 50% de représentants des salariés et à 50% de représentants d'employeurs.

Base légale

Date de décision	26/06/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	26/06/2029
Date de dernière délivrance possible	26/06/2033

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42467/>