L'attribution du titre RNCP s'obtient par la validation de l'ensemble des blocs de compétences ci-dessous et la validation de la thèse professionnelle.

Cette thèse constitue l'étape ultime d'évaluation du participant selon les critères de rigueur scientifique, de pertinence sectorielle et d'utilisabilité pour l'entreprise à laquelle elle se réfère. Elle est une modalité d'évaluation globale et transversale du cursus et fait la synthèse de toutes les compétences acquises, qu'elles soient d'ordre stratégique ou opérationnel. Elle démontre l'aptitude du / de la candidat(e) à exposer et analyser par écrit la problématique retenue et à la présenter de façon claire et convaincante à l'oral devant un jury. La validation de la thèse professionnelle est indispensable pour obtenir la certification.

BLOCS	COMPETENCES
1. Réaliser l'architecture cybersécurisée d'un réseau télécom ou d'un système d'information	C1-C7
2. Piloter et réaliser un projet de développement de la cybersécurité dans le domaine des réseaux ou des systèmes d'information	C8-C11
3. Gérer la gouvernance de la sécurité des réseaux et des systèmes d'information	C12-C15
4. Sécuriser, protéger et défendre un réseau ou un système d'information	C16-C19

Référentiel d'activités	Référentiel de compétences	Référentiel d'évaluation	
		Modalités d'évaluation	Critères d'évaluation
1. Analyse du besoin de l'entreprise ou de son client en termes de conception ou d'évolution sécurisée du SI ou du réseau -Traduction du besoin en cahier des charges -Analyse de la réponse technique d'un appel d'offre -Appui sur des solutions existantes	C1. Analyser le besoin de l'entreprise ou de son client en termes de réseau ou de système d'information sécurisé, en tenant compte de l'existant et en transposant le cahier des charges en exigences de réalisation, afin de déterminer une solution cible.	**E1. Etude de cas (C1 à C4)** *Domaine des réseaux télécoms : document technique* A partir d'un cahier des charges donné, le candidat élabore un document technique (architecture HLD[1]) pour un réseau cible. Production individuelle sur table.	**Pour E1, E2 et E3** : Analyse qualitative du besoin : La formalisation des objectifs fait apparaitre la prise en compte de la problématique. L'architecture proposée est clairement expliquée en mettant en avant la sécurisation des échanges, notamment en prenant en compte par exemple la segmentation des réseaux, les protocoles de sécurité adaptés. **Pour E2 et E3 :** Pertinence des réponses aux questions : La problématique et le besoin sont compris, Les aspects techniques de la solution sont justifiés. **Pour E2 :** Des hypothèses sont formulées pour spécifier les modalités du problème.

[1] Architecture HLD (high level design) = La conception de haut niveau explique l'architecture qui serait utilisée pour développer un système. Le diagramme d'architecture donne une vue d'ensemble d'un système complet, identifiant les principaux composants qui seraient développés pour le produit et leurs interfaces.

-Caractérisation des éléments ou des fonctions du réseau, du SI ou du système de communication -Identification des besoins matériels -Prise en compte des besoins en cybersécurité -Echange avec les décisionnaires (client, direction générale...)	C2. Agréger l'ensemble des facteurs externes susceptibles d'influencer la conception ou l'évolution du système ou du réseau, en identifiant les enjeux d'analyse de risque, de réglementation, de technologies, d'infrastructures, de capacités, de qualité de service, d'utilisateurs et de sécurité, afin de détailler la solution cible et son évolution.	**E2. Mise en situation professionnelle dans le domaine des systèmes d'information (C1 à C5)** *Domaine des SI : projet de transformation de SI (fusion des deux systèmes d'information, acquisition de société, passage au cloud, suppression...)* Ce projet est présenté en Direction Générale pour approbation. Un rôle fonctionnel est attribué à chaque candidat membre du groupe projet. A partir des éléments d'un scénario, le candidat émet des hypothèses pour traiter le projet. Projet collectif soutenu devant un jury. Notation individuelle.	**Pour E1, E2 et E3 :** Réponse au problème posé : Les facteurs externes pertinents au regard du contexte sont analysés (analyse de risque, prise en compte de la réglementation, des technologies et infrastructures existantes...). Ces facteurs sont pris en compte dans l'élaboration de la solution.
2. Elaboration d'une architecture fonctionnelle répondant au besoin -Prise en compte des besoins des directions métiers de l'entreprise dans l'architecture du SI	C3. Traduire le besoin en termes d'architecture fonctionnelle du réseau télécom ou du système d'information, en tenant compte de l'existant, des contraintes de l'entreprise, des défaillances à corriger, en identifiant et caractérisant les éléments et fonctions du système afin de créer une architecture adaptée à l'organisation.	**E3. Mise en situation professionnelle (C1 à C7)** *Réponse à Appel d'offre dans le domaine de la sécurité* Le contexte de la demande est présenté aux candidats sous la forme d'un cahier des charges. A partir d'un	**Pour E2:** Analyse correcte des éléments structurants donnés dans le projet : Les contraintes et opportunités engendrées par la transformation du SI sont exposées selon les différents domaines fonctionnels affectés.

-Document d'architecture technique (HLD) -Proposition d'évolution des composants technologiques de l'architecture réseau télécom ou système d'information -Définition des solutions techniques à mettre en place -Identification de scénarios d'évolution	C4. Transposer l'architecture fonctionnelle en spécifications de réalisations techniques et déterminer les composants d'architecture du réseau ou du système d'information, les équipements matériels et logiciels, les outils supports afin de répondre aux spécifications.	cahier des charges, il s'agit de proposer une architecture de sécurité adaptée et couvrant le besoin de protection des informations et des échanges internes et externes des collaborateurs de l'entreprise. La réponse à l'appel d'offre sous la forme d'un livrable doit comporter : la présentation de la société, la formalisation des objectifs, la réponse au cahier des charges sur les aspects techniques d'architecture réseaux et éléments de sécurité, et financiers au travers des éléments matériels et logiciels nécessaires. Une séance de questions/ réponses se déroule après la présentation de l'offre. Soutenance orale en groupe devant un jury. Notation individuelle.	**Pour E2 :** Transposition effective de l'architecture fonctionnelle en architecture opérationnelle, prenant en compte les domaines du SI et les différences de traitement.
	C5. Anticiper les évolutions du système en prenant en compte sa croissance, en s'appuyant sur de nouvelles technologies identifiées au cours d'une veille continue et en s'assurant que le système reste aligné avec la stratégie d'entreprise, afin de garantir la pérennité du système.		**Pour E2 et E3 :** Des projections de croissance du système sont proposées en phase avec les objectifs de l'organisation. Les technologies proposées sont en adéquation avec les besoins du système.
3. Ingénierie sécurisée des éléments du réseau ou du système d'information -Mise en place de solutions d'architectures sécurisées adaptées au système cible -Rédaction du document d'ingénierie général et détaillé du SI / réseau pour chaque élément -Rédaction des protocoles utilisés, règles de dimensionnement et de mise en œuvre -Plan de sécurité du SI ou du réseau	C6. Concevoir l'ingénierie sécurisée des éléments du réseau télécom, en spécifiant pour chaque élément à implémenter ses fonctionnalités, les protocoles utilisés, les règles de dimensionnement et de mise en œuvre, afin de pouvoir déployer la solution.		**Pour E3 :** A propos de l'ingénierie sécurisée : les fonctionnalités, protocoles utilisés, règles de dimensionnement et de mise en œuvre de la solution sont exposées de manière exhaustive.
	C7. Intégrer les aspects de sécurité dans l'architecture et dans les éléments du système d'information ou du réseau, en définissant l'architecture adéquate et en proposant des choix de technologies, afin de le sécuriser.		**Pour E3 :** Les aspects de sécurité dans l'architecture sont intégrés au projet. Les technologies de sécurisation du système proposées sont en adéquation avec le besoin

<table>
<tr>
<td rowspan="2">4. Gestion de projet ou de services dans les réseaux ou les systèmes d’information
-Sélection de la méthode de gestion de projet adaptée
-Analyse des risques du projet
-Suivi du projet : vérification de la conformité du projet au cahier des charges, rédaction de compte-rendu de suivi et d'avancement.

-Tableaux de bord
-Contrôle de l'atteinte de l'objectif
-Mesure des résultats au regard du cahier des charges</td>
<td>C8. Piloter un projet de développement de la cybersécurité du domaine des réseaux télécom ou du SI, en sélectionnant la méthode adaptée au projet concerné, en s'assurant de sa conformité au cahier des charges et en rédigeant des comptes rendus de suivi et d'avancement, afin de garantir que la mise en œuvre du projet réponde bien aux besoins identifiés.</td>
<td rowspan="2">E4 Mise en situation professionnelle (C8 à C11)

Projet collectif fil rouge

A partir d'un domaine du numérique (réseaux, cybersécurité…) croisé à des enjeux de société, le candidat met en application la gestion de projet. Il doit sélectionner en équipe un projet à forte valeur ajoutée en lien avec le domaine retenu (ex : politique des smart cities, innovation technologique...) et trouver des financements, en effectuant notamment une planification du projet, en dressant des KPI, une analyse SWOT, une analyse de risque et un plan de remédiation des risques.

Projet collectif. Soutenance orale devant un jury. Notation individuelle.</td>
<td>Pour E4 :
A propos du pilotage de projet :
le document de soutenance et l’argumentaire lors de la soutenance mettent en avant l'analyse des contraintes du projet (pratiques, techniques et humaines).</td>
</tr>
<tr>
<td>C9. Réaliser le plan de gestion du projet, en ordonnançant les tâches, en dressant une cartographie réaliste des risques et des palliatifs, en déterminant les éléments de coût-délai-qualité, afin de faciliter la mobilisation des acteurs tout au long du projet.</td>
<td>A propos du plan de gestion :
la planification est présentée selon un découpage en phases prenant en compte les contraintes du projet.
Des indicateurs de performance clé sont définis et pertinents au regard de la complexité du projet.
Une estimation des coûts et ressources est présentée et sa dimension réaliste est argumentée au moment de la soutenance.
Une analyse des risques du projet est réalisée de façon approfondie (exhaustivité des domaines concernés, classification en fonction de la gravité) et s'accompagne d'un plan de mitigation de risque (propositions d'action de remédiation cohérentes avec les risques soulevés).</td>
</tr>
</table>

5. Management d'équipe projet -Coordination des étapes et des partenaires du projet (internes, externes, nationaux et internationaux) -Plan de recrutement -Communication auprès des parties prenantes du projet -Animation et mobilisation -Prise en compte des situations de handicap	C10. Elaborer un plan de recrutement de l'équipe projet, en tenant compte des compétences nécessaires, en s'appuyant sur les enjeux, les produits à livrer, les contraintes de coût, délai et qualité identifiés, afin d'appuyer la réalisation du projet.		A propos du plan de recrutement : le contexte, les objectifs et les enjeux du projet sont intégrés dans la justification du plan de recrutement. La matrice RACI[2] est utilisée. Les organigrammes techniques du projet (RH et produits) sont élaborés afin d'appuyer sa réalisation.
	C11. Communiquer auprès des parties prenantes du projet, y compris en situation de handicap, en utilisant le support adéquat, en argumentant sur les enjeux du projet, afin de mobiliser les acteurs pour atteindre les objectifs du projet.		Discours pertinent : Il est adapté au public (direction générale, client...) Les situations de handicap sont prises en compte. Clarté du support, du discours et des réponses aux questions. Le ton et le discours employés font ressortir une attitude professionnelle : posture, argumentaire, syntaxe respectée. Les facteurs-clés de succès du projet sont mis en avant lors de la soutenance. L'argumentation sur le projet est étayée et le déroulé de la présentation suscitent de la motivation et de l'enthousiasme pour le projet.

[2] Matrice RACI (*Responsibility Accountability Consult Inform*) = l'acronyme RACI ou RAM désigne dans le domaine du management une matrice des responsabilités. Elle indique les rôles et les responsabilités des intervenants au sein de chaque processus et activité.

6. Analyse des besoins en cybersécurité -Analyse du contexte sécuritaire -Définition du périmètre de sécurité retenu -Analyse de risque -Qualification et analyse des causes de dysfonctionnement -Identification des failles de sécurité -Identification et priorisation des risques -Préconisation des mesures correctives	C12. Définir le périmètre de sécurité du système en s'appuyant sur des normes et/ou des méthodes de référence afin de recenser les éléments (biens supports, réseaux, informations, personnes ...) à retenir du système.	**E5 Etude de cas (C12 et C13)** Analyse de risque en sécurité de l'information permettant notamment de traiter les menaces de type APT[3], en utilisant la méthode EBIOS Risk Manager[4] A partir d'un contexte classique de cybersécurité pour une entreprise, le candidat prenant le rôle de RSI (Responsable de la sécurité de l'information). Il doit appliquer la méthode EBIOS RM (découpée en ateliers) pour analyser les risques en identifiant les sources de menaces et les objectifs visés. Il doit aussi élaborer les scénarios qui en découlent. Travail collectif. Livrable sous la forme d'un document. Notation individuelle.	**Pour E5 :** La constitution du socle de sécurité (atelier 1 de la méthode EBIOS RM) montre des choix pertinents des référentiels et des mesures de sécurité par rapport au contexte. L'ensemble des éléments à retenir du système est recensé.
	C13. Réaliser une analyse de risque en sécurité en utilisant une méthode appropriée afin d'identifier les principaux risques ou failles de sécurité du système et proposer un traitement des risques.		**Pour E5 :** Les 5 ateliers sont décrits de façon individualisée dans le respect de la méthode utilisée (EBIOS RM). Les principaux risques ou failles de sécurité du système sont identifiés. L'élaboration des scénarios stratégiques (chemins d'attaque) et opérationnels (modes opératoires) (ateliers 3 et 4) montre un enchainement satisfaisant et une pertinence de déclinaison du scénario stratégique en scénario opérationnel. Le déroulement de la méthode conduit au traitement des risques (atelier 5).

[3] APT (Advanced Persistent Threat) = type de piratage informatique furtif et continu, ciblant une entité spécifique.
[4] EBIOS RM = EBIOS RM permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser. Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue.

7. Elaboration d'une politique de sécurité de l'information -Définition des objectifs de sécurité, de type mise en place d'actions permettant de prévenir / réduire les risques, mise en place d'outils de réduction des risques (vérification...), mise en place d'un CERT[5] (*computer emergency response team*) -Participation à l'écriture de la PSSI[6] de l'entreprise (budgets attribués) - Formation / sensibilisation des acteurs aux outils -Respect et application des normes et règlements de sécurité (ex : mise en place du RGPD)	C14. Proposer des éléments prioritaires devant faire l'objet d'une protection de nature organisationnelle ou technique à partir d'éléments issus d'analyse de risque, de documents d'architecture du système, d'objectifs de sécurité déjà existants ou recensés, afin de participer à l'élaboration ou à l'évolution de la politique de sécurité de l'information de l'organisme.	**E6 Etude de cas (C14 et C15)** *Participation à l'élaboration de la politique de sécurité d'une entreprise existante* Le candidat, à partir de documents définissant le contexte de l'entreprise (domaine d'activités, information sensible, enjeux, description globale de l'architecture du SI) élabore une politique de sécurité et définit le SMSI[7] associé. Livrable sous la forme d'un document élaboré en groupe. Notation individuelle.	Pour E6 : A propos de la politique de sécurité : le document fournit la définition du périmètre, des éléments stratégiques et l'organisation de la sécurité (au plan organisationnel et technique) Les priorités proposées sont cohérentes au regard des objectifs du SMSI.
	C15. Recueillir les incidents de sécurité, en s'appuyant sur l'analyse de risque, un SOC[8] ou au travers d'un CERT, pour organiser de manière technique les mesures de sécurité face à une cyberattaque du système.		Pour E6 : La politique de sécurité prend en compte l'analyse de risque. Les incidents de sécurité rapportés sont analysés et cette analyse permet de justifier les mesures de sécurité proposées.

[5] CERT = Un computer emergency response team ou computer security incident response team est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous

[6] PSSI = La politique de sécurité des systèmes d'information est un plan d'action défini pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information.

[7] SMSI = Un SMSI est un système de management permettant de définir des actions (techniques, organisationnelles) pour atteindre un objectif fixé. Ce modèle contribue à la gestion de la sécurité au sein de l'organisation, tout en atténuant les risques, en particulier sur la thématique de la sécurité de l'information.

[8] SOC = Un Security Operations Center ou centre des opérations de sécurité est une division, dans une entreprise, qui assure la sécurité de l'organisation et surtout le volet sécurité de l'information.

8. Configuration de la protection du SI ou du réseau -Amélioration de la sécurité des éléments du système -Concept de *zéro trust* (confiance zéro) : vérification des autorisations des accès aux données (volet IAM[9]) -Prise en compte de la sécurité physique et environnementale -Mise en place d'un système de journalisation (SOC) pour comprendre le cheminement d'une attaque et évaluer son impact -Identification d'éléments techniques de sécurité ou d'outils de collecte et d'analyse de type EDR[10], de solutions de sécurisation, détection, protection contre les intrusions, traçabilité	C16. Identifier les éléments techniques de sécurité ou les outils à mettre en œuvre, en couvrant la mise en place de solutions de sécurisation des communications (protocoles de sécurité, chiffrement, certificats), segmentation de réseau et cloisonnement, dispositif de filtrage, solution de détection et de protection contre les intrusions sur le réseau et les terminaux (IPS, IDS), l'identification l'authentification forte et le contrôle d'accès, la traçabilité en temps réel ou en temps différé de l'ensemble des activités, la sécurité physique et les outils de contrôle, afin d'améliorer la sécurité des systèmes et des réseaux.	**E7 Etude de cas (C16 et C17)** *Configuration de la protection du SI* Sur la base d'un document présentant la demande de sécurisation du SI d'une entreprise, accompagnée d'une analyse de risque montrant les sources de menace auxquelles l'entreprise doit faire face, le candidat identifie les mesures de sécurité afin de réduire les menaces. Il traduit les mesures de sécurité sous la forme de solutions de sécurisation du système de défense du SI et de ses composants. Production écrite individuelle.	**Pour E7 :** Les éléments techniques de sécurité répondent à la demande de sécurisation du SI. Des solutions pratiques de sécurité sont proposées en adéquation avec la demande, de type sécurisation du système, segmentation de réseau, dispositif de filtrage…
	C17. Analyser le ou les outils du marché le(s) mieux adapté(s) à la protection du SI ou du réseau, en les comparant selon différents critères liés aux contraintes et demandes de l'entreprise (coût, technique, souveraineté), afin d'aider à la prise de décision.		**Pour E7 :** Les solutions proposées prennent en compte les outils disponibles sur le marché. Le choix des outils est justifié au regard des critères techniques et des enjeux de souveraineté.

[9] IAM = « Identity and Access Management », ensemble de mesures permettant la protection des données, notamment sur les infrastructures critiques. Elles répondent notamment à 4 règles : identification, authentification, droits d'accès et comptes d'administration.

[10] EDR = Détection et réponse des terminaux (EDR) est une solution de sécurité des terminaux qui inclut la surveillance en temps réel et la collecte des données de sécurité des terminaux avec un mécanisme de réponse automatisée aux menaces.

9. Traitement des incidents de sécurité -Détection des anomalies de sécurité : choix des outils -Gestion de la continuité du réseau / SI : mise en œuvre d'un plan de continuité -Passage en crise / forensique	C18. Détecter, classifier les incidents et les gérer, en mobilisant les outils adaptés de surveillance afin d'anticiper ou de réagir à une cyberattaque du système.	**E8 Etude de cas (C18 et C19)** : *Elaboration d'une politique de continuité et de gestion de crise* Une entreprise doit élaborer une politique de continuité et de gestion de crise afin de pouvoir faire face à une cyberattaque. Le contexte est fourni au candidat. Celui-ci, prenant le rôle du RSI, doit élaborer un document de référence en la matière. Production écrite individuelle.	**Pour E8 :** A propos de la gestion des incidents : le document identifie et classifie les incidents potentiels. Il recense également les outils adaptés de surveillance.
	C19. Etablir un plan de continuité et de reprise d'activités, en définissant les processus et en identifiant les ressources techniques et humaines ainsi que les compétences mobilisables, afin de rétablir le bon fonctionnement du système.		**Pour E8 :** A propos du plan de continuité: le document contient des éléments d'organisation de la continuité (niveau de performance accepté, redondance, …) et de décision de passage en crise (seuil de décision)