Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 1 : Analyse stratégique des cyber-risques	*<u>Contexte</u> : Le manager de la cyber sécurité situe son action dans le contexte international des menaces criminelles sur les systèmes d'information, dans le but de protéger les infrastructures et les données de son entreprise.*	E2 : Travaux écrits E3 : Etude de cas E4 : Mise en situation professionnelle E5 : Présentation orale devant le jury	*Aux critères objectifs listés ci-dessous s'ajoute l'appréciation des « soft skills » lors des mises en situation professionnelle et des épreuves orales devant le jury.*
A1. Veille géopolitique sur les cyber-menaces et la cybercriminalité • Repérage des sources • Organisation de la veille • Cartographie	C1. Analyser une situation géopolitique propice à la cyberguerre, en recensant les cyberattaques passées, dans le but de cartographier les menaces potentielles sur les systèmes d'information d'un pays ou d'une industrie.	E2 – E3 (C1) <u>Etude de cas donnant lieu à une note de synthèse écrite remise au jury.</u> Exemple d'un pays balte.	• (C1) Qualité de l'analyse géopolitique - *La méthodologie d'analyse est correcte et structurée* - *Les incidents passés sont classés par catégories et niveaux de gravité* - *Les menaces potentielles sont identifiées et leurs niveaux d'occurrence estimés* - *Les conclusions de l'étude sont claires et pertinentes*
A2. Identification des risques d'intrusion dans les systèmes d'information de l'entreprise • Audit des systèmes d'information • Analyse des risques cyber	C2. Conduire un audit du système d'information et des réseaux de son entreprise, afin d'identifier leurs points de vulnérabilité au regard des menaces d'intrusion inhérentes au cyberespace.	E2 – E4 – E5 (C2 à C4) <u>Mise en situation professionnelle à l'occasion du stage</u> Le candidat mène une analyse exhaustive des cyber-risques et menaces sur l'entreprise qui l'accueille en stage. Rapport écrit remis au jury et présentation orale à celui-ci.	• (C2) Précision de l'analyse des risques et menaces sur l'entreprise - *La méthodologie de conduite de l'audit est correcte et justifiée* - *Les vulnérabilités du système d'information sont identifiées et précisément décrites* - *Les conclusions de l'analyse sont clairement présentées* - *Les réponses aux questions du jury sont pertinentes*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A3. Analyse des risques affectant les données numériques • Analyse des risques de captation ou de dommages aux données • Travaux préparatoires à l'élaboration du cahier des charges de la cyber sécurité • Conformation aux normes internationales	C3. Dresser un état des dommages potentiels devant résulter des attaques au système d'information de son entreprise, en caractérisant les atteintes possibles aux données numériques (altération, captation ou destruction) traitées ou stockées par celui-ci, en vue d'établir un cahier des charges de la cyber sécurité. C4. Se conformer à la norme ISO 27032, dans le cadre du budget disponible, afin de répondre aux impératifs de protection de l'activité et des données.	E2 – E4 – E5 (C2 à C4) <u>Mise en situation professionnelle à l'occasion du stage</u> Le candidat mène une analyse exhaustive des cyber-risques et menaces sur l'entreprise qui l'accueille en stage. Rapport écrit remis au jury et présentation orale à celui-ci.	• Précision de l'analyse des menaces sur les données (C3) - *La méthodologie d'analyse est correcte et structurée* - *Les risques de dommages aux données sont identifiés et précisément décrits* - *Les menaces sont caractérisées* (C4) - *La norme ISO 27032 est connue et mise en œuvre* - *Les conclusions de l'analyse sont clairement présentées* - *Les réponses aux questions du jury sont pertinentes*
A4. Mise en œuvre de l'intelligence économique • Collecte de données • Analyse de la concurrence	C5. Organiser la surveillance de l'environnement concurrentiel de son entreprise, en collectant les informations économiques et stratégiques utiles, afin d'anticiper sur les intentions des concurrents sur le marché national et international.	E2 – E3 (C5) <u>Etude de cas donnant lieu à une note de synthèse écrite remise au jury.</u> Etude sur la situation concurrentielle de l'entreprise d'accueil.	• (C5) : Connaissance des méthodes de l'intelligence économique - *La méthodologie de collecte des données est explicitée et justifiée* - *Les critères d'analyse de la position concurrentielle de l'entreprise sont précisés* - *Les conclusions de l'analyse sont formulées en lien avec la stratégie commerciale de l'entreprise*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 2 : Conception et organisation de la sécurité des SI et des réseaux	*<u>Contexte</u> : Le manager de la cyber sécurité intervient dès la conception des systèmes d'information et des réseaux de son entreprise, afin d'intégrer tous les dispositifs nécessaires à la prévention des risques d'intrusion.*	E1 : Questionnaire E2 : Travaux écrits E4 : Mise en situation professionnelle E5 : Présentation orale devant le jury	*Aux critères objectifs listés ci-dessous s'ajoute l'appréciation des « soft skills » lors des mises en situation professionnelle et des épreuves orales devant le jury.*
A1. Conception d'une architecture de sécurité adaptée au niveau de risques • Elaboration du schéma général de la cyber sécurité • Choix d'un type d'architecture SI adapté aux attentes • Spécification technique de l'architecture SI et des solutions de cyber sécurité à mettre en place **A2. Conduite d'un appel d'offres sur les architectures et solutions de sécurité** • Rédaction du cahier des charges • Rédaction et conduite de l'appel d'offres	C6. Etablir le schéma général de la cyber sécurité dans son entreprise, en s'appuyant sur l'audit de vulnérabilité des systèmes d'information et des réseaux, afin de déterminer les caractéristiques d'une nouvelle architecture à mettre en place. C7. Traduire en spécifications techniques les attentes en matière d'architecture et de solutions de sécurité, en vue de la rédaction du cahier des charges d'un appel d'offres sur le marché des prestataires. C8. Coordonner la rédaction du cahier de charges et de l'appel d'offres, conformément au schéma général de la cyber sécurité préalablement établi, en vue de la sélection des prestataires et sous-traitants.	E2 - E4 – E5. (C6 à C10) <u>Mise en situation professionnelle à l'occasion du stage</u> Le candidat participe au lancement d'un appel d'offres sur les architectures et solutions de sécurité. Il analyse les attentes et contribue à la réalisation de l'appel d'offres, depuis la rédaction du cahier des charges jusqu'au choix des prestataires. Compte-rendu écrit intégré au rapport de stage et présentation orale au jury.	• Précision de l'analyse fonctionnelle (C6) - *Le candidat démontre sa connaissance des principes de l'architecture SI* - *Les caractéristiques de l'architecture à mettre en place au regard des impératifs de cyber sécurité sont identifiées* (C7) - *Les spécifications techniques des attentes sont précises et justifiées* - *Les conclusions sont clairement présentées* - *Les réponses aux questions du jury sont pertinentes* • (C8) Compréhension des mécanismes de l'appel d'offres - *Le cahier de charges et les documents de l'appel d'offres sont complets* - *Le candidat rend compte précisément des rôles des parties prenantes dans la rédaction*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A3. Choix des prestataires en cyber sécurité • Analyse de la solidité financière des prestataires • Choix des solutions optimales à l'issue de l'appel d'offres	C9. Analyser la situation économique et financière des répondants à l'appel d'offres, afin d'assurer la viabilité à long terme des solutions retenues. C10. Choisir une prestation de cyber sécurité, dans le respect du budget imparti et du cahier des charges, afin d'optimiser la couverture des risques.	E2 - E4 – E5. (C6 à C10) <u>Mise en situation professionnelle à l'occasion du stage</u> Le candidat participe au lancement d'un appel d'offres sur les architectures et solutions de sécurité (suite). Compte-rendu écrit intégré au rapport de stage et présentation orale au jury.	• Maîtrise des mécanismes de l'appel d'offres (C9) - *La méthodologie d'analyse des situations financières des répondants est explicite et justifiée* - *Les critères retenus sont justifiés* - *Les résultats de l'analyse sont présentés et argumentés* (C10) - *Les réponses sont classées au regard des attentes et budgets impartis au titre du cahier des charges* - *La présentation orale est claire et structurée.* - *Les réponses aux questions du jury sont argumentées.*
A4. Veille réglementaire • Organisation d'un dispositif de veille réglementaire générale • Suivi et mise en œuvre de l'actualité de la réglementation et des recommandations des organismes spécialisés	C11. Concevoir et utiliser un système de veille sur l'actualité des contraintes légales et réglementaires, à l'aide des outils numériques de recherche sur les sites des organismes spécialisés en matière de cyber sécurité et les bases de données juridiques du domaine, afin d'assurer la conformité légale des dispositifs de sécurité mis en place.	E1 (C11) <u>Questionnaire général écrit sur la réglementation en matière de cyber sécurité</u> Le candidat répond à un questionnaire juridique détaillé sur l'ensemble des contraintes légales et réglementaires.	• (C11) 70% de bonnes réponses au questionnaire

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 3 : Déploiement de la sécurité des SI et des réseaux	*<u>Contexte</u> : Après la phase de conception, le manager de la cyber sécurité coordonne la mise en place de tous les dispositifs de protection choisis pour les infrastructures et les données, dans le but d'assurer la continuité de l'activité en toutes circonstances.*	E2 : Travaux écrits E4 : Mise en situation professionnelle E5 : Présentation orale devant le jury	*Aux critères objectifs listés ci-dessous s'ajoute l'appréciation des « soft skills » lors des mises en situation professionnelle et des épreuves orales devant le jury.*
A1. Sécurisation des réseaux et des services • Mise en place des pare-feux et alertes sur les réseaux • Installation des backups **A2. Protection des données et du patrimoine immatériel de l'entreprise** • Protection des dispositifs de stockage • Cryptage des données	C12. Identifier les emplacements des pares-feux et alertes les mieux adaptés à la prévention des intrusions, afin d'optimiser les temps de détection et de réponse. C13. Installer les dispositifs de remplacement des réseaux infectés, dans le but d'assurer la continuité des services aux utilisateurs. C14. Protéger l'accès aux espaces de stockage et aux données par des systèmes de codes d'accès et de cryptage adaptés aux menaces, afin d'assurer la conservation du patrimoine immatériel de l'entreprise.	E2 - E4 – E5. (C12 à C16) <u>Mise en situation professionnelle à l'occasion du stage</u> Le candidat est intégré à la direction des systèmes d'information de l'entreprise qui l'accueille en stage et participe à la mise en place de dispositifs de cyber sécurité. Compte-rendu écrit intégré au rapport de stage et présentation orale au jury.	• (C12, C13) Niveau de compétence technique - *Le candidat démontre sa maîtrise technique des solutions de sécurité* - *Le placement des pare-feux et des alertes est justifié* - *Les backups sont en place et justifiés* - *La continuité de service est assurée et démontrée* • (C14) Connaissance des principales techniques de protection des données - *La hiérarchie des codes d'accès est cohérente et adaptée tant aux menaces qu'à l'organisation de l'entreprise* - *Les principales techniques de cryptage des données et leur utilisation sont connues et correctement mises en oeuvre*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A3. Sécurisation des locaux et des infrastructures sensibles • Prévention des agressions physiques sur les locaux et infrastructures • Sécurisation des alimentations en énergie	C15. Identifier les risques d'atteinte aux infrastructures physiques en vue de placer les alertes et protections à même d'anticiper sur toutes tentatives d'intrusion dans les locaux. C16. Optimiser les solutions de fourniture d'énergie et les dispositifs de secours en cas de défaillance, afin d'assurer l'alimentation permanente des systèmes d'information et des réseaux de l'entreprise.	E2 - E4 – E5. (C12 à C16) <u>Mise en situation professionnelle à l'occasion du stage</u> Le candidat est intégré à la direction des systèmes d'information de l'entreprise qui l'accueille en stage et participe à la mise en place de dispositifs de cyber sécurité. Compte-rendu écrit intégré au rapport de stage et présentation orale au jury.	• Niveau de compétence technique en protection (C15) - *Le candidat a compris les impératifs de la sécurité des bâtiments et les liens ce celle-ci avec la cyber sécurité* - *Ses propositions sont pertinentes et justifiées* (C16) - *La question des sources d'énergie (alimentations électriques et autres sources) est présentée en détails et les solutions proposées sont justifiées*
A4. Mise en place de la sûreté de fonctionnement • Elaboration du schéma général de la sûreté de fonctionnement	C17. Etablir le schéma général de la sûreté de fonctionnement à l'intention des services internes à l'entreprise, en vue de garantir la continuité de l'activité quelles que soient les attaques sur le système d'information.	E2 (C17) <u>Rédaction du schéma général de la sécurité de fonctionnement</u> A l'issue de son stage, le candidat rédige une note présentant les différents aspects de la sûreté de fonctionnement de l'entreprise qui l'a accueilli. Note écrite remise au jury.	• (C17) Qualité du schéma général - *La notion de sûreté de fonctionnement est maîtrisée* - *Le schéma général de la sûreté de fonctionnement est exact et sa présentation adaptée aux publics internes* - *La présentation orale est claire et structurée.* - *Les réponses aux questions du jury sont argumentées.*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 4 : Management de la cyber sécurité dans l'entreprise	*Contexte* : *Le manager de la cyber sécurité est responsable de l'organisation générale de la cyber sécurité dans l'entreprise et de la formation des personnels aux impératifs de celle-ci. Il conduit le changement et anticipe sur la gestion des crises.*	E2 : Travaux écrits E4 : Mise en situation professionnelle E5 : Présentation orale devant le jury	*Aux critères objectifs listés ci-dessous s'ajoute l'appréciation des « soft skills » lors des mises en situation professionnelle et des épreuves orales devant le jury.*
A1. Elaboration du schéma organisationnel de la cyber sécurité • Exploitation des audits de risques • Analyse systémique • Répartition des responsabilités • Management d'équipes	C18. Sur la base des audits de risques cyber sur les systèmes et réseaux, les données et les infrastructures, conduire une analyse systémique de l'organisation de son entreprise en vue de répartir les responsabilités dans un organigramme général de la cyber sécurité.	E2 – E4 - E5. (C18, C19) Mise en situation professionnelle durant la période de stage Le candidat à la certification dresse l'organigramme de la cyber sécurité dans l'entreprise, à partir d'une analyse systémique de son organisation. Il décrit les responsabilités à chaque niveau de l'entreprise.	• (C18) Précision de l'analyse systémique - *La méthodologie de l'analyse systémique est comprise et mise en œuvre* - *Les responsabilités sont précisées pour chaque catégorie de personnel* - *Un organigramme est présenté en synthèse des observations*
A2. Formation et conseil aux services supports • Analyse des compétences • Elaboration de plan de formation	C19. Analyser les compétences du personnel de son entreprise en matière de cyber sécurité, au moyen de questionnaires et d'entretiens, en vue de concevoir et mettre en place un plan de formation des personnels et de conseil aux services supports.	Il recense et analyse les besoins de formation des personnels. Il rédige un rapport remis au jury et soutenu oralement devant celui-ci.	• (C19) Qualité d'élaboration du plan de formation - *Les besoins en compétences sont identifiés et décrits précisément* - *Le projet de plan de formation est cohérent et couvre l'ensemble des besoins* - *Le conseil aux services supports est en ligne avec le plan de formation* - *Le rapport écrit est complet et bien structuré* - *La présentation orale au jury est précise et argumentée*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A3. Inclusion handicap et multiculturalité • Analyse des situations de travail • Inclusion handicap • Prise en compte des différences culturelles • Conception universelle	C20. Prendre en compte le référentiel général d'amélioration de l'accessibilité (RGAA) et les recommandations de la norme internationale WCAG 2.1 (Web Content Accessibility Guidelines) à un niveau aaa, dans le but d'adapter le management interne de la cyber sécurité aux personnes handicapées. C.21 Prendre en compte la multiculturalité des personnels de son organisation, dans le but d'adapter le management interne de la cyber sécurité aux modes particuliers d'appréhension des directives.	E2 – E4 - E5. (C20 à C24) <u>Mise en situation professionnelle durant la période de stage</u> Le candidat participe à la mise en place (au perfectionnement) d'une organisation adaptée aux impératifs de la cyber sécurité dans l'entreprise qui l'accueille en stage. Il mène des projets avec méthode par une action auprès des collaborateurs concernés. Il contribue à la rédaction et à la diffusion de documents de communication à l'intention du personnel.	• (C20) Qualité du plan d'inclusion handicap - *Les situations de travail des personnes handicapées sont précisément décrites* - *La mise en œuvre du RGAA et des recommandations WCAG est conforme aux situations de travail étudiées* - *La notion de conception universelle est connue et judicieusement mise en œuvre* • (C21) Niveau de prise en compte des différences culturelles - *Les caractéristiques multiculturelles sont identifiées* - *Les mesures d'inclusion préconisées sont pertinentes et correctement justifiées*
A4. Conduite de projet et conduite du changement • Accompagnement • Résolution de problèmes • Management des équipes	C22. Utiliser une méthode de gestion de projet pour la mise en place d'une nouvelle organisation de la cyber sécurité dans l'entreprise. C23. Accompagner le changement nécessité par les dispositions locales et internationales en matière de cyber sécurité, au plus près des postes de travail, afin d'assurer le bon fonctionnement de l'organisation mise en place.	Compte-rendu écrit intégré au rapport de stage et présentation orale au jury.	• (C22, C23) Qualité de la gestion de projet - *Le candidat démontre qu'il maîtrise la méthodologie de la gestion de projet et de l'accompagnement* - *Les projets dont il est responsable sont décrits (objectifs, délais, personnels impliqués)* - *Les comptes-rendus d'étapes sont présentés et complets*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A5. Anticipation de la gestion des crises • Rédaction des contenus de communication • Diffusion aux responsables	C24. Concevoir et déployer dans l'entreprise une communication destinée à anticiper sur la gestion des crises occasionnées par les tentatives d'intrusion cyber.	E2 – E4 - E5. (C20 à C24) <u>Mise en situation professionnelle durant la période de stage</u> Le candidat participe à la mise en place (au perfectionnement) d'une organisation adaptée aux impératifs de la cyber sécurité dans l'entreprise qui l'accueille en stage. Il mène des projets avec méthode par une action auprès des collaborateurs concernés. Il contribue à la rédaction et à la diffusion de documents de communication à l'intention du personnel. Compte-rendu écrit intégré au rapport de stage et présentation orale au jury.	• (C24) Qualité de la communication - *Les objectifs de la communication interne sont précisés* - *Les recommandations sont cohérentes* - *Le candidat démontre de bonnes qualités de rédaction* - *La présentation orale au jury est claire et bien structurée* - *Les réponses aux questions du jury sont argumentées.*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 5 : Gestion budgétaire et financière	*Contexte* : *Le manager de la cyber sécurité est responsable de la prévision des investissements en cyber sécurité et du suivi budgétaire de la mise en place et de la maintenance des dispositifs ad hoc. Il accorde une attention particulière au suivi des sous-traitants.*	E2 : Travaux écrits E4 : Mise en situation professionnelle E5 : Présentation orale devant le jury	*Aux critères objectifs listés ci-dessous s'ajoute l'appréciation des « soft skills » lors des mises en situation professionnelle et des épreuves orales devant le jury.*
A1. Elaboration du budget prévisionnel et du plan de financement • Evaluation des investissements • Négociation et mise en place des solutions de financement • Construction du budget	C25. Estimer les investissements (coûts et calendrier), afin de déterminer les besoins de financement. C26. Négocier les conditions de financement en tenant compte des évolutions probables des technologies de la cyber sécurité, en vue de construire un budget fiable à moyen terme.	E2 – E4 - E5. (C25 à C29) Mise en situation professionnelle durant la période de stage Le candidat à la certification réalise l'étude financière d'un projet d'investissement en cyber sécurité de l'entreprise qui l'accueille en stage. Il estime le coût complet de l'investissement et étudie différentes solutions de financement. Il assure le suivi du budget de réalisation, le suivi et le contrôle des sous-traitants. Il rédige un rapport remis au jury et soutenu oralement devant celui-ci.	• (C25) Précision dans l'estimation de l'investissement - *La méthodologie d'évaluation de l'investissement est explicite et justifiée* - *Les aspects techniques, humains, économiques et financiers sont pris en compte* - *Les solutions de financement sont étudiées en relation avec la direction financière* • (C26) Maîtrise de la construction budgétaire - *Le candidat démontre sa capacité à identifier et négocier des conditions de financement* - *Il prend en compte les évolutions prévisibles de la cyber sécurité* - *La construction du budget est réaliste et prend en compte l'ensemble des données d'investissement et de fonctionnement*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A2. Contrôle de gestion et pilotage budgétaire • Choix des indicateurs • Gestion des tableaux de bord • Analyse des écarts et mise en place de mesures correctives	C27. Choisir des indicateurs de suivi budgétaire adaptés au contexte de la cyber sécurité, en vue de constituer les tableaux de bord de gestion conformes aux principes de son entreprise. C28. Analyser en continu les écarts budgétaires, afin de décider la mise en place des mesures correctives et d'assurer la réalisation des projets dans le cadre imparti.	E2 – E4 - E5. (C25 à C29) <u>Mise en situation professionnelle durant la période de stage</u> Le candidat à la certification réalise l'étude financière d'un projet d'investissement en cyber sécurité de l'entreprise qui l'accueille en stage. Il estime le coût complet de l'investissement et étudie différentes solutions de financement. Il assure le suivi du budget de réalisation, le suivi et le contrôle des sous-traitants. Il rédige un rapport remis au jury et soutenu oralement devant celui-ci.	• (C27) Qualité des tableaux de bord de suivi - *Le choix des indicateurs de pilotage est pertinent* - *Les tableaux de bord de gestion sont correctement structurés* - *Les principes du contrôle de gestion dans l'entreprise sont pris en compte* • (C28) Efficacité du pilotage budgétaire - *L'identification des écarts est réalisée en continu* - *L'analyse des écarts est précise et les explications fournies sont justifiées* - *Les mesures correctives proposées sont pertinentes*

Manager de la cyber sécurité – Niveau 7

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A3. Suivi et contrôle des sous-traitants • Suivi des contrats de sous-traitance • Surveillance des garanties	C29. Assurer le suivi des contrats de sous-traitance en vérifiant régulièrement la solidité des garanties financières, afin d'éviter les ruptures dans la fourniture et la maintenance des systèmes de sécurité mis en place.	E2 – E4 - E5. (C25 à C29) <u>Mise en situation professionnelle durant la période de stage</u> Le candidat à la certification réalise l'étude financière d'un projet d'investissement en cyber sécurité de l'entreprise qui l'accueille en stage. Il estime le coût complet de l'investissement et étudie différentes solutions de financement. Il assure le suivi du budget de réalisation, le suivi et le contrôle des sous-traitants. Il rédige un rapport remis au jury et soutenu oralement devant celui-ci.	• (C29) Qualité du suivi des contrats de sous-traitance - *Le candidat démontre sa capacité à suivre et contrôler régulièrement les contrats des prestataires, sur les plans techniques et financiers* - *Les comptes-rendus de suivi sont précis* - *Les difficultés rencontrées sont analysées* - *La présentation orale au jury est précise et argumentée*

MODALITES D'EVALUATION

E1 : Questionnaire
(Epreuve écrite en temps limité, questions ouvertes ou fermées)
E2 : Travaux écrits
(Notes de synthèse relatives aux études de cas, rapport de stage)
E3 : Etude de cas
(Les études de cas supports des évaluations sont proposées par les entreprises partenaires de l'ILV-IIM)
E4 : Mise en situation professionnelle
(Sur études de cas en centre de formation, ou sur le terrain durant le stage en entreprise)
E5 : Présentation orale devant le jury
(Présentation orale individuelle)

Les modalités d'évaluation (1/3 temps, assistance) peuvent être adaptées en fonction des situations des personnes handicapées (Charte handicap & accessibilité de l'Institut Léonard de Vinci).

BLOCS DE COMPETENCES

Les compétences évaluées sont réparties en cinq blocs :

1. Mener une analyse stratégique des risques cyber
2. Concevoir et organiser la sécurité des SI et des réseaux
3. Déployer la sécurité des SI et des réseaux
4. Manager la cyber sécurité dans l'entreprise
5. Gérer les aspects budgétaires et financiers de la cyber sécurité

La validation des cinq blocs de compétences est obligatoire pour l'obtention du titre.

La validation partielle d'un bloc n'est pas possible. La validation partielle de la certification est constituée des blocs dont la totalité des compétences à évaluer est reconnue.