5 – REFERENTIELS EXPERT(E) EN SECURITE DIGITALE -NIVEAU 7

Article L6113-1 En savoir plus sur cet article... Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V)

« *Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un* ***référentiel d'activités*** *qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un* ***référentiel de compétences*** *qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un* ***référentiel d'évaluation*** *qui définit les critères et les modalités d'évaluation des acquis.* »

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 N° 1 Prévenir et anticiper les menaces cyber pesant sur les systèmes d'information			
A1.1 **Analyse préventive des faiblesses et vulnérabilités des systèmes d'information** - Organisation et pilotage d'un test d'intrusion - Application d'une méthodologie rigoureuse en matière de test d'intrusion	**C1.1** Encadrer un projet de test d'intrusion vis à vis d'une organisation, en définissant son périmètre, l'aspect contractuel, les règles d'engagements et les étapes à suivre dans le respect des lois et de la réglementation en vigueur afin de signer un contrat d'engagement.	***Mise en situation professionnelle (C1.1, C1.2, C1.3)*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information et dans un environnement simulé, le candidat devra effectuer un	-Tous les éléments de contexte et contractuels sont définis. - Des règles d'engagement sont appliquées et la réglementation en vigueur est respectée. - La méthodologie utilisée est cohérente par rapport au contexte et aux règles d'engagement définies.

- Identification des différents scénarii de risques SI exploitable et cohérent au contexte de l'organisation. - Conception des échelles et tableaux d'impacts liés vulnérabilités et impacts business	**C1.2** Piloter les différentes phases composants un test d'intrusion en planifiant des scénarii d'attaque en lien avec le contexte de l'organisation et en rédigeant un plan de test dans l'objectif de mettre en évidence les vulnérabilités présentes au sein des systèmes d'information.	test d'intrusion et rédiger son rapport en prenant en considération l'ensemble des règles d'engagement initialement convenues. Ensuite, il fera une soutenance orale de son rapport devant le jury de validation.	- Le périmètre et le plan du test sont respectés. - Le choix des outils est adapté au test à exécuter. - Le temps imparti est respecté. - Les vulnérabilités de l'infrastructure sont identifiées de manière exhaustive.
- Restitution et synthèse auprès de la direction les impacts et plans d'action	**C1.3** Rédiger un rapport d'intrusion en mettant en avant les failles de sécurité identifiées et en expliquant la méthodologie utilisée afin de soutenir les conclusions du test auprès du donneur d'ordre.		-Les différentes étapes du test sont décrites. - Les différentes failles de sécurité et la démarche utilisée pour les identifier sont décrites. - Les conclusions du test présentées à l'oral sont compréhensibles.
- Organisation et maintien d'une veille sur les différentes thématiques liées à la cybercriminalité -	**C1.4** Organiser une veille sur les différentes menaces ainsi que sur les moyens modernes de protéger les systèmes d'information des organisations en identifiant de manière exhaustive les	***Mise en situation professionnelle (C1.4)*** A partir d'une thématique liée à la sécurité de l'information proposée par le candidat et validée par le jury, celui-ci devra expliquer la méthodologie et les références utilisées pour effectuer ses opérations de veille et de suivi de	-L'environnement de la recherche est contextualisé. -La ou les problématiques lié(es) à la thématique validée est (sont) définie(s). - Les axes de réflexions entrepris sont modélisés.

	thématiques clés et les sources à surveiller pour d'obtenir un avantage stratégique et temporel sur les attaquants.	cybermenaces sous la forme d'un rapport écrit. Une présentation orale du rapport aura lieu devant le jury de validation. .	- La recherche doit comporter un niveau de profondeur à la hauteur de la problématique identifiée. - Les sources utilisées lors de la veille sont fiables et cohérentes avec la problématique identifiée. - Les résultats de la veille sont projetés sur les futurs enjeux des organisations. - La présentation est claire et synthétique. - Le temps de présentation est respecté.

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 N° 2 Auditer la sécurité des systèmes d'information et conduire le déploiement des mesures de défenses.			
A2.1 **Audit de la sécurité des systèmes d'information**	**C2.1** Auditer les différentes mesures de sécurité actives au sein d'une organisation en mesurant leurs niveaux de maturité par rapport au contexte légal, réglementaire et contractuel et en utilisant une méthodologie d'audit		- Le contexte et l'environnement de l'organisation sont pris en considération. - Les mesures de sécurité présentes sur le périmètre sélectionné ont été auditées.

- Identification du contexte et de l'environnement de l'organisation en matière légales, règlementaires et contractuelles vis-à-vis de la sécurité de l'information - Sélection et application d'une méthodologie d'audit de la sécurité des systèmes d'information	spécifique afin de définir des potentiels écarts entre les mesures mises en place dans l'organisation, les attentes stratégiques et les obligations légales.	***Mise en situation professionnelle (C2.1, C2.2, C2.3)*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra décrire les différentes actions entreprises afin d'analyser l'environnement SI de l'organisation, identifier les points de défaillance de la sécurité des systèmes d'information et proposer un plan d'action adéquat sous la forme d'un rapport écrit. Une soutenance orale de son rapport aura lieu devant le jury de validation. .	- Une vue synthétique et globale de l'état des mécanismes de cyberdéfense est proposée. - Une méthodologie d'audit est choisie.
- Collecte les différentes mesures techniques et organisationnels liées à la sécurité de l'information - Analyse approfondie des informations collectées - Rédaction de rapport d'audit de sécurité de l'information	**C2.2** Evaluer les écarts identifiés lors de l'audit en utilisant une méthodologie de positionnement de ceux-ci par rapport aux attentes de l'organisation et aux obligations légales et en rédigeant un rapport d'audit afin d'émettre des préconisations techniques et organisationnelles d'amélioration de la sécurité de l'information.		- Une analyse des différents problèmes liés à la sécurité de l'information et leurs sources potentielles est générée. - La rédaction du rapport d'audit doit prendre en compte le contexte et les résultats de l'audit. - Les différentes phases de la méthodologie choisie sont respectées. - Le rapport d'audit est claire et exploitable dans un contexte professionnel.
- Elaboration d'un plan d'actions - Prise en considération des contraintes du Retour sur investissement en adéquation avec les impacts business identifiés	**C2.3** Formaliser des préconisations adaptées au système cible en tenant compte des principes du Retour sur investissement (ROI) en adéquation avec l'analyse d'impacts business (B.I.A.), afin de convaincre des donneurs d'ordre pour renforcer la sécurité de l'organisation et		- Un plan d'action des différentes mesures à mettre en œuvre ou à réajuster est proposé en prenant en considération le contexte, l'environnement de l'organisation et l'adéquation entre le retour sur investissement et les impacts business.

	réduire au maximum la surface d'attaque.		- Le temps de présentation est respecté.
A2.2 **Gestion des incidents de sécurité** - Identification des actifs clés pour l'organisation en matière de SI - Etude des processus de remontés d'incidents - Intégration d'un SOC au sein d'une organisation - Pilotage d'un SOC - Intégration des solutions de gestion des incidents - Elaboration d'indicateurs liés à la sécurité de l'information - Création d'une matrice des compétences - Identification des ressources manquantes - Management d'une équipe SOC au quotidien	**C2.4** Organiser la mise en œuvre d'un centre des opérations de sécurité (Security Operations Center-SOC) au sein d'une organisation en définissant son organisation, son périmètre et les moyens nécessaires à sa mission et en déployant une solution de type management des évènements et de la sécurité de l'information (SIEM) afin d'identifier et de gérer les différents événements de sécurité qui surviennent au sein des systèmes d'information. **C2.5** Manager l'équipe du SOC en s'assurant de la compétence et de la disponibilité des équipes en prenant en compte les éventuelles situations de handicap afin de garantir un niveau de service contractualisé en amont.	***Mise en situation professionnelle (C2.4, C2.5, C2.6)*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information et dans un environnement simulé, le candidat devra expliquer dans un rapport écrit son organisation quant à la mise en place d'un SOC notamment à travers le dimensionnement de l'équipe en lien avec la topologie de l'infrastructure SI. Le candidat élaborera ensuite une matrice des compétences nécessaires au maintien en condition opérationnelle du SOC et des compétences disponibles dans les équipes en identifiant les éventuels écarts.	- Les rôles et responsabilités en matière de gestion du SOC sont identifiés. - Les processus liés aux activités du SOC sont modélisés. - Une étude de la topologie de l'infrastructure SI est créé. - Une organisation est mise en œuvre quant à la collecte, le stockage ainsi que l'analyse des évènements de sécurité. - Des patterns de détection de type SIEM sont modélisées et mises en œuvre. - Une matrice des compétences nécessaires et de celles disponibles est réalisée. - La matrice prend en compte les situations de handicap le cas échéant.

- Pilotage de la gestion d'incidents au travers les indicateurs	**C2.6** Analyser le respect des engagements contractuels sur les indicateurs de pilotage et de contrôle en relevant des incidents et en vérifiant la pertinence des alertes afin de garantir l'opérationnalité de la protection.	Le candidat doit mener une réunion d'équipe pour résoudre une problématique du management du SOC Enfin, une analyse des écarts entre les indicateurs et les obligations business sera effectuée.	- Des réunions d'équipe sont organisées régulièrement. - Une étude des flux et une analyse des détections remontées sont réalisées. - Une synthèse des détections est effectuée.

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC N° 3 Analyser et sécuriser les systèmes d'information après une cyber-attaque			
A3.1 **Investigation numérique au sein d'un système d'information** - Application de méthodologie rigoureuse en matière chronologie ainsi que de relevés de preuves numériques - Collecte des différentes données au sein d'un investigation - Analyse approfondie des différents artefacts - Présentation d'une chronologie des faits - Elaboration d'un rapport d'une investigation numérique légale	**C3.1** Réaliser une investigation numérique légale (Forensic) en appliquant des protocoles d'investigation numérique respectant les procédures légales afin d'apporter des preuves d'un acte malveillant ayant été commis au sein des systèmes d'information d'une organisation. **C3.2** Formaliser les résultats de l'investigation numérique en élaborant un rapport détaillant les différentes données analysées et contextualisé en fonction de sa finalité afin d'informer les acteurs concernés.	***Mise en situation professionnelle (C3.1, C3.2)*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information et dans un environnement simulé, le candidat(e) devra expliquer et détailler dans un rapport les différentes étapes utilisées afin de mener à bien son investigation numérique en respectant les procédures légales en vigueur et remonter les différentes preuves recueillis au sein d'un rapport. Une synthèse de l'investigation devra être proposée. Ce rapport sera soutenu devant le jury de validation. .	- Le contexte et le périmètre de l'investigation sont définis. - Les étapes de l'investigation sont détaillées. - L'investigation est menée sur le périmètre ciblé. - Les éléments contextualisant le cybercrime sont identifiés. - L'origine de la cyber-attaque est identifiée. - Les différents preuves recueillies au cours de l'investigation sont présentées. - Une synthèse des éléments liés à l'investigation est rédigée. - La synthèse est exploitable dans un contexte professionnel. - Une chronologie des faits constatés pendant l'investigation est présentée

- Identification des différentes menaces de type malwares pesant sur les systèmes d'information - Identification des points d'entrées et sources potentielles de l'attaque - Analyse des fonctionnements de propagation	**C3.3** Encadrer une analyse de malware en identifiant, en cartographiant et en analysant des éléments de type "malware" dans l'objectif d'ajuster les mesures de sécurité en découlant de ces nouvelles menaces.	***Mise en situation professionnelle*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information et dans un environnement simulé, le candidat(e) devra décomposer l'ensemble de ses modes opératoires afin d'identifier une menace de type malware.	- Le périmètre et l'environnement de l'analyse sont présentés. - Le système ciblé par le malware est analysé - Les impacts générés par le malware sont identifiés - Les modes opératoires sur l'isolation, l'identification ainsi que sur le fonctionnement du malware sont exposés.
A3.2 **Renforcement des systèmes d'information** - Rédaction d'un plan d'amélioration technique et organisationnelle	**C3.4** Proposer un plan d'amélioration technique et organisationnelle en s'appuyant sur les résultats de l'investigation numérique afin de garantir un niveau de sécurité en accord avec les contraintes économiques de l'organisation.	***Mise en situation professionnelle*** A partir des résultats de l'investigation numérique réalisée et en prenant en compte le contexte de l'organisation, le candidat doit rédiger un plan de correction des défauts de sécurité identifiés.	- Un plan de correction permettant d'empêcher l'attaque de se reproduire est rédigé. - Les mesures techniques et organisationnelles proposées doivent répondre à la problématique identifiée dans le rapport d'investigation numérique rédigé.
- Modélisation des mécanismes de frein à la propagation des malwares dans les systèmes cibles - Mise en œuvre d'une solution de renforcement de systèmes	**C3.5** Mettre en œuvre des solutions techniques pour freiner la propagation des malwares en modélisant des mécanismes spécifiques afin de réduire les potentielles menaces de type malware.	***Mise en situation professionnelle*** A partir de l'analyse du malware effectuée, le candidat(e) devra proposer des mesures de sécurité techniques à mettre en œuvre pour freiner une menace de type malware.	- Des actions techniques à mener pour empêcher ou freiner le malware sont proposées. - Les actions proposées sont pertinentes pas rapport aux menaces identifiées

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC N° 4 Piloter la sécurité organisationnelle			
A4.1 **Analyse de la sécurité organisationnelle** - Identification du contexte légale, réglementaire et contractuel vis à vis de la sécurité de l'information - Analyse des différentes risques légaux pesant sur une organisation - Intégration d'un processus d'appréciation des risques SI au sein d'une organisation - Etude et analyse des scénarios de risques SI - Elaboration et proposition de plan de traitement des risques	**C4.1** Réaliser une analyse du contexte réglementaire, en identifiant les différentes obligations légales et contractuelles pesant sur les systèmes d'information d'une organisation ainsi que sur les différents postes liés à la cybersécurité dans l'objectif de maintenir une conformité légale et réglementaire. **C4.2** Réaliser une évaluation des risques SI en se basant sur la norme internationale ISO 27005 et en utilisant une méthodologie adaptée tel qu'Ebios RM afin d'établir une cartographie des risques positionnés selon leur occurrence et leur criticité.	***Mise en situation professionnelle (C4.1, C4.2)*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra rédiger un rapport expliquant les étapes utilisées afin de mener une analyse de risques SI comprenant à minima les éléments suivants : - Une analyse du contexte légal, réglementaire et contractuel - Un encadrement du projet analyse des risques - L'application de l'appréciation analyse des risques - La mise en œuvre d'un plan de traitement de risques	- La stratégie de l'organisation est prise en considération (mission, vision, stratégies, objectifs). - Une identification des obligations légales, réglementaires et contractuelles touchant la sécurité de l'information est réalisée. - Le contexte de l'analyse de risques est détaillé (objectifs, contraintes, choix de la méthode, périmètre, rôles et responsabilités, etc..). - Les différentes étapes de la méthodologie sélectionnée permettant une appréciation des risques SI sur le périmètre cible sont réalisées. - Un plan de traitement des risques identifiés lors de l'appréciation des

- Analyse d'écart entre les mesures de sécurité et les meilleurs pratiques en matières de sécurité de l'information (ISO27001/ISO27002) - Identification des besoins en continuité de l'organisation - Calcul des impacts des différents risques liés à la perte de continuité d'activité	**C4.3** Déterminer les besoins en termes de continuité d'activité d'une organisation et implémenter les préconisations adaptées au système cible en tenant compte des notions de risques SI ainsi que du B.I.A. (Business Impact Analysis), afin de convaincre les donneurs d'ordre sur les stratégies à mettre en application.	- Une synthèse de la situation des risques ***Mise en situation professionnelle*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra au sein d'un rapport identifier les différents besoins d'une organisation dans l'objectif de proposer une gestion de la continuité de l'activité efficace et efficiente. Cette gestion de la continuité se fera à travers l'identification des risques et les conséquences liés à la perte de disponibilités des activités critiques de l'organisation.	risques est rédigé en prenant en considération les obligations de résultats évoqué dans la phase contextuelle. - Une démarche d'amélioration continue est intégrée nativement aux différentes mesures de sécurité qui seront proposées dans le plan de traitement. - Le contexte et l'environnement de l'organisation sont pris en considération au sein du rapport - Le domaine d'application du système de gestion de la continuité (SMCA) est défini en fonction des objectifs et des besoins en disponibilité de l'organisation. - Une identification ainsi qu'une estimation du niveau d'efficacité et d'efficience des mesures de sécurité couvrant la perte de continuité doit être effectué. - Les activités les plus critiques pour l'organisation sont cartographiées. - Le recueil des besoins en continuité ainsi que les impacts en cas de dépassement de ces mêmes besoins

			doit être généré (analyse d'impact business).
- Analyse d'écart vis-à-vis du RGPD - Application d'une analyse relative à la protection des données (PIA)	**C4.4** Vérifier la conformité d'une organisation vis-à-vis de ses données à caractère personnelles et implémenter un plan de traitement dans l'objectif d'un alignement au RGPD en rédigeant un rapport contenant une analyse d'impact relatives à la protection des données (AIDP) en utilisant les outils et bonnes pratiques fournies par la CNIL afin de d'analyser et de réduire les écarts vis-à-vis du RGPD.	***Mise en situation professionnelle*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra recueillir au sein d'un rapport les différentes catégories de données à caractère personnelles présentes et mener une analyse d'impact relatives à la protection des données (AIDP) en utilisant les outils et bonnes pratiques fournies par la CNIL dans l'objectif de garant à l'organisation une conformité vis-à-vis du règlement général sur la protection des données. Un plan de traitement issu de l'analyse d'impact est proposé.	- Le périmètre de l'étude est identifié en fonction des différentes obligations applicables. - Les données à caractères personnelles ainsi que leurs plans de traitement respectifs sont identifiés. - Un audit des différentes mesures de sécurité présentes au sein de l'organisation et sécurisant les données à caractère personnelles est mené. - Une analyse d'impact relative à la protection des données (PIA) est réalisée en s'appuyant sur les différentes informations précédemment citées. - Un plan de traitement est proposé en fonction des différentes non-conformités remontées lors de l'analyse d'impacts.

A4.2 **Structuration de la sécurité organisationnelle** - Proposition d'une vision claire des impacts générés par les risques liés à la sécurité de l'information - Elaboration de schéma directeur SSI - Analyse d'écart entre les processus liés aux mesures de sécurité et les exigences de la norme ISO 27001	**C4.5** Conseiller les décideurs sur les différentes mesures de sécurité incontournables vis-à-vis des risques identifiés lors des analyses de sécurité de l'information afin de dimensionner un budget pour la sécurité de l'information. **C4.6** Rédiger un schéma directeur de la sécurité des systèmes d'information en s'appuyant sur les résultats des différentes analyses afin de planifier l'ensemble des projets liés à la sécurité de l'information pour l'organisation. **C4.7** Mettre en œuvre des actions permettant une conformité aux exigences de la norme internationale ISO 27001 en s'appuyant sur l'analyse des risques effectuée dans l'objectif	***Mise en situation professionnelle*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra défendre devant le jury de certification les différentes mesures envisagées afin de couvrir les risques identifiés au sein de son analyse et proposer un budget associé à ces différentes mesures. ***Mise en situation professionnelle*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra élaborer un schéma directeur de la sécurité des systèmes d'information issu du plan de traitement de l'analyse de risques précédemment menée. ***Mise en situation professionnelle*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra au sein d'un rapport réaliser une analyse de la	- Les mesures de sécurité manquantes ainsi que le renforcement des mesures existantes sont exposées. - Une estimation des coûts est présentée - Les mesures de sécurité validées et présentes au sein du plan de traitement des risques sont catégorisées. - Une projection des différents projets issus du plan de traitement est réalisée. - Une analyse de la maturité de l'organisation vis-à-vis des exigences de la norme ISO 27001 est menée. - Les objectifs de l'organisation liés au projet ISO 27001 sont identifiés.

-Proposition d'un plan d'actions vis-à-vis des écarts	de renforcer la maturité de l'ensemble de la sécurité des systèmes d'information.	maturité de la sécurité de l'information existante. Ensuite, il devra identifier les différentes étapes à mettre en œuvre pour se conformer aux exigences de la norme internationale ISO 27001.	- Le périmètre du projet ISO 27001 est défini en fonction des différents objectifs fixés par l'organisation. - Une étude des différentes mesures de sécurité présentes est réalisée. - Un plan d'action est proposé en prenant en considération, le contexte, l'environnement, les parties prenantes, les mesures des sécurité existantes ainsi que l'ensemble des non-conformités préalablement identifiés. Les différentes mesures devront intégrer la notion d'amélioration continue de manière native au sein de leurs processus.
A4.3 **Pilotage de la sécurité organisationnelle** - Suivi des projets associés au schéma directeur - Utilisation de méthodes de gestion de projet	**C4.8** Conduire des projets associés au schéma directeur de sécurité des systèmes d'information au travers différentes méthodes de gestion de projet pour garantir l'atteinte des objectifs de l'organisation.	***Mise en situation professionnelle (C4.8, C4.9)*** A partir d'un cas réel ou fictif issu des problématiques liées à la sécurité de l'information, le candidat devra défendre devant le jury de validation l'organisation	- Un alignement est démontré quant à l'utilité du projet vis-à-vis de la stratégie de l'organisation. - Le projet est structuré et les éléments suivants sont présentés : • Contexte et l'environnement • Objectifs • Rôles et responsabilités • Planning • Les risques inhérents au projet • Le pilotage et les différents jalons importants du projet

- Maintien en condition opérationnelle des risques SI liés à la sécurité de l'information - Maintien et suivi des indicateurs liés à la sécurité de l'information - Maintien en condition opérationnelle des différentes mesures de sécurité présentes au sein de l'organisation	**C4.9** Structurer une démarche d'amélioration continue et de maintien en condition opérationnelle des projets cyber en s'appuyant sur une méthode de gestion de la qualité (PDCA) afin de garantir l'efficacité et l'efficience des projets mis en œuvre.	proposée quant à l'implémentation d'un projet lié à sécurité de l'information.	- La méthode de gestion de la qualité choisie permet un pilotage efficace du projet cyber de maintien en condition opérationnelle - Le choix des indicateurs de pilotage est en lien avec les scénarios et les types de menaces de l'organisation.
-Animation de comités de pilotage -Management des équipes en prenant en compte des situations de handicap le cas échéant -Coordination des acteurs externes	**C4.10** Manager les équipes internes et coordonner les acteurs externes en animant des comités de pilotage afin d'assurer un bon suivi des opérations.	***Jeu de rôles*** A partir de scénarii issus de problématiques managériales réelles fournis, le candidat devra, à travers un jeu de rôle, démontrer sa capacité à résoudre des situations de management.	- Les différents problèmes liés au management au sein du scénario ont été identifiés. - Les éventuelles situations de handicap sont prises en compte. - Une priorisation des actions à mener est exposée. - Une explication détaillée des actions prioritaires est proposée.

Le cas échéant, description de tout autre document constitutif de la certification professionnelle

La certification est acquise par :

- La validation totale des 4 blocs de compétences ci-dessus. Chaque bloc de compétences est acquis par la validation de l'ensemble des compétences du bloc.
- La réalisation d'une période de stage ou d'alternance d'au moins 2 mois
- La soutenance d'un mémoire professionnel devant le jury de validation