CentraleSupélec | université PARIS-SACLAY

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

REFERENTIEL D'ACTIVITES, DE COMPETENCES ET D'EVALUATION – EXPERT EN CYBERSECURITE (MS)

Bloc n°1 – Concevoir la sécurité d'un système d'information

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'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1.1. Réalisation d'une analyse de risque - Gestion des risques dans le cadre normatif ISO 31000 & 27005 - Méthodes d'analyse de risque Ebios Risk Manager - Identification des biens essentiels et des biens supports de l'organisation - Cartographie des possibilités d'incidents (scénarios d'attaques) dans une organisation donnée. - Appréciation des risques : évaluation de la gravité des incidents, leurs coûts et leurs probabilités d'occurrence. - Proposition de moyens de remédiation adéquat aux risques identifiés.	**C1** Identifier les biens essentiels et supports ainsi que procédures d'exploitation de l'organisation en vue de déterminer les risques afférents en recensant les biens au sein du périmètre de l'étude ainsi que leurs relations fonctionnelles.	**E1. Mise en situation professionnelle portant sur une analyse de risques (de C1 à C5)** Le candidat est évalué sur l'étude d'un cas pratique représentatif de cas réels en suivant la méthodologie EBIOS Risk Manager. L'étude donne lieu à un rapport écrit devant mettre en évidence - Une cartographie des biens essentiels et supports - Une cartographie des risques associés - Des scénarios de menace opérationnels vraisemblables - Des mesures de sécurité complémentaires - La priorité des remédiations et budget estimatif.	Pour C1 : La cartographie des biens supports et essentiels recense l'ensemble des éléments rentrant dans le périmètre de l'étude. Les relations fonctionnelles figurent dans la cartographie.
	C2 Analyser des enjeux liés à la sécurité du SI en vue de gérer les risques associés en termes technique, économique et juridique en s'appuyant sur une étude du contexte.		Pour C2 : La cartographie des risques est précise et exhaustive : elle comprend les risques techniques, économiques et juridiques ;
	C3 Évaluer la vraisemblance d'un scénario de menace en mettant en regard le potentiel des sources de menaces considérées, l'exposition à ces menaces et la facilité d'exploitation des vulnérabilités identifiées afin d'estimer la plausibilité de celui-ci et déterminer la nature de la réponse à apporter.		Pour C3 : Les menaces sont identifiées et caractérisées. Elles sont associées à une mesure de plausibilité réaliste.
	C4 Évaluer les coûts liés à la sécurité en mettant en regard les coûts d'un incident de sécurité, d'une mesure préventive et d'une remédiation en vue de déterminer la nature de la réponse à apporter.		Pour C4 : L'appréciation des coûts associés aux risques et mesures préventives ou de remédiation est précise, justifiée et mesurée au regard des coûts moyens pour un incident de sécurité, une mesure préventive et une remédiation. Les moyens préventifs et de remédiation proposés sont pertinents et cohérents avec l'analyse de risque et l'estimation des coûts associés aux risques identifiés est réaliste.

	C5 Restituer l'analyse de risque et des moyens de remédiation auprès d'un donneur d'ordre (autorité, chef de projet, chef DSI...) dans le domaine de la SSI en réalisant un rapport et une présentation orale adaptés aux parties prenantes concernées (dont les personnes en situations de handicap) afin de sensibiliser les parties prenantes et d'arbitrer les réponses à apporter au regard de l'analyse établie.		Pour C5 : L'analyse des risques est restituée. Qualité rédactionnelle et/ou d'expression du candidat dans la restitution écrite et/ou orale de l'analyse de risques : le vocabulaire métier est maîtrisé, employé à bon escient et adapté à l'auditoire.
A1.2. Mise au point d'une stratégie de traitement du risque en accord avec l'analyse de risques - Spécification de l'architecture fonctionnelle d'un SI respectant les contraintes SSI et l'analyse de risque. - Définition des procédures techniques d'exploitation et d'utilisation des équipements informatiques respectant les contraintes SSI.	**C6** Évaluer la pertinence d'une mesure technique de sécurité en mettant en regard le contexte technique, légal et organisationnel afin d'apporter une réponse adaptée au regard des risques identifiés.	**E2 : Mise en situation professionnelle portant sur la sécurisation d'un service fourni (C6, C7)** Le candidat est évalué sur sa stratégie de sécurisation mise en œuvre qui donne lieu à la rédaction d'un rapport d'architecture et d'une restitution orale devant un jury de professionnels de la SSI. Le rapport doit comprendre : - Les choix fonctionnels effectués - Une architecture SI avec son analyse de risques	Pour C6 : Les choix fonctionnels sont mesurés et discutés au regard du service et de l'analyse de risque. L'architecture détaillée dans le rapport répond de manière adaptée aux enjeux de l'analyse de risque tout en garantissant le service attendu.
	C7 Proposer une articulation de moyens techniques et organisationnels répondant aux enjeux de l'analyse de risques en définissant des procédures d'exploitation et d'utilisation des équipements informatiques dans le respect des contraintes SSI en vue de répondre de manière adaptée aux exigences issues de l'analyse de risque		Pour C7 : Le rapport d'architecture détaille la matrice des flux. Qualité rédactionnelle du rapport, exhaustivité et qualité des justifications des choix présentés.

Bloc de compétences n°2 : Déployer les mesures techniques et organisationnelles répondant aux exigences de sécurité du SI considéré.			
A2.1 Déploiement d'une architecture de sécurité répondant aux exigences de SSI et assurant la protection des données et services numériques en accord avec la législation - Conception d'une architecture technique satisfaisant à une spécification fonctionnelle de SSI. - Mise en place des procédures organisationnelles répondant à des exigences de sécurité dans tous les niveaux. - Réalisation de phases de tests et recette de l'architecture développée.	**C8** Identifier le contexte légal en s'appuyant sur les référentiels standards (droits, obligations, normes et standards) de la sécurité concernant la protection des données et services numériques afin de mesurer les périmètres de responsabilité en matière de sécurité informatique.	**E3 : Mise en situation professionnelle portant sur la mise en place d'une architecture physique (de C8 à C10)** Le candidat conçoit l'architecture, met en place des procédures répondant aux exigences de sécurité et réalise les tests inhérents. Les solutions proposées sont évaluées par de professionnels de la SSI.	Pour C8 : Les choix de conception sont cohérents avec l'architecture fonctionnelle attendue et le contexte légal est considéré.
	C9Déployer les différents équipements et protocoles employés dans une architecture sécurisée en vue de garantir le juste niveau de sécurité en s'appuyant sur l'état de l'art.		Pour C9 : Les configurations des équipements sont alignées avec les exigences fonctionnelles, les exigences de sécurité et les différents guides de bonnes pratiques en matière de SSI.
	C10 Rendre compte auprès des équipes techniques (SI, Security Operations center (SOC), Computer Emergency Response Team (CERT)...) des mesures mises en œuvre dans le domaine de la SSI au travers de communications écrites et orales en s'adaptant à l'audience et aux potentiels profils singuliers (situation de handicap, interculturalité, ...) afin de garantir l'appropriation, par les parties prenantes, d'un vocabulaire et d'une connaissance partagée des processus mis en œuvre.		Pour C10 : Le vocabulaire technique et métier est maîtrisé, employé à bon escient et adapté à l'auditoire. Qualité rédactionnelle et/ou d'expression du candidat dans la restitution écrite et/ou orale des mesures techniques choisies ; Le vocabulaire métier maîtrisé, employé à bon escient et adapté à l'auditoire.
A2.2. Mise en place des outils de supervision des équipements informatiques et de leur sécurité - Traçabilité des actions sensibles. - Remontée des alertes aux équipes en charge de la supervision.	**C11** Déployer un juste niveau de supervision en plaçant et configurant de manière adaptée des sondes dans le SI afin de fournir des indicateurs et historiques d'actions utiles à la réponse à incident, à l'investigation numérique et la SSI.	**E4 : Etude de cas (C11, C12)** Cet examen porte sur la maîtrise des fondamentaux nécessaires au déploiement d'une architecture de sécurité, à travers un audit d'architecture de sécurité sur la base du rapport produit. Il est attendu du candidat l'emploi du vocabulaire adapté aux comptes-rendus à réaliser auprès des équipes techniques.	Pour C11 : Les équipements mettent en œuvre un juste niveau de traçabilité des actions entreprises sur le système considéré, garantissant horodatage à l'échelle du SI. Ils veillent également à l'intégrité des enregistrements et à la redondance de cet historique.
	C12 Estimer la criticité d'une alerte de sécurité, en mettant en regard le contexte de celle-ci, le cadre global de l'architecture et son lien aux biens essentiels, en vue de hiérarchiser les alertes pour faciliter le traitement de celles-ci et la recherche de corrélations.		Pour C12 : Les tentatives d'intrusion sont décelées Des alarmes remontées sont associées à un indicateur de compromission[1].

[1] Indicateur de compromission = en sécurité informatique, est un artefact observé sur un réseau ou dans un système d'exploitation qui indique, avec un haut niveau de certitude, une intrusion informatique.

CentraleSupélec | université PARIS-SACLAY

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Bloc de compétences n°3 : Exploiter en sécurité un SI			
A3.1 : Contrôle de l'application des procédures qualité et sécurité des systèmes d'information et télécoms - Intervention en sécurité sur des équipements d'interconnexion - Intervention à distance et en sécurité sur des ressources de type Windows. - Intervention à distance et en sécurité sur des ressources de type Unix**.** - Respect des référentiels qualité et sécurité internationaux (ISO / IEC 27001 / 27002, série ISA-99 / IEC 62443, guides NIST, etc.) et européens et nationaux (RGS, II901, guides ANSSI, guides CNIL…)	**C13** Collecter des preuves d'audits ou des indicateurs de compromission en sécurité en respectant les procédures qualité et sécurité des SI afin de vérifier l'adéquation entre le plan initial et la mise en œuvre effective.	**E5 : Mise en situation professionnelle simulée portant sur l'exploitation d'un SI proposé au candidat (C13 à C17)** *Restitution orale individuelle* Le candidat doit exploiter l'architecture, mettre en place des procédures répondant aux exigences de sécurité et réaliser les tests inhérents. Les solutions proposées sont évaluées par de professionnels de la SSI. Le candidat présente le résultat de ses travaux lors d'un entretien oral.	Pour C13 : Les procédures utilisées sont conformes en regard des guides de bonnes pratiques associés aux équipements à administrer.
	C14 Assurer la conformité des configurations et fonctionnalités des différents composants du SI dans le respect du cadre global de la réglementation en vigueur et des différents référentiels afin d'intervenir en sécurité sur les équipements et les ressources.		Pour C14 : Les éléments de configurations sont cohérents entre eux et l'ensemble satisfait aux exigences de sécurité du SI.
	C15 Assurer l'adéquation entre les configurations et les évolutions techniques pour garantir un juste niveau de sécurité en mobilisant les principes fondamentaux des outils cryptographiques.		Pour C15 : Les concepts cryptographiques nécessaires au fonctionnement en sécurité du SI sont identifiés et compris. La configuration des équipements fournie répond au besoin des éléments cryptographiques identifiés**.**
A3.2 : Veille au respect de la loi Informatique et Libertés, du RGPD dans l'entreprise, gestion de la liste des	**C16** S'assurer du respect du cadre législatif par les opérateurs techniques dans un SI complexe et hétérogène en ayant recours aux procédures		Pour C16 : Les mesures techniques mises en œuvre respectent le cadre législatif

traitements de données à caractère personnel et interface avec la CNIL - Intervention dans un SI complexe. - Réalisation de rapport**.**	qualités et sécurité afin de garantir la conformité aux réglementations en vigueur.		
	C17 Rendre compte, auprès d'un public à compétences légales et/ou donneur d'ordres ainsi qu'aux autorités compétentes, de l'adéquation ou des éventuels écarts au cadre législatif des traitements relatifs aux données à caractère personnel effectué en réalisant des rapports et présentations orales adaptées aux spécificités du public (dont les personnes en situations de handicap) afin de leur permettre une prise de décision avertie.		Pour C17 : Qualité du compte rendu, des justifications apportées concernant les mesures techniques choisies au regard du cadre légal, adaptation au public cible.

Bloc de compétence n°4 : Maintenir de manière continue la sécurité d'un SI			
A4.1. Audit ou supervision d'audit de la sécurité du SI et compte-rendu de l'audit - Rédaction d'un programme d'audit (périmètre, critères et objectifs). - Collecte d'informations dans le but d'établir des preuves d'audit en regard des critères d'audit. - Analyse des preuves d'audit afin d'établir des constatations en regard des objectifs de l'audit**.** - Rédaction d'un rapport d'audit à partir des constations de l'audit.	**C18** Intervenir dans un système complexe et inconnu en rédigeant un programme d'audit comprenant le périmètre, les critères et les objectifs de sorte à collecter des preuves d'audits.	**E6 : Mise en situation professionnelle simulée portant sur l'audit d'un système d'information (C18, C19)** A partir d'un programme d'audit, le candidat collecte les informations dans le but d'établir les preuves d'audit, les analyser afin d'établir des constats recensés dans un rapport.	Pour C18 : La démarche d'investigation est justifiée, cohérente, et en accord avec le périmètre, les critères et la nature (boite noire, blanche, ...) de l'audit.
	C19 Documenter les procédures permettant la collecte de preuves d'audit en analysant les preuves et en établissant des constatations afin de rejouer ces scénarios de collecte.		C19 : Les procédures sont suffisamment documentées pour apporter des éléments de preuves au regard des critères d'audit Le programme d'audit délimite le périmètre d'intervention, détermine les objectifs et les critères d'audit
	C20 Restituer, auprès d'un public technique et/ou de donneur d'ordres, un audit relatif aux procédures effectuées en collectant les preuves d'audit et les conclusions en termes de SSI, en veillant à ce qu'il soit adapté à tous les lecteurs (dont les personnes en situation de handicap) afin de réaliser des préconisations techniques et/ou organisationnelles	**E7 : Mise en situation professionnelle simulée portant sur l'audit de systèmes reposant sur les technologies du web (C20)** Le candidat mesure la sécurité d'une application web réaliste à travers un test d'intrusion (*pentest*). Il identifie les vulnérabilités présentes dans l'application, évalue leur exploitabilité par un attaquant, leur criticité et propose des contremesures. Ses résultats sont synthétisés dans un rapport de *pentest similaires aux rapports attendus en milieu professionnel évalué par des professionnels en activité dans ce domaine. Ce rapport comprend :*	Pour C20 : Qualité du compte rendu, des justifications apportées concernant les mesures techniques choisies au regard du cadre légal, adaptation au public cible.

		- **Résumé exécutif** : Une vue d'ensemble des principales découvertes et lrecommandations. - **Méthodologie** : Description des méthodes et des outils utilisés. - **Découvertes** : Liste des vulnérabilités identifiées. Chaque vulnérabilité est accompagnée des implications pour la sécurité, et des preuves de son existence - **Recommandations** : Conseils sur la manière de corriger les vulnérabilités identifiées. - **Plan de remédiation** : Un plan détaillé pour la mise en œuvre des recommandations .	
A4.2 : Veille continue au regard de l'évolution du contexte global (technique, menace, organisationnel, législatif, ...); comptes-rendus et force de proposition. - Veille sur les évolutions technologiques des systèmes d'information et de télécommunications ; proposition et mise en œuvre des évolutions techniques. - Veille sur l'évolution de la menace et proposition des réponses techniques ; préconisation d'actions préventives et formatives.	**C21** Réaliser une veille continue concernant les dernières évolutions technologiques, des systèmes d'informations et des télécommunications en évaluant leurs impacts et leurs coûts en termes de SSI afin de rendre compte et proposer des évolutions pertinentes en conséquence.	**E8 : Mise en situation professionnelle simulée portant sur une analyse de risques (C21)** Le candidat établit une étude bibliographique et constitue un rapport d'analyses de risques	Pour C21 : Les outils de références bibliographiques sont connus et exploités ; l'analyse de l'état de l'art est pertinente au regard du périmètre fonctionnel du SI et des choix techniques de SSI. Les évolutions techniques proposées répondent aux besoins recensés et aux contraintes de coûts dans le respect de l'analyse de risques courante Les actions entreprises dans le cadre de l'analyse de sécurité d'un produit sont cohérentes au

- Adaptation de l'analyse de risques courante en regard de l'évolution des menaces et des évolutions techniques, structurelles et législatives.			regard des différents référentiels liés à la certification (CSPN[2], Critères communs, …).
	C22 Réaliser une veille continue concernant les dernières vulnérabilités, menaces et produits de sécurité pour les analyser, en évaluant les impacts d'une vulnérabilité ou d'une menace afin de contribuer à maintenir la sécurité d'un système, en relation avec les acteurs du projet (spécialistes informatiques, les administrateurs, RSSI) et les utilisateurs.	**E9 : Mise en situation professionnelle simulée portant sur l'analyse de sécurité d'un produit de sécurité (C22, C23)** Le candidat rédige un rapport technique détaillant les vulnérabilités d'un produit de sécurité identifiées avec une cotation de celles-ci.	Pour C22 : Les outils classiques de *threat intelligence*[3] sont connus et exploités de manière régulière pour déterminer l'évolution de la menace et des vulnérabilités. L'impact des nouvelles vulnérabilités concernant le SI est clairement établi.

[2] CPSN : la Certification de Sécurité de Premier Niveau, aussi appelée « Visa de Sécurité de l'ANSSI », est une des certifications délivrée par l'Agence nationale de la sécurité des systèmes d'information pour des produits des technologies de l'information. Mise en place en 2008, elle consiste en des tests en « boîte noire » effectués en temps et délais contraints. La CSPN est une alternative aux évaluations Critères Communs, dont le coût et la durée peuvent être un obstacle, et lorsque le niveau de confiance visé est moins élevé. Cette certification s'appuie sur des critères, une méthodologie et un processus élaborés par l'ANSSI. Cette méthodologie est enseignée dans le programme de formation adossé à la certification.

[3] *Threat intelligence* = aussi appelée, Cyber Threat Intelligence, discipline basée sur des techniques du renseignement qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyberespace, afin de dresser un portrait des attaquants ou de mettre en exergue des tendances.

	C23 Gérer les risques associés en adaptant l'analyse de risques courante en regard de l'évolution des menaces et des évolutions techniques, structurelles et législatives afin d'opérer une gestion des risques actualisée et optimale.		Pour C23 : Les nouvelles menaces concernant le périmètre de l'analyse de risque sont identifiées et analysées. La mise à jour de l'analyse de risque courante est pertinente au regard de ces évolutions. L'analyse de risques courants est actualisée en fonction des évolutions techniques structurelles et législatives

<table>
<tr><th colspan="4">Bloc de compétence n°5 : Réagir à un incident de sécurité</th></tr>
<tr>
<td rowspan="3">A5.1. : Détection d’un incident de sécurité et adoption d’une posture adaptée au contexte : gestion de crise

- Analyse de l’environnement et de l’incident de sécurité (combien de temps, quel impact…).

- Collecte et analyse d’informations.

- Capitalisation des indicateurs de compromission, synthèse des analyses, mesures de remédiation et révision de la posture.</td>
<td>C24 Identifier la portée temporelle et fonctionnelle d’un incident de sécurité en ayant recours aux différentes sources d'informations à disposition (documents d'architecture, alertes de sécurité et analyse de risque courante...) afin de caractériser la menace.</td>
<td rowspan="3">E10 : Mise en situation professionnelle simulée portant sur un incident de sécurité (de C24 à C28)

Le candidat propose une architecture de détection d’intrusion :
- Il propose les phases de tests
- Il doit collecter et analyser les informations de l’incident
- Il collecte des indicateurs de compromissions et coordonne la gestion de crise
- Il rédige le diagnostic et émet des préconisations</td>
<td>Pour C24 :
La portée temporelle et fonctionnelle de l’incident de sécurité est identifiée.
La menace est identifiée et la posture adéquate est adoptée, de manière justifiée.</td>
</tr>
<tr>
<td>C25 Collecter des indicateurs de compromission en mesurant les coûts associés à l’incident afin d’agir en accord avec la posture[4] adaptée.</td>
<td>Pour C25 :
Les indicateurs de compromission sont collectés, et permettent de valider ou invalider l’hypothèse de la menace</td>
</tr>
<tr>
<td>C26 Coordonner la gestion de crise et la réponse à incident en prenant en compte les contextes techniques et organisationnels en vue de limiter la portée temporelle et fonctionnelle de l'incident.</td>
<td>Pour C26 :
Les éléments de communication permettent la coordination de la gestion de crise et de la réponse à incident : les éléments sont clairs et factuels, les hypothèses et certitudes clairement identifiées ainsi que l’impact de la crise.
Les éléments liés à l’incident sont communiqués en temps réel tout au long de la crise de façon factuelle
Les hypothèses et certitudes sont identifiées
L’impact de la crise est explicité</td>
</tr>
</table>

[4] « Posture » est ici un terme employé au sens du référentiel PRIS (prestataire de réponse à incident de sécurité). La posture désigne « ensemble composé de la démarche de réponse à incident, du niveau de discrétion à adopter vis-à-vis de l’attaquant, des ressources à engager et du calendrier des activités. »

A5.2. : Contrôle de la sécurité de la reprise d'activité. - Diagnostic de la nature et de l'origine des incidents et mise en œuvre de mesures correctives (origine et validation des hypothèses) - Rédaction d'un rapport d'incident en émettant des préconisations curatives et formatives	**C27** Diagnostiquer, en sécurité, la nature et l'origine des incidents en vue d'exhiber le scénario d'attaque effectif et d'ainsi faire évoluer l'analyse de risque en conséquence.		Pour C27 : La démarche de diagnostic est cohérente au regard des éléments collectés (*ex.,* logs, indices de compromission) ; le processus d'investigation permettant d'avancer des hypothèses, de valider certaines d'entre elles par la collecte de nouveaux éléments, est clairement décrit. Les hypothèses concernant la nature et l'origine de/des incident/s sont explicitées Les hypothèses sont validées, la nature et l'origine du/des incident/s est déterminée
	C28 Établir un rapport d'incident détaillant le scénario d'attaque effectif en préconisant des actions curatives et formatives en vue de déterminer des contre-mesures adéquates.		Pour C28 : Le scénario d'attaque effectif est exhibé Les recommandations formulées permettent d'améliorer l'analyse de risque en conséquence Le vocabulaire métier est maîtrisé, employé à bon escient et adapté à l'auditoire. Qualité rédactionnelle et/ou d'expression du candidat dans la restitution écrite et/ou orale du rapport d'incident.

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

Les compétences évaluées sont réparties en cinq blocs :

1. Concevoir la sécurité d'un système d'information
2. Déployer les mesures techniques et organisationnelles répondant aux exigences de sécurité du SI considéré
3. Exploiter en sécurité un système d'information
4. Maintenir de manière continue la sécurité d'un système d'information
5. Réagir à un incident de sécurité

La certification s'obtient par la validation de l'ensemble des blocs de compétences et de la thèse professionnelle dans le cadre des voies d'accès par la formation. Il est possible de valider partiellement la certification en validant un ou plusieurs blocs de compétences.

La thèse professionnelle est un travail de recherche appliquée à un domaine particulier ou à une fonction particulière. Orienté vers la pratique, il est en général lié à une thématique de la mission en entreprise. C'est un véritable projet d'action qui traite une problématique d'entreprise et débouche sur l'élaboration de propositions concrètes permettant à chacun d'appliquer immédiatement les concepts, méthodes et outils acquis pendant la formation. Elle constitue un retour d'expérience et une expertise dans le domaine. Ce travail donne lieu à la rédaction d'un document et à une soutenance individuelle devant un jury composé du tuteur école et du tuteur entreprise. Le choix du sujet est laissé au soin de l'apprenant qui doit en faire part au Responsable du programme concerné pour validation et attribution d'un tuteur école. Ce dernier encadrera l'apprenant dans la rédaction de son travail selon un calendrier précis qui lui sera remis en début d'année académique. Le tuteur école est un enseignant à CentraleSupélec reconnu pour son expertise dans le domaine. Par ailleurs, l'apprenant est encadré au sein de l'entreprise par un tuteur entreprise.

Pour la voie d'accès VAE, la certification s'obtient par validation de l'ensemble des blocs de compétences.

La formation et la certification sont accessibles aux candidats en situation de handicap. En ce sens, des aménagements dans le cadre des modalités d'évaluation sont possibles et seront définies au cas par cas auprès du Référent Handicap.