REFERENTIEL D'ACTIVITES, DE COMPETENCES ET D'EVALUATION

Article L5113-1 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.* »

Candidat en situation de handicap :
Dans le cadre du respect du règlement d'examen, tout candidat peut saisir le référent handicap du certificateur pour aménager les modalités d'évaluation et obtenir l'assistance d'un tiers lors de l'évaluation. Les supports et le matériel nécessaires à la réalisation des évaluations pourront être adaptés.
Sur conseil du référent handicap et dans le respect des spécifications du référentiel, le format de la modalité pourra être adaptée.

Sur avis motivé du référent handicap le jury de certification peut décider d'exempter le candidat de certains critères d'évaluation. :
- dans la mesure où cela ne remet pas en question la capacité professionnelle globale du candidat
- si le critère au regard de la nature du handicap n'a pas vocation à s'appliquer dans la pratique professionnelle future du candidat
Ces deux critères étant cumulatifs.

L'ingénieur de certification s'engage dans la mesure du possible à élaborer des modalités d'évaluation inclusives permettant une adaptation du format. Dans le cas d'une modalité spécifique à une situation de travail, il s'engage à préciser le cadre des aménagements possibles.

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 DE CERTIFICATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
Activité 1 : Conception et pilotage de la politique de sécurité de l'information au sein d'une/plusieurs organisations	C1.1 Elaborer un dispositif de veille scientifique, technique, technologique, règlementaire, sectorielle et concurrentielle portant sur les	**Mémoire professionnel :** Dans le cadre d'une problématique en matière de cybersécurité	Présentation d'une cartographie des principaux domaines de veille exposant la finalité générale, les objectifs précis et les moyens mobilisés pour chacun d'entre eux.

A1.1 Pilotage d'un système de veille scientifique, technique, technologique, règlementaire, sectorielle et concurrentielle	évolutions en matière de cybersécurité en : - définissant les objectifs de veille, - mobilisant des méthodologies de recherche, traitement et exploitation de données, - évaluant la fiabilité du protocole, afin d'anticiper les enjeux de cybersécurité des organisations	rencontrée par une/plusieurs entreprise(s), le candidat doit : 1) Proposer une analyse réflexive de sa méthodologie de travail et de son dispositif de veille en lien avec la problématique 2) Elaborer un dispositif de veille et présenter un tableau de veille 3) Présenter et analyser l'état de l'art portant sur les aspects techniques et/ou règlementaires d'une problématique de cybersécurité --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.*	Démontre la pertinence des outils de veille utilisé au regard des objectifs recherchés. Démontre la pertinence et la fiabilité des sources utilisées. Structure l'information et démontre sa capacité à la restituer : fréquence, destinataires et formalités de diffusion. Les principaux articles de recherche et d'ouvrages fondamentaux abordant le thème sont cités et analysés. Il démontre sa connaissance technique des bonnes pratiques, de l'état de l'art, et des normes réglementaires régissant l'activité (en particulier le droit du numérique (RGPD / Secret des Affaires / Réponses Pénales / Atteintes à la Réputation / INFOX …).
A1.2 Réalisation d'audit périodique de cybersécurité	C1.2 Piloter la réalisation et/ou réaliser un audit de cybersécurité au sein d'une organisation sur un périmètre	**Mise en situation professionnelle :**	Démontre la connaissance des méthodologies et outils du diagnostic d'un système de management de la

auprès d'une/plusieurs organisations A1.3 Identification des enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation	préalablement établi avec le commanditaire en : - définissant les objectifs visés par l'audit, - réalisant des interviews auprès des audités (administrateurs système, développeurs, commanditaire, collaborateurs …) - réalisant des analyses techniques sur des points de contrôles précisés, afin de réaliser un état des lieux exhaustif des risques menaçant l'organisation et de la maturité des système SI en matière de cybersécurité	Dans le cadre d'une mise en situation professionnelle réelle ou reconstituée le candidat doit : - Formaliser le protocole d'audit à partir des informations recueillies dans le brief - Analyser les réponses issues d'interviews réelles ou reconstituées, - Identifier les failles de sécurité et risques associés - Réaliser un rapport d'audit synthétique --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.*	sécurité de l'information, et leur mise en application dans un contexte préétabli dans lequel s'inscrit l'organisation. Le/la candidat(e) démontre l'identification exhaustive des ressources de l'organisation (ressources humaines, matérielles, immatérielles, financières) par rapport au périmètre audité (domaine d'application du SMSI). Il identifie les facteurs environnementaux, organisationnels et réputationnels représentant un risque sur l'organisation Il dresse un tableau complet comprenant les risques en matière de sécurité de l'information pour l'organisation. Il présente une synthèse sous la forme d'un rapport d'audit.
A1.4 Définition de la politique de sécurité et d'organisation de l'information	C1.3 Elaborer la politique de sécurité de l'information d'une/plusieurs organisations en définissant :	**Mise en situation professionnelle :**	Le candidat démontre sa capacité à identifier l'activité de l'organisation, ses actifs et/ou biens générateurs de valeur.

A1.5 Définition des axes et des objectifs stratégiques en matière de cybersécurité	- le périmètre du système de management de la sécurité de l'information, - les objectifs en matière de niveau de sécurité attendu (*intégrité, confidentialité et disponibilité de l'information*) et en tenant compte des actifs/biens de l'organisation et de son activité	Dans le cadre d'une mise en situation professionnelle réelle ou reconstituée le candidat doit : - Présenter les objectifs stratégiques en matière de cybersécurité de l'organisation, - Etablir des recommandations concernant la politique de sécurité de l'information de l'organisation à partir des résultats de l'audit, dans le respect de la législation en vigueur. - Démontrer que ces recommandations concourent à la réalisation des objectifs stratégiques --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.*	Le candidat identifie correctement les axes stratégiques de l'organisation aux vues de ses actifs et de sa politique de développement. Il décline ces axes stratégiques en objectifs SMART en matière de cybersécurité. Le candidat démontre sa capacité à tenir compte des enjeux internes et externes ainsi que de leurs impacts éventuels sur capacité de l'organisation à gérer les risques et atteindre les objectifs fixés. La politique de sécurité de l'information proposée par le candidat permettrait d'assurer un niveau adéquat de sécurité en termes de confidentialité, disponibilité et d'intégrité des actifs informationnels contre toutes les menaces préalablement identifiées. Le candidat a bien intégré le droit d'accès, de rectification, d'opposition, de portabilité et d'effacement des données pour les prospects, clients ou salariés, dans sa politique de sécurité de l'information.

A1.6 Planification du déploiement de la politique de sécurité à l'échelle d'une organisation	C1.4 Planifier les plans d'actions annuels et/ou pluriannuels permettant le déploiement de la politique de sécurité de l'information en déterminant les objectifs et les mesures de sécurité, ainsi qu'un calendrier d'audit interne de manière à permettre le suivi des risques initialement identifiés, les mesures prises et les nouvelles menaces associées	**Mise en situation professionnelle :** Dans le cadre d'une mise en situation professionnelle réelle ou reconstituée, le candidat doit : - Expliciter les objectifs de sa politique de sécurité de l'information, - Traduire ses objectifs en indicateur de performance, - Proposer des lignes directives (plans d'actions) permettant la réalisation des objectifs - Proposer un calendrier de déploiement --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant*	Les objectifs définis intègrent à minima : des objectifs d'amélioration de la sécurité des informations auprès des parties prenantes, la continuité des activités critiques en cas de risque avéré, la conformité voire l'anticipation des évolutions règlementaires. Les indicateurs de performance proposés sont pertinents au regard des objectifs préalablement identifiés et permettent de mesurer efficacement leur atteinte. Les plans d'actions proposées intègrent l'ensemble des exigences légales, réglementaires et contractuelles, et viennent soutenir les objectifs définis. Le calendrier est réaliste aux vues de la nature des chantiers, du budget et de l'organisation.

		l'ensemble des éléments précités. Les critères restent les mêmes.	
Activité 2 : Déploiement et exploitation des mesures et de la politique de sécurité de l'information 2.1 Evaluation de la nature et de la criticité des risques 2.2 Organisation des structures de pilotage des plans de traitement des risques en matière de sécurité au sein de l'organisation	C2.1 Établir un plan de traitement des risques à partir d'une définition du niveau de sécurité selon divers scénarii, la nature et la criticité des risques rencontrés et les exigences légales, règlementaires et contractuelle, dans le but d'adresser l'ensemble des risques d'une organisation	**Mise en situation professionnelle :** Dans le cadre d'une mise en situation professionnelle réelle ou reconstituée le candidat doit : - Proposer un plan de traitement des risques selon des scénarii préétablis --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.*	Démontre sa capacité à positionner le niveau adéquat de sécurité dans tous les composants d'un Système d'Information en fonction des besoins des métiers et des actifs du commanditaire. Le candidat identifie de façon exhaustive l'ensemble des risques associés aux valeurs métier. Il présente des scénarii clairs et détaillés (scénarios stratégiques) représentant les chemins d'attaque qu'une source de risque est susceptible d'emprunter. Selon les scénarii, il évalue de façon réaliste l'étendue et la gravité de leurs impacts par rapport aux métiers et actifs identifiés. Il évalue et caractérise le niveau de vraisemblance des scénarios opérationnels obtenus, de façon précise et réaliste.

A2.3 Définition des mesures organisationnelles et techniques nécessaire à l'atteinte des objectifs de sécurité	C2.2 Déployer des mesures de sécurité opérationnelle sur l'ensemble du parc informatique et des SI, grâce à : - des mesures organisationnelles (politique d'habilitation, cartographie de la donnée, sensibilisation, politique de confidentialité…) - des mesures techniques (outils d'anonymisation de la donnée, protection des serveur, process d'identification et d'authentification, techniques de cryptographie …) de manière à limiter les risques en matière de cybersécurité	**Mise en situation professionnelle :** Dans le cadre d'une mise en situation professionnelle réelle ou reconstituée le candidat doit définir des mesures techniques et organisationnelles et à minima y : - Présenter des mesures de sécurité opérationnelle, - Expliciter la gestion des accès utilisateurs, - Planifier un plan de sauvegarde des données, - Créer une procédure de cryptographie pour sécuriser l'accès aux données préalablement identifies. --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.*	Les mesures de sécurité opérationnelle présentées répondent aux exigences et contraintes règlementaires (notamment en matière de droit du numérique et RGPD). Le candidat explicite la gestion et le contrôle des accès via le biais d'un fichier/répertoire. Cette gestion doit inclure obligatoirement une politique de contrôle d'accès restreinte. La planification du plan de sauvegarde est cohérente par rapport à la nature de l'activité de l'organisation, à la nature des risques identifiés et à leur criticité, ainsi qu'aux objectifs en matière de sécurité préalablement identifiés. Le candidat démontre sa maîtrise des techniques de cryptographie en créant une clé publique, permettant le chiffrement ; une privée, permettant le déchiffrement. Le candidat démontre sa capacité à réaliser une politique de sécurité complète intégrant des mesures techniques dédiées à sécuriser la donnée, et des mesures organisationnelles (procédure…) pour garantir la qualité de cette donnée.

			Ces mesures techniques et organisationnelles sont adaptées par rapport aux risques identifiés préalablement, à leur nature et leur criticité.
A2.4 Gestion de incidents liés à la sécurité de l'information	C2.3 Diagnostiquer un incident de sécurité en recherchant et analysant les informations liées à l'incident (*traces informatiques, journaux d'évènements, diagrammes de topologie réseau* …) à l'aide d'outils afin d'évaluer l'ampleur de l'incident et de proposer des actions correctrices	**Etude de cas :** Sur la base d'une étude de cas réelle ou reconstituée présentant un incident cybersécurité, intégrant notamment des journaux d'évènements et des diagrammes de topologie réseau, le candidat doit : - Réaliser un diagnostic de l'incident, - En déterminer le scénario possible d'incident, - Et évaluer l'impact associé.	Le candidat démontre sa capacité à élaborer un scénario réaliste en se basant sur les éléments intégrés aux journées d'évènements, et en les agençant selon une ligne de temps. Il classe les évènements par nature et catégorie, en discriminant ceux qui ne permettent pas d'affiner le diagnostic. Le candidat propose des hypothèses pertinentes au regard des éléments analysés et de la nature de l'incident. L'impact associé est évalué de façon réaliste et présenter sous forme visuelle pour aider à la prise de décision.
A2.5 Diffusion d'une culture SSI à destination des utilisateurs et décideurs grâce à de la formation et de la sensibilisation	C2.4 Former et sensibiliser les collaborateurs au travers de : - la rédaction d'une charte informatique, - la réalisation de campagne d'information (*communication, sensibilisation et formation*),	**Mise en situation professionnelle** Dans le cadre d'une mise en situation professionnelle, le candidat doit réaliser une campagne de sensibilisation des	Le candidat détermine des objectifs qualitatifs et quantitatifs en amont de la réalisation de sa campagne de sensibilisation.

A2.6 Réalisation d'actions de sensibilisation ponctuelles selon les besoins et risques identifiés	- l'animation de campagne de live-hacking, En partageant les risques en matière de cybersécurité et les impacts RSE associés, afin de diminuer les risques de cybersécurité liée aux comportements humains	collaborateurs, en expliciter la mise en œuvre et les résultats attendus vs réels. Cette campagne doit intégrer une dimension RSE.	La campagne proposée est cohérente avec l'organisation et les enjeux rencontrés par celle-ci selon l'environnement dans lequel elle s'inscrit. La campagne répond aux objectifs préalablement établis, et dans le cas contraire, le candidat expose une analyse réflexive de sa pratique afin de proposer des axes d'amélioration pertinents. Cette campagne est innovante dans son format et/ou dans son contenu (live hacking, mise en avant des techniques utilisées par les pirates, gamification …) Le candidat intègre la dimension RSE et éthique dans sa campagne de sensibilisation, afin d'alerter les parties intéressées des risques sociétaux et éthiques.
A2.7 Réalisation d'un reporting régulier auprès de sa hiérarchie sur le niveau de couverture courant des risques de sécurité SI	C2.5 Elaborer des tableaux de bord mesurant l'efficacité des mesures et la conformité du système, à destination de la direction de l'organisation, de manière à superviser le déploiement de la politique de sécurité de l'information	**Mise en situation professionnelle :** Dans le cadre d'une mise en situation professionnelle réelle ou reconstituée le candidat doit présenter un reporting en : - Présentant des tableaux de bord intégrant les différents indicateurs permettant de superviser le	Les tableaux de bord sont exploitables et intègrent l'ensemble des indicateurs préalablement établis. Des seuils permettent de réaliser des alertes visuelles représentant un risque pour l'organisation.

		déploiement de la politique de sécurité de l'information. --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.*	Le candidat démontre sa capacité à dresser une analyse à partir de tableaux de bord pré-remplis.
Activité 3 : Management de projet de transformation et/ou d'innovation SI/cybersécurité	C3.1 Concevoir un projet de transformation et/ou d'innovation SI/cyber sur la base d'une étude d'opportunité et de faisabilité, évaluant le retour sur investissement, en mobilisant des outils d'idéation et innovation technologique afin de soutenir les objectifs stratégiques SI et cybersécurité de l'organisation	**Dossier de consulting :** Dans le cadre d'une problématique rencontrée par une entreprise réelle ou fictive, le candidat doit proposer un projet de transformation et/ou d'innovation. --- *Lorsqu'un candidat se présente uniquement sur un bloc de*	Le/la candidat(e) identifie les besoins du client interne/externe (gestion et/ou pilotage de la data, problématique business, risque sécurité, problématique réputationnelle…). Il/elle traduit les besoins du client en objectifs qualitatifs et quantitatifs. Le/la candidat identifie une problématique répondant à un enjeu rencontré par une organisation.

		compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.	Il conçoit un projet SI et/ou cyber répondant à la problématique rencontrée par l'organisation. Il/elle explicite son choix et démontre la pertinence du projet du point de vue du client interne/externe. Il/elle propose une évaluation réaliste des retombées attendues. Il/elle rédige un cas d'affaire du projet respectant les usages et standards.
A3.1 Evaluation des ressources matérielles, financières et humaines nécessaires à la réalisation du projet A3.2 Pilotage du déploiement du projet (de la gestion des tâches, au livrables)	C3.2 Définir l'organisation et les étapes d'un projet de transformation et/ou d'innovation, les principaux livrables, les besoins en ressources humaines, matérielles et financières, ainsi que les contraintes spécifiées par la maîtrise d'ouvrage afin de prioriser les différents chantiers SI	**Dossier de consulting :** Dans le cadre d'une problématique rencontrée par une entreprise réelle ou fictive, le candidat doit présenter : - La méthodologie de gestion de projet SI utilisée, - Les contraintes MOE/MOA, - Un rétroplanning, Les différents jalons de déploiement et livrables associés --- *Lorsqu'un candidat se présente uniquement sur un bloc de*	Il/elle choisit et détaille une méthodologie de projet adaptée à l'organisation et aux objectifs du projet SI/Cybersécurité. Démontre sa maîtrise de la méthodologie de gestion de projet SI (*compréhension de la mécanique et capacité de mise en œuvre*). Il/elle propose un compte rendu et un document de suivi pertinents, intégrant les différentes contraintes MOE/MOA. Le document de suivi est visuel et reprends les solutions sélectionnées, le rétroplanning et les livrables attendus.

		compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.	Les indicateurs de performance sélectionnés sont cohérents par rapport au projet mené. La méthodologie d'études permet d'apporter de la donnée exploitable pour répondre aux indicateurs préalablement définis.
A3.3 Sélection de partenaires A3.4 Évaluation du niveau de sécurité auprès des partenaires, notamment à travers la réalisation d'audits périodiques et de contrôles permanents	C3.3 Identifier et sélectionner des partenaires (prestataires, fournisseurs, experts…) sur la base d'une grille de critères spécifiques base, dans le respect de la politique et des règles de sécurité des SI de manière à lancer un projet de transformation et/ou d'innovation SI/Cybersécurité	**Dossier de consulting :** Dans le cadre d'une problématique rencontrée par une entreprise réelle ou fictive, le candidat doit présenter une cartographie des prestataires et/ou fournisseurs susceptibles d'intervenir sur tout ou une partie du projet de transformation et/ou d'innovation. Il doit expliciter leur secteur d'intervention. Le candidat doit présenter les règles de sécurité applicables dans l'organisation et vis-à-vis des sous-traitants, et expliciter la façon dont il s'assure de leur respect par lesdits sous-traitants. ----------	Le candidat présente l'ensemble des besoins pouvant être externalisés. Il sélectionne des indicateurs d'évaluation permettant de montrer la pertinence des prestataires choisis par rapport aux besoins (délai, qualité, notoriété, …) et au respect de la politique et des règles de sécurité (objet durée, et finalité du traitement des données externalisées, transparence et traçabilité des actions réalisées, information en cas de fuite des données…) Le candidat identifie des prestataires susceptibles de répondre aux besoins du projet de transformation et/ou d'innovation SI sur la base d'un travail de veille et de l'application de la grille d'évaluation. Il démontre l'exploitation des outils créés, ainsi que l'adéquation

		Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.	entre les prestataires choisis et les critères préalablement définis.
A3.5 Promotion des chartes de sécurité informatique sur son périmètre A3.6 Sensibilisation des parties intéressées du projet de cybersécurité, ou SI à fort enjeux sécurité	C3.4 Piloter l'accompagnement au changement suite au déploiement d'un projet SI/Cybersécurité en mobilisant des outils (charte de sécurité, procédure…) et méthodes de conduite du changement adaptés à la singularité des personnes (handicap, intergénérationnel…) et du projet de cybersécurité de manière à permettre l'acculturation des collaborateurs et la gestion des résistances	**Dossier de consulting :** Dans le cadre d'une problématique rencontrée par une entreprise réelle ou fictive, le candidat doit rédiger une note intégrant les préconisations en matière d'acculturation et d'accompagnement aux changements. Il doit présenter une charte de sécurité informatique et des supports de sensibilisation aux enjeux cybersécurité associés au projet. --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de*	Le/La candidat(e) sélectionne et utilise des méthodes et des techniques d'élaboration de "la mission, la vision et la valeur" adapté au projet. Il/elle démontre sa maîtrise de la psychologie comportementale et cyber. Il/elle détermine clairement le sens de mission. Il/elle rédige un plan d'accompagnement à destination des collaborateurs comprenant une période de communication, de sensibilisation et de formation. Le/la candidat(e) identifie clairement les facteurs de résistances aux changements, en capitalisant sur ses connaissances de la culture de la

		bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.	différence humaine et de la singularité des individus. Il propose des réponses adaptées aux freins susmentionnés. La charte de sécurité intègre différents éléments permettant la préservation de la sécurité du système d'information de l'entité. Elle est écrite de manière à faire de l'utilisateur un acteur essentiel à la réussite du projet.
Activité 4: Management des hommes et des équipes dans un contexte de pilotage de chantiers cyber A4.1 Identification des besoins en compétences nécessaires au déploiement de projet IT / Cyber	C4.1 Evaluer l'adéquation entre les compétences des collaborateurs d'une DSI et/ou d'une équipe projet cyber et le besoin en compétences nécessaires au soutien des besoins fonctionnels et stratégiques IT de manière à déployer un plan de développement de compétences, de formation, et/ou de recrutement	**Etude de cas :** Dans le cadre d'une étude de cas portant sur une entreprise réelle ou fictive, le candidat doit émettre des préconisations pour améliorer l'organisation des ressources humaines à l'échelle d'une direction IT et/ou d'une équipe projet cyber	Le/la candidat(e) évalue justement le besoin en compétence de l'organisation en prenant en compte les spécificités de l'organisation et les orientations stratégiques. Il propose des modifications pertinentes pour améliorer l'organisation des ressources humaines au sein de l'entreprise. La planification est réaliste au regard des résultats du diagnostic cyber/audit préalablement réalisés et des ressources disponibles.

A4.2 Recrutement des membres d'une direction IT et/ou d'une équipe projet cyber	C4.2 Organiser des entretiens de recrutement (interne et externe) adaptés aux postes à pourvoir, en collaboration avec la direction des ressources humaines, en veillant à la non-discrimination des candidats (notamment liée au handicap), afin de renforcer une direction IT et/ou une équipe projet cyber	**Etude de cas :** Dans le cadre d'une problématique rencontrée par une entreprise réelle ou fictive, le candidat doit proposer un processus de recrutement incluant a minima une fiche de poste (présentation des activités et compétences attendues, …) d'un métier de l'IT et/ou de la cybersécurité, ainsi que les canaux de recrutement. Le candidat devra démontrer qu'il intègre les règles d'inclusion du handicap dans sa façon de rédiger l'offre et d'adapter son entretien.	Il/elle sélectionne les modes et canaux de recrutement adapté *(réseaux pro, identifications d'écoles spécialisées, …)* Il/elle propose un processus de recrutement exhaustif et réaliste comprenant l'identification du périmètre, la conduite de l'entretien et l'onboarding. Les activités et compétences à maîtriser sont écrites de façon claire et intelligible au sein d'une fiche de poste. Le candidat est inclusif. Il n'utilise pas de critère de nature discriminante lors de l'entretien.
A4.3 Supervision de la réalisation des objectifs individuels et collectifs A4.4 Animation de réunion d'équipe auprès d'une direction IT et/ou d'une équipe projet cyber	C4.3 Accompagner les collaborateurs dans la définition et la réalisation de leurs objectifs individuels et collectifs dans le respect des obligations légales et contractuelles en : - Evaluant le niveau de compétences et de motivation, - Capitalisant sur les résultats des entretiens individuels d'évaluation et entretiens professionnels, - Organisant des réunions d'équipe rappelant les actions, les objectifs et les moyens nécessaires,	**Etude de cas :** Dans le cadre d'une étude de cas portant sur une entreprise réelle ou fictive, le candidat doit déterminer les objectifs individuels de collaborateurs pour répondre à la stratégie de développement d'une BU. Il/elle propose une recommandation dans le cadre d'une résolution de conflit.	Le/la candidat(e) identifie correctement les objectifs globaux de l'organisation, ainsi que les indicateurs associés. Il/elle élabore un premier scenario pour la fixation individuelle des objectifs de performance.

	- Résolvant les problèmes d'organisation et les conflits éventuels, - En veillant à l'adaptation de leur poste de travail notamment pour les publics en situation de handicap		Il/elle propose un plan réaliste pour l'accompagnement à l'appropriation de ces objectifs par l'équipe. Le candidat identifie la problématique sous-jacente. Il/elle propose un plan de résolution de conflit adapté à la situation.
A4.5 Délégation de tâches, missions et responsabilités aux membres d'une direction IT et/ou d'une équipe projet cyber	C4.4 Mettre en œuvre un management de délégation en définissant des objectifs SMART, les méthodes et les modalités de mise en œuvre ainsi que les indicateurs de performance afin de renforcer l'efficacité collective dans le cadre du déploiement de projet IT / cyber	**Etude de cas :** Dans le cadre d'une étude de cas portant sur une entreprise réelle ou fictive, le candidat doit déterminer les missions et responsabilités délégables et le processus de délégation mis en œuvre.	Le candidat identifie les tâches, missions et responsabilités pouvant être déléguées et justifie son choix. Les objectifs identifiés sont SMART (spécifique, mesurable, atteignable, réalisable et temporellement défini) Il sélectionne des indicateurs de performance adapté, permettant de contrôler l'atteinte des résultats. Son processus de délégation comprend une phase de contrôle et une phase d'évaluation. La phase d'évaluation doit se baser sur le recueil et l'exploitation d'éléments permettant d'expliciter les raisons de l'atteinte ou non des objectifs initialement prévus.

Activité 5.A - option conseil & la recherche 5A.1 Identification d'une problématique de recherche en cybersécurité 5A.2 Proposition de solutions innovantes et créatrices de connaissances, de technologies et de valeur, de nouvelles approches, de nouvelles méthodes	C5.A1 Concevoir et piloter un projet de recherche scientifique en matière de cybersécurité, en autonomie et/ou en partenariat avec des pairs au sein de son organisation ou d'un laboratoire, de manière à renforcer les échanges entre les laboratoires de recherche et les milieux socio-économiques et contribuer au processus d'innovation	**Mémoire** Le candidat doit rédiger un mémoire de recherche en lien avec une problématique professionnelle. Dans ce cadre, le candidat doit : 1) Identifier une problématique qui contribue au développement de produits, de procédés ou de services innovants en matière de cybersécurité, 2) Présenter une méthodologie de recherche scientifique en documentant l'ensemble des travaux réalisés 3) Présenter et analyser l'état de l'art portant sur les aspects techniques et/ou règlementaires d'une problématique de cybersécurité 4) Emettre des préconisations permettant de valoriser et	Le candidat démontre sa capacité à mobiliser différents champs scientifiques, techniques et académiques au service d'une problématique de sécurité. Démontre la pertinence de sa méthodologie de recherche au regard des objectifs recherchés. Démontre la pertinence et la fiabilité des sources utilisées. Les principaux articles de recherche et d'ouvrages fondamentaux abordant le thème sont cités et analysés. Il démontre sa connaissance technique des bonnes pratiques, de l'état de l'art, et des normes réglementaires régissant l'activité (en particulier le droit du numérique (RGPD / Secret des Affaires / Réponses Pénales / Atteintes à la Réputation / INFOX …). Respect des attendus et contraintes de la construction du savoir scientifique en

		capitaliser sur les résultats obtenus	matière de méthode et de restitution des résultats.
5A.3 Rédaction d'une réponse à un appel d'offre 5A.4 Evaluation des moyens humains, techniques et organisationnels nécessaires à la réalisation de l'appel d'offre	C5.A2 Répondre à des appels d'offre de marché public, et auprès d'entreprises privés, en : - présentant l'organisation et démontrant son expertise sur la problématique de travail, son éthique et sa dimension RSE, - précisant le mémoire technique (analyse, méthodologie…) , - évaluant l'offre de prix en partenariat avec les équipes commerciales, De manière à développer le CA de l'organisation et de décrocher de nouveaux marchés	**Mise en situation professionnelle :** Le candidat doit constituer une réponse à un appel d'offre portant sur un besoin en cybersécurité.	Le candidat respecte le formalisme de la réponse à un appel d'offre. Il propose des tarifs réalistes par rapport à la nature de sa proposition. Pour se faire, il justifie son positionnement prix en fonction de la qualité, les délais attendus, l'expertise technique apportée… Le candidat explicite ses éléments de différenciations par rapport aux entreprises existantes qui se positionnerait sur ce marché. Le candidat réalise une proposition technique réaliste et de qualité, cad qu'il intègre à la fois une évaluation des moyens humains (nombre, expertise technique, type de mission…), les moyens techniques (solution SI, cryptographie…), et organisationnel (mesure de sécurité, contrôle qualité, politique RSE).

5A.4 Conseil stratégique en matière de cybersécurité	C5.A3 Emettre des recommandations et préconisations portant sur la définition et le déploiement d'une stratégie de cybersécurité et de conformité (à une réglementation, à des référentiels d'exigences) auprès de clients externes, en veillant à l'évaluation du budget nécessaire à la réalisation de la prestation	**Dossier de consulting** A partir d'un cas d'entreprise, portant sur un la définition et le déploiement d'une stratégie de cybersécurité, le candidat analyse la problématique et détermine des pistes de solutions adaptés aux enjeux clés de l'organisation	Les méthodes et/ou outils de collecte et de gestion de données permettant de réaliser le diagnostic de la problématique cybersécurité sont adaptés à la nature de la demande et de l'entreprise. Les sources de création de valeur en matière de cybersécurité sont mises en perspectives au regard des risques associés pour l'entreprise. Plusieurs pistes de solutions sont explorées et les potentialités sont bien identifiées (à minima 2) L'évaluation comprend une analyse stratégique sur différents champs (réglementaire, environnemental, socio-économique, géopolitque…) susceptibles d'impacter l'entreprise.
Activité 5.B – option audit & la gestion d'incident de sécurité 5B.1 Identification des enjeux et du contexte de la cybermenace 5B.2 Réaliser une veille sur les menaces émergentes, et les	C5.B1 Piloter les activités de renseignement en matière de cybersécurité d'une organisation en collectant, qualifiant, organisant, recoupant et analysant diverses sources de données (*dark web, renseignements open source, média sociaux, CERT, etc*.) de manière à anticiper les risques et attaques cybersécurité	**Dossier professionnel** Basé sur une entreprise réelle, le candidat doit réaliser un dossier professionnel intégrant une veille complète pour identifier les enjeux cybersécurité selon le contexte dans lequel se trouve l'entreprise.	Le candidat démontre sa capacité à mobiliser différents champs scientifiques, techniques et académiques au service d'une problématique de sécurité. Démontre la pertinence et la fiabilité des sources utilisées, et notamment des informations collectées sur le darkweb,

nouvelles évolutions en matière de cybersécurité			open source ou les médias sociaux. Il qualifie le degré de fiabilité de chacun des sources. Le regroupement d'information et l'analyse qu'il en produit permet de détecter des signaux faibles en matière de cybersécurité. Il démontre sa connaissance technique des bonnes pratiques, de l'état de l'art, et des normes réglementaires régissant l'activité (en particulier le droit du numérique (RGPD / Secret des Affaires / Réponses Pénales / Atteintes à la Réputation / INFOX …).
5B.3 Analyse des techniques d'attaques et les modes opératoires connus 5B.4 Amélioration des capacités de détection	C5.B2 Piloter le système d'amélioration continue des moyens de détection, en : - capitalisant sur les activités de renseignement préalablement mené, - en produisant des documents d'analyse permettant l'alimentation des outils de détection, - en capitalisant sur les apprentissages générés lors de précédents incidents ou de crises de cybersécurité	**Dossier de consulting** Basé sur une entreprise réelle, le candidat doit présenter son système d'amélioration continue des moyens de détection. Il doit produit des documents d'analyse concernant les outils de détection de cyberattaques.	Les indicateurs permettant de calculer le ROI de chaque action d'amélioration continus définis sont simples, objectifs mesurables et adaptés à une évaluation de la performance et de la qualité (efficacité et efficience) de l'action menée. Des valeurs de références sont définis pour chaque indicateur afin d'évaluer la situation de départ et celle d'arrivée au regard de la stratégie de cybersécurité L'outil d'analyse de données proposé permet de traiter les informations de

			manière automatique et rapide et de mettre en évidence les axes d'amélioration à prévoir (outils de traitement de données technologiques,…) en capitalisant sur les activités de renseignement. Les documents d'analyse produits sont qualitatifs (lisibilité, forme, rédaction…)
5B.5 Animation d'une cellule de crise décisionnelle et contribution aux cellules de crise opérationnelles 5B.6 Coordination de l'action des différentes parties en présence et la diffusion des informations vers les parties prenantes	C5.B3 Piloter une cellule de crise décisionnelle et contribuer aux cellules de crise opérationnelles en : - organisant et d'articulant un dispositif global de gestion de crise - analysant la situation et évaluant les conséquences pour l'entreprise, - délimitant les périmètres de chaque cellule et le rôle de chaque interlocuteur de manière à solutionner la crise en limitant ses impacts.	**Mise en situation professionnelle :** Dans le cadre d'une cyberattaque au sein d'un simulateur de cyberattaque, le candidat doit réunir et piloter une cellule de crise décisionnelle.	Le candidat doit inclure dans son pilotage de cette crise une rotation des équipes qui traitent l'incident et des acteurs de la cellule de crise. Dans le cadre de cette cellule de crise décisionnelle, le candidat identifie des experts internes ou externes qu'ils conviendraient d'inviter. Le candidat pose les bonnes questions pour identifier les impacts de l'attaque sur le/les métiers concernés et évaluer les risques. Le candidat propose des mesures palliatives pertinentes au regard du contexte dans lequel s'inscrit la crise pour sa résolution.

Activité 5.C – option conception & maintien d'un système d'information sécurisé 5C.1 Définition d'une architecture cybersécurisée	C5.C1 Elaborer une architecture cybersécurisée en intégrant des solutions d'acquisition, de traitement et de stockage de données, de détection de programmes malveillants et de menaces de manière à détecter en temps réel des incidents en cybersécurité	**Mise en situation professionnelle :** Dans le cadre d'une mise en situation professionnelle, le candidat doit concevoir une architecture cybersécurisée --- *Lorsqu'un candidat se présente uniquement sur un bloc de compétences (capitalisation de bloc), la modalité est amenée à évoluer. Dans ce cadre, le candidat doit présenter un « dossier professionnel » reprenant l'ensemble des éléments précités. Les critères restent les mêmes.*	La stratégie de collecte des journaux d'événements définit les règles de collectes et de traitement. Les règles de collectes sont correctement définies. Elles permettent de retracer les actions du système. Les règles, politiques et procédure de corrélations sont définies. Elles permettent d'analyser les journaux d'événements. Les menaces à la sécurité du système d'information sont détectées et qualifiées. Les informations et les évènements relatifs à la sécurité sont correctement gérés grâce à la solution de sécurité. Les règles de corrélation permettent d'identifier l'événement ayant généré les suivants. La configuration de la solution de sécurité SIEM permet d'obtenir une visibilité sur les activités au sein de l'environnement informatique, de détecter les failles, et d'en contrôler la conformité.

5C.2 Codage et intégration de solution technique, organisationnel et de contrôle d'accès	C5.C2 Développer des solutions techniques, organisationnelles et de contrôle des accès, et les intégrer au sein d'un SI de manière à protéger le réseau de la corruption des données	**Mise en situation professionnelle dans la salle de Simulation Cyber du Groupe Galileo Education au sein du Cybercampus** Dans le cadre d'une mise en situation professionnelle, le candidat doit développer une nouvelle solution / fonctionnalité à intégrer dans un SI existant de manière à répondre aux besoins du commanditaire.	L'ensemble des fonctionnalités programmées fonctionne. Les standards d'usage du langage informatique utilisés sont respectés. Le code est suffisamment clair pour se passer de commentaire sur l'intention de la programmation (ce que fait le code). Le code est suffisamment commenté pour comprendre son fonctionnement et permettre les évolutions futures. Le code ne présente pas de faille de sécurité connue. Les solutions techniques, organisationnelles ou de contrôles des accès réalisés s'insèrent bien dans le SI global.
5C.4 Planification d'actions correctives et préventives	C5.C3 Planifier des actions correctives et préventives suite à l'identification d'un incident cybersécurité en adoptant une approche DevSecOps de manière à remédier à la situation et de limiter le risque de reproduction de cette faille	**Mise en situation professionnelle dans la salle de Simulation Cyber du Groupe Galileo Education au sein du Cybercampus,** le candidat doit	Les actions correctives proposées sont pertinentes au regard du diagnostic réalisé. Les actions permettent de couvrir l'ensemble des impacts (réputation, perte de données, rgpd, conséquences civiles et pénales éventuelles…)

		-Proposer des actions correctives permettant de résoudre l'incident sécurité, -Proposer des actions préventives pour éviter le risque de reproduction de cet incident.	Le candidat démontre sa capacité à prendre du recul afin de proposer des actions préventives pour capitaliser sur les apprentissages tirés de l'incident en cours et éviter qu'ils ne se reproduisent Démontre sa capacité à adopter une approche devops dans la résolution d'une problématique nécessitant une intervention sur l'architecture technique.