5 - REFERENTIELS

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.* »

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. Conception de la stratégie de sécurité du système d'information et conseil à la gouvernance			
A1.T1 Analyse de la sécurité du S.I existant	**A1C1. Étudier** le système d'information d'une structure dans sa globalité, en identifiant les points faibles du système, afin d'évaluer le niveau de sécurité au sein de l'organisation	**Epreuve I** **Mise en situation professionnelle reconstituée (MSPR)** **Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat doit être capable de rédiger d'une façon claire et précise une synthèse du : • Le cadre stratégique qui définit la stratégie de l'entreprise en matière de S.I (l'analyse du schéma directeur informatique est cohérent par rapport aux concepts abordés dans le document) • La politique de sécurité, définissant les règles générales de sécurité de l'entreprise (l'interprétation d'un référentiel général de sécurité (PSSI) est correcte par rapport aux informations produites dans le document) • Le cadre commun d'urbanisation définissant la démarche d'urbanisation (la réalisation de la cartographie est juste et représente les 4 vues du S.I de l'entreprise) • Le cadre commun d'interopérabilité (La production de la liste des cohérences techniques est exhaustive et comporte : normes, standards et règles d'architecture applicables)
	A1C2. Identifier les enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation et vis-à-vis des tiers et sous-traitants et les exigences de conformité légale afin de garantir à l'entreprise d'être en conformité vis à vis de la règlementation française en matière de droit	**Epreuve I** **Mise en situation professionnelle reconstituée (MSPR)**	Le candidat doit être capable de réaliser les actions suivantes : • La liste complète de chaque sous domaine de la sécurité d'un S.I est présentée et comporte les éléments suivants : processus,

	informatique ainsi que la bonne mise en application des normes et certifications du domaine	**Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	régularité, application, projet, respect de la législation • Pour chaque sous domaine présent dans sa liste, il présente les principaux enjeux et risques associés • Il porte une appréciation sur la capacité de l'organisation en terme du corpus minimal mis en place en vue d'assurer la conformité règlementaire de son S.I (politique du S.I, politique de sécurité du S.I, charte d'utilisation, la documentation informatique à jour, la sécurité des développements informatiques, la gestion rigoureuse des droits d'accès au S.I)
	A1C3. Décliner les axes et les objectifs stratégiques en matière de sécurité informatique et cybersécurité afin de sensibiliser la Direction générale au sujet et lui permettre de vérifier sa bonne correspondance avec la stratégie de développement de l'entreprise	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR)** **Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat doit être capable de présenter un reporting régulier et complet. Ce reporting comporte des éléments indispensables sur les axes et objectifs en sécurité : • Les failles potentielles de l'entreprise, qu'elles soient internes (comportement des collaborateurs, architecture des sites et des outils) ou externes (prestataires de paiement, fournisseurs d'internet) • Rançongiciel ou ransomware • Le Maliciel • L'ingénierie social • L'hameçonnage ou pishing
A1.T2. Définition de la stratégie de sécurité et cybersécurité	**A1C4. Définir** la feuille de route stratégique adaptée aux besoins et à la culture de la structure, en lien avec les parties prenantes (informaticiens et les responsables des services) concernés afin de répondre à des objectifs de sécurité métiers et IT stratégiques face à l'augmentation de la cybermenace	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR)** **Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur**	Le candidat doit être capable de présenter une feuille de route de sécurité S.I détaillant : • Facteurs clés de succès dépendant de la spécificité de l'entreprise (la maturité informationnelle de l'entreprise, la qualité des données, le respect de délais en développement…) • Politique de sécurité adéquate (charte de sécurité proposée aux acteurs de l'entreprise, les règles de sécurité appliquées au SI de l'entreprise…)

		Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn **15 min de présentation de la réalisation en groupe** **15 min d'entretien individuel (questions en lien avec les compétences)**	• Une démarche globale de l'organisation de la sécurité en adaptation avec la structure de l'entreprise (Classification et contrôle des actifs, Sécurité du personnel, gestion des communications et des opérations, Gestion des identifiants et des mots de passe, Contrôle des accès, Développement et maintenance des systèmes)
	A1C5. Définir une stratégie de mise en conformité en lien avec la règlementation RGPD et le droit informatique afin de proposer un descriptif du process de la sécurité tenant compte de ce paramètre et ainsi, faciliter les relations avec les autorités de régulation en cas de contrôle réglementaires (auditeur RGPD et CNIL principalement)	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR) Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de rédiger d'une façon claire et précise une stratégie pour la conformité aux exigences légales et réglementaires : Un document détaillant : • Le process de protection des données personnelles proposé • Un process de respect de la propriété intellectuelle proposé • Un process de conservation de l'information proposé • Un process d'audits de sécurité réguliers proposé L'ensemble des éléments proposés sont conforme à la règlementation en vigueur et tiennent compte des grands concepts en droit informatique
	A1C6. Définir les mesures organisationnelles et techniques permettant de minimiser les risques liés à la sécurité du système d'information dans le but d'assurer une protection optimale et appropriée des données de l'entreprise et atteindre ainsi les objectifs de sécurité définis par la gouvernance	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR) Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur**	Le candidat doit être capable de proposer une liste d'indicateurs de qualité couvrant : • Mesures organisationnelles liées à l'entourage du S.I • Des mesures assurant : la sécurité des locaux, la sécurité des salles de serveurs, la sécurité des places de travail, l'identification et l'authentification des utilisateurs l'accès aux données des utilisateurs gérer les accès à distance… • Mesures techniques, directement liées au système d'information

		Phase II-Production écrite individuelle à réaliser	• Des mesures assurant : la sécurité du stockage, de traitement du transfert des données (réseaux systèmes, applications, chiffrement, signatures…)
	A1C7. Définir l'organisation de la cybersécurité en proposant une charte de sécurité informatique de l'organisation afin de sensibiliser régulièrement les équipes et évaluer leurs connaissances en matière de règle de sécurité informatique	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR) Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn**	Le candidat doit être capable de rédiger un document à portée juridique détaillé et complet : • Le périmètre de la charte informatique • Les règles d'usage de la sécurité informatique • Les règles d'usage de la messagerie • Les mesures de contrôle • Les sanctions qui peuvent être appliquées • L'opposabilité de la Charte informatique La présentation de document doit être précise et synthétique de manière à clarifier les informations clés du document
	A1C8. Concevoir un référentiel SSI de l'organisme (schéma directeur, meilleures pratiques, directives internes…) permettant de formaliser, de justifier les choix, de légitimer les plans d'action et de garantir la cohérence avec le contexte particulier de l'organisme	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR) Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat doit être capable d'élaborer un document détaillé de la politique de sécurité d'un S.I en se basant sur le guide proposé par la DCSSI de l'ANSSI qui présente : • Liste les principes de sécurité • Liste la politique et les règles de sécurité à mettre en place • Liste les documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires...). Le document proposé est complet et conforme aux préconisations de l'ANSSI
A1.T3. Conseil et veille stratégique auprès de la gouvernance	**A1C9. Conseiller** l'organisation en proposant des préconisations et des recommandations sur l'amélioration du niveau de sécurité afin de lui permettre une meilleure compréhension des enjeux et risques de cybermenaces et augmenter sa capacité de gestion de crises	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR)**	Le candidat, en se basant sur les Directive Network and Information Security (NIS) de l'ANSSI et selon le besoin du S.I en sécurité est capable de citer • Recommandations à l'état de l'art

		Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur **Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn**	• Recommandation alternative de premier niveau • Recommandation alternative de second niveau • Recommandation renforcée complémentaire La présentation est soutenue en anglais technique et parfaitement compréhensible.
	A1C10. Informer les directions générales et les directions métiers sur les enjeux de la sécurité informatique, cybersécurité et l'état de la menace afin de les sensibiliser sur l'évolution du contexte de la sécurité et la cybersécurité en utilisant des supports de communication inclusifs	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR)** **Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn**	Le candidat est capable de proposer sous forme d'un serious game ou jeu de rôles sur la thématique de la cyber attaques. Il présente les éléments suivants : • Des présentations et des documents permettant de développer une culture interne "cybersécurité" • Panorama de la cyber menace • Une synthèse claire qui permet d'acquérir les bonnes pratiques SSI • Des exemples de la création de mots de passe forts en passant par l'ingénierie sociale Le candidat responsabilise chacun en attribuant des rôles aux membres du jury (hackers, responsable métier, un RSI, utilisateur final) La conception de l'exercice doit être de qualité : Rythme, contenu, différentes actions et présentant une pédagogie progressive
	A1C11. Apporter une expertise juridique auprès de la gouvernance en matière de conformité (à une règlementation, à des référentiels d'exigences) afin de fournir aux dirigeants des entreprises les règles et les bonnes pratiques à applique faces aux nouvelles exigences en matière de conformité règlementaire	**Epreuve I- Mise en situation professionnelle reconstituée (MSPR)** **Analyse et conseil d'une politique de sécurité informatique d'une structure à partir d'une**	Le candidat doit être capable de rédiger un document qui représente les éléments de veille juridique en lien avec le contexte de l'entreprise. Il tient compte de la réglementation quelle que soit la filiale et propose des documents conformes aux exigences des lois et des décrets

		situation réelle ou reconstituée proposée par le certificateur **Phase II-Production écrite individuelle à réaliser**	Les documents présentent une belle aisance rédactionnelle et présentent les éléments techniques

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**
A2. Pilotage de projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante			
A2.T1. Management d'équipe interne et externe à l'entreprise	**A2C1. Identifier** l'ensemble des étapes de réalisation du système d'information pour organiser le projet en tâches et livrables en répartissant les activités en fonction des ressources humaines (tous profils confondus), techniques et financières à mobiliser	**Epreuve II Mise en situation professionnelle reconstituée (MSPR) Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser** **Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn** **15 min de présentation de la réalisation en groupe** **15 min d'entretien individuel (questions en lien avec les compétences)**	Le candidat est en capacité de présenter l'organisation du projet en précisant les points suivants : • Le découpage du projet en actions à entreprendre/activités • L'organisation : les tâches, l'enchainement de celles-ci, les ressources à affecter pour chacune d'entre elles • Les objectifs délais : dates début, lancement, jalons • Les objectifs coûts : budget alloué dans sa globalité et par ressource Résultats attendus : Graphe PERT ou Graphe d'ordonnancement des tâches (au choix du candidat) précisant les ressources matérielles, humaines, la durée et les délais par tâche ainsi que le chemin critique Le candidat doit être capable de proposer des planning avec une prise en compte des aménagements liés aux 6 grandes familles de handicap : visuel, mental, invalidant, psychique, moteur et auditif
	A2C2. Concevoir les cahiers des charges technique et fonctionnel d'un projet de développement S.I. à l'aide des besoins utilisateurs collectés afin de cadrer le développement	**Epreuve II Mise en situation professionnelle reconstituée (MSPR) Gestion d'un projet de mis en place d'une stratégie de sécurité et**	Le candidat présente un cahier des charges techniques qui contient : • Les objectifs • Les ressources planifiées • Les outils d'évaluation • La mise en œuvre.

		cybersécurité pour une structure proposée par le certificateur Phase II-Production écrite individuelle à réaliser	Le candidat présente un cahier des charges fonctionnel qui contient : • Les objectifs des directions métiers • Les fonctionnalités • Les indicateurs de performance • Les dates clés des livrables
	A2C3. Piloter les prestataires extérieurs éventuels gérant les ressources informatiques d'un système d'information existant listées dans la cartographie établie afin de sécuriser la mise en œuvre technique	**Epreuve II Mise en situation professionnelle reconstituée (MSPR) Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur Phase II-Production écrite individuelle à réaliser**	Le candidat est en capacité de présenter un tableau de bord précisant les éléments suivants : • Coordonnées des prestataires • Nature des prestations • Type de prestation : niveaux de services (niveaux SLA) • Dates et durée des contrats de prestation • Les indicateurs de performance retenus pour le suivi de chacun des prestataires : Il précise les pénalités associées qui doivent être en cohérence avec les SLA (niveau de service) • Fréquence du suivi : journalier, hebdomadaire, mensuel Le candidat démontre une utilisation appropriée d'un tableur pour concevoir son tableau de bord avec utilisation : • De calculs complexes • De tableaux croisés • De graphiques pour argumenter son analyse Le résultat attendu de ce tableau de bord correspond aux attendus d'un tableau de suivi de performance en tant que manager
	A2C4. Établir des tableaux de bord de suivi de performance (qualitative et quantitative) de l'ensemble des ressources allouées à chaque étape-projet pour anticiper, visualiser et corriger les écarts en temps réel afin de limiter les contraintes de ressources et les retards	**Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur**	Le candidat est capable d'outiller le suivi de son projet : • Il présente un diagramme de Gantt conforme

		Phase II-Production écrite individuelle à réaliser	• Il propose des indicateurs quantitatifs et qualitatifs (productivité, performance, qualité de la fonctionnalité...) • Il utilise un outil de planification de tâches (type MS Project, Trello…) • Il propose une organisation des réunions de suivi cohérente avec la mise en place d'un projet agile (DailyMeeting)
A2.T2. Gestion de projet selon une démarche agile	**A2C5. Gérer** un projet agile en utilisant les méthodes et outils adaptés à ce mode de fonctionnement pour tester, modifier et procéder par itération afin de réduire les délais de remise des projets de développement S.I.	**Epreuve II Mise en situation professionnelle reconstituée (MSPR) Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de gérer un projet agile de A à Z : • Choix de la méthode agile appropriée (Scrum, FDD, Lean Software, Kanban) • Il met en place un outil de communication pour échanger avec les acteurs du projet (Slack, GitHub…) • Il utilise de façon approprié un outil de centralisation des tâches (Jira, Trello…)
	A2C6. Conduire une équipe projet en diffusant les fondamentaux de l'agilité : adaptation, flexibilité et amélioration continue au sein de l'équipe afin d'être en mesure d'absorber les changements de priorité qui peuvent intervenir dans un contexte de forte contrainte de temps et d'incertitudes	**Epreuve II Mise en situation professionnelle reconstituée (MSPR) Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de gérer une situation difficile • Il attribue les rôles à chaque acteur du projet • Il propose un processus agile avec plusieurs scénarios possibles • Son organisation tient compte des contraintes de temps et des évènements exceptionnels • Il prévoit au sein de son équipe une personne relais en cas de situation d'urgence
	A2C7. Proposer des solutions innovantes afin de favoriser les interactions et l'inclusion au sein de l'équipe et d'anticiper des conflits de travail liés aux malentendus multiculturels et des profils en situation d'handicap	**Epreuve II Mise en situation professionnelle reconstituée (MSPR)**	Le candidat est capable d'imaginer et de proposer des situations de rencontres et d'échanges interculturelles, il cite à

		Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur **Phase II-Production écrite individuelle à réaliser**	minima trois solutions favorisant les échanges : • Serious game à distance • Temps de partage informel (petit déjeuner, séminaire…) • Webinaire sur les thématiques culturelles (mentalités, tabous, éthiques…) Le candidat doit proposer une stratégie d'accueil aux handicaps afin de favoriser l'inclusion des profils en situation de handicap au sein de l'équipe et permettre leur pleine intégration, en collaboration avec le référent handicap de l'entreprise
A2.T3. Accompagnement de l'équipe en favorisant un processus de communication adéquat	**A2C8. Accompagner** l'équipe dans l'appropriation du travail à distance ou du télétravail en proposant des solutions managériales afin de favoriser la motivation et la résilience et permettre ainsi de préserver équilibre entre vie professionnelle/vie privée dans un souci de productivité et de bien-être	**Epreuve II Mise en situation professionnelle reconstituée (MSPR)** **Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat propose un plan d'accompagnement de l'équipe à distance : Le candidat est capable • De formuler les besoins et contraintes de son service • Le candidat structure le contenu des points journaliers et/ou hebdomadaires • Le calendrier des échanges tient compte des décalages horaires/ organisations des équipes à l'étranger et des vie privée des collaborateurs • Le candidat propose des missions en accord avec les intérêts professionnels de ses collaborateurs en s'appuyant sur l'analyse d'un test de motivation (Motiva, application web sur l'emploi store via la plateforme Pole emploi, …)
	A2C9 : Concevoir un processus de communication inclusif régulier au sein de l'équipe afin de synchroniser les activités quotidiennes et mettre en place un fil de discussion à l'aide d'outils numériques	**Epreuve II Mise en situation professionnelle reconstituée (MSPR)** **Gestion d'un projet de mis en place d'une stratégie de sécurité et**	Le candidat propose une stratégie d'organisation du partage d'informations : • Il propose des outils numériques adaptés

		cybersécurité pour une structure proposée par le certificateur **Phase II-Production écrite individuelle à réaliser**	• Il propose des schémas d'utilisations des outils • Il propose une présentation du schéma d'organisation à l'aide d'un outil numérique (powerpoint, caneva, ...) • Il proposer un ensemble de règles • de bonnes pratiques , des outils permettant l'inclusion des profils en situation de handicap •
	A2C10. Communiquer avec l'équipe en adoptant les modes de communication adéquats selon les cultures et la langue des collaborateurs afin de garantir l'intégration de tous les membres de l'équipe	**Epreuve II Mise en situation professionnelle reconstituée (MSPR)** **Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur** **Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn** **15 min de présentation de la réalisation en groupe** **15 min d'entretien individuel (questions en lien avec les compétences)**	Le candidat présente rapidement en anglais la culture d'un pays au choix et fait preuve d'une qualité orale dans sa présentation Lors du questionnement du jury il fait preuve d'écoute active • Le candidat reformule de façon fidèle les dires de son interlocuteur sans interprétation • Dans sa reformulation, le candidat s'appuie sur une des références culturelles du pays présenté
	A2C11. Animer des réunions à distance afin de maintenir une dynamique de groupe et renforcer l'esprit d'équipe des membres en télétravail et/ou à distance	**Epreuve II Mise en situation professionnelle reconstituée (MSPR)** **Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur** **Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn**	Le candidat est capable de présenter un support d'animation La séquence d'animation proposée est structurée • Il a conçu des séquences d'animation interactive • Il propose les outils digitaux de communication qu'il juge appropriée (padlet, kahoot,

		15 min de présentation de la réalisation en groupe **15 min d'entretien individuel (questions en lien avec les compétences)**	Klaxoon…) permettant l'inclusion numérique
	A2C12. Concevoir un processus de partage d'information afin de faciliter la collaboration entre les membres (tous profils confondus) en télétravail et/ou à distance en utilisant des outils numériques	**Epreuve II Mise en situation professionnelle reconstituée (MSPR)** **Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat propose une stratégie d'organisation du partage d'informations : Il propose une présentation du schéma d'organisation à l'aide d'un outil numérique (powerpoint, caneva, ...) Il propose des outils qui permettent l'inclusion numérique

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**
A3. Déploiement d'une architecture fonctionnelle et technique en vue de renforcer la sécurité du S.I et faire face aux cybermenaces			
A3.T1. Organisation d'une architecture fonctionnelle de sécurité informatique et cybersécurité	**A3C1. Assurer** la mise en place des structures organisationnelles des plans d'actions de sécurité au sein des entités afin de garantir la protection de données et le niveau de sécurité du système d'information	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de mettre en place une structure organisationnelle de la sécurité de S.I • Il propose un organigramme complet d'une structure dédiée à la gestion de la sécurité de l'information : Exemple un comité sécurité ou un responsable de la sécurité du système d'information (RSSI) en lien avec différents correspondants sécurité dans les unités. Il présente la structure d'encadrement du système d'organisation conçu • Il définit les règles formelles, les procédures et le processus de son plan d'action fonctionnel
	A3C2. Paramétrer les mesures organisationnelles permettant la surveillance de la sécurité globale d'une organisation (des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques) afin d'assurer la mise en place d'un SOC (Security Operation Center)	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de paramétrer : • Des procédures d'autorisation de matériels ou logiciels conformes à la stratégie de sécurité informatique • Des procédures applicables à l'accès aux informations de l'organisation par des tiers cohérent avec le plan d'action • Les dispositifs prévus incluent l'implication des employés (participation des agents à la conception des dispositifs techniques et des règles du plan d'action)

	A3C3. Déployer les mesures organisationnelles de sécurité en se basant sur la stratégie de sécurité informatique de l'organisation afin d'assurer le fonctionnement opérationnel et les maintenir à l'état de l'art	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de déployer des procédures : • Il établit un inventaire détaillé et hiérarchise les entités/ actifs par valeur pour l''organisation. • Il attribue pour tout actif important, un propriétaire • Il déploie un système de classification qui définit un ensemble approprié de niveaux de protection pour que chaque actif étudié
A3.T2. Déploiement d'une architecture technique de sécurité/ cybersécurité	**A3C4. Déployer** des architectures et ou des solutions de sécurité de la couche matériels et logiciels de l'entreprise permettant de garantir l'évolutivité et la haute-disponibilité du système d'information	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase II-Production écrite individuelle à réaliser Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn 15 min de présentation de la réalisation en groupe 15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	Le candidat est capable de : • Déployer une architecture ou un outil centralisé pour pouvoir administrer à distance en cas de besoin (effacement, mises à jour, etc.) la couche matérielle de l'entreprise • Déployer une infrastructure selon le besoin de l'entreprise : ○ virtualisée ○ maximum de garantie d'évolutivité et de haute-disponibilité. • Installer une solution de mises à jour des logiciels • Des solutions qui améliorent la sécurité globale de votre architecture informatique L'administration de la sécurité système et réseaux fonctionne conformément à ce qui a été défini dans la politique de sécurité informatique

			Les paramétrages sont correctement réalisés et permettre de répondre aux objectifs
	A3C5. Piloter la procédure de paramétrage des politiques (habilitations) et configuration des droits d'accès appliqués sur son périmètre et vis-à-vis des tiers et des sous-traitants afin de garantir une utilisation sécurisée des moyens informatiques mis à disposition des utilisateurs finaux	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase II-Production écrite individuelle à réaliser Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn 15 min de présentation de la réalisation en groupe 15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	Le candidat est capable de proposer un descriptif du process de pilotage : • Il décline les étapes du process et propose des deadlines pour la mise en place de la politique de sécurité interne Il décrit un process régulier de contrôle en s'assurant du respect de la politique • Il propose un process de suivi de la gestion des mots de passe et un process de vérification les accès réseaux. • Il définit un process d'accès de sécurité en identifiant les différents outils informatiques • Le descriptif présenté est détaillé et conforme aux enjeux techniques. • Le processus doit être conforme au cadre légal de l'entreprise
	A3C6. Contribuer au pilotage de la mise en œuvre des outils et des solutions de sécurité autour des données de l'organisation et leur sauvegarde en fournissant une assistance technique et méthodologiques aux équipes informatiques afin de s'assurer de la pertinence des solutions/ outils choisis et participer lui-même à la bonne mise en place de la stratégie	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase II-Production écrite individuelle à réaliser Phase III -Soutenance orale sous forme d'une démonstration**	Le candidat est capable de • Réaliser une procédure de sécurisation des accès en rédigeant un document technique correspondant aux différents espaces de stockage de fichiers et documents structurée • Proposer une solution de sauvegarde régulière des données englobant une gestion large des problématiques récurrentes en entreprise et en capacité de traiter les fichiers clients, bases de données, mails, etc.

		technique devant un jury de professionnel Durée : 30 mn **15 min de présentation de la réalisation en groupe** **15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	• Paramétrer la solution de sauvegarde en ligne • Déployer un PRA (Plan de Reprise d'Activité) conforme et externalisé (second site)
	A3C7. Assurer le déploiement du programme et des initiatives cybersécurité dans l'ensemble des entités tout en respectant la cohérence globale et la coordination entre ces différentes entités afin que chaque entité s'approprie les nouvelles solutions/plateformes techniques et les services en cybersécurité dans une organisation.	**Epreuve III Mise en situation professionnelle reconstituée (MSPR)** **Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de mettre en place un process de déploiement, il doit définir : • Une planification prospective • Des ressources adéquates (Identifier l'équipe nécessaire pour mettre en œuvre la méthode de déploiement) • Une surveillance et une évaluation continue • Une communication solide Les éléments proposés sont conformes au concepts clés du plan d'action de la sécurité globale de l'entreprise
	A3C8. Assurer la mise en place d'un service de détection des incidents de sécurité SOC (Security Opération center) au sein de l'organisation afin d'évaluer le niveau de vulnérabilité et détecter des activités suspectes en prenant compte des exigences réglementaires	**Epreuve III Mise en situation professionnelle reconstituée (MSPR)** **Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser** **Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn**	Le candidat est capable de : • Paramétrer une plateforme de supervision et d'administration de la sécurité S.I (pare-feu, IPS/IDS, solutions de détection des brèches, surveillance de réseaux) Installer et paramétrer le SIEM (Security information Event Management) La plateforme fonctionne conformément à ce qui a été défini dans la politique de sécurité informatique Les paramétrages sont correctement réalisés et permettent de répondre aux objectifs

		15 min de présentation de la réalisation en groupe **15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	
	A3C9. Conduire des plans d'action sur la détection et la réaction aux incidents, en fournissant des informations pertinentes aux équipes afin d'assurer l'efficacité des outils de détection déployés dans le SOC	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser** **Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn** **15 min de présentation de la réalisation en groupe** **15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	• Le candidat est capable de proposer des actions sous forme de fonctionnalités et ou solutions pour une meilleure détection d'incidents • Un mécanisme de surveillance du système d'information et de détection des conditions d'incident est proposé • Il propose une liste d'outils de collecte des données concernant les incidents et des outils d'analyses sécurité Il décline le process que les experts doivent élaborer pour la mise en place des nouveaux scénarios de détection
A3.T3. Intégration de la Data science pour la détection et la prévention des menaces	**A3C10. Analyser** des données brutes issues de différentes sources (dark web, renseignement open source, média sociaux, CERT) en utilisant la data science afin d'étudier l'évolution des modes opératoires des hackers et ajuster ensuite sa stratégie de cybersécurité	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur**	Le candidat est capable de démontrer son process de collecte et d'analyse de données : • Il présente sa démarche méthodologique de collecte en s'appuyant un référentiel de signatures des attaques (sélection des sources de données liées à la cybersécurité,)

		Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn **15 min de présentation de la réalisation en groupe** **15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	• Il présente son process d'automatisation d'acquisition des données en utilisant de façon conforme des outils de type ETL ou web scarping • Il présente son analyse des données en utilisant des indicateurs statistiques (tendance, …) et ou des approches prédictives de machine learning pour une analyse comportementale des attaques
	A3C11 Renforcer les capacités de détection des activités malveillantes menaçant le système d'information en utilisant des solutions IA afin de réduire le risque des cybers attaques et rendre plus performant le SI de l'entreprise	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat présente une étude comparative des différentes solutions de détection des intrusions s'appuyant sur l'IA en mobilisant le process de veille technologique qu'il a construit. • Le référentiel proposé est exhaustif et rédigé en anglais technique
	A3C12. Proposer des nouvelles approches innovantes basées sur l'IA en s'appuyant sur une veille technologique et industrielle concernant les nouveaux produits et process métiers mobilisant de l'IA afin d'améliorer la procédure de prévention d'intrusion de l'organisation et réinterroger son dispositif interne en initiant la mise en place d'un processus d'amélioration continue efficace	**Epreuve III Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité/ cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn**	• À partir de la veille technologique réalisée, il présente d'une façon approfondie une solution innovante sélectionnée. • La présentation se déroulera en anglais technique

		15 min de présentation de la réalisation en groupe **15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE
Document présenté en annexe

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**
A4. Supervision, audit et gestion de la sécurité informatique et des cyberattaques			
A4.T1. Supervision et audit de la sécurité	**A4C1. Définir** les plans d'audits et de contrôles au sein de l'organisation afin d'évaluer la bonne application, l'efficacité et la conformité des politiques et procédures de sécurité de l'entreprise	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de définir des procédures de vérification et de contrôle contenant les modalités suivantes : • La disponibilité du système d'information • L'intégrité des données • La confidentialité des accès • Les documents qui permettent de savoir qui accède, à quel moment, à telle ou telle donnée ou application. L'ensemble de la production proposé par le candidat respecte la méthodologie de l'audit sécurité informatique
	A4C2. Mener des contrôles permanents et/ou périodiques de sécurité, notamment sur la base de revues documentaires, de collecte de preuves, d'accès aux consoles et aux rapports des outils de sécurité ou de l'utilisation d'outils automatisés de contrôle de conformité afin de mettre à jour le niveau de la sécurité du SI de l'entreprise	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou**	Le candidat est capable de réaliser : • Audit de l'infrastructure physique, du système, du réseau et de l'organisation Et Proposer • Des recommandations • Un plan d'action pour corriger les vulnérabilités et réduire les risques

		reconstituée proposée par le certificateur **Phase II-Production écrite individuelle à réaliser**	L'ensemble de la production proposé par le candidat respecte la méthodologie de l'audit sécurité informatique
	A4C3. Rédiger des rapports intégrant une analyse des vulnérabilités et écarts constatés ainsi que les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes et d'informer la direction générale de l'avancement du ou des projets de déploiement	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat doit être capable de rédiger d'une façon claire précise un rapport décrivant pour chaque menace : • Les vulnérabilités correspondantes • Les actifs à risque • L'impact sur l'infrastructure informatique • La probabilité d'occurrence • Les recommandations de contrôle. Le document proposé doit présenter la bonne utilisation d'un langage technique et démontrer une aisance rédactionnelle
	A4C4. Informer les équipes en charge de la sécurité des nouvelles menaces importantes et recommander des mesures tactiques pour les contrer en se basant sur sa veille technologique et son étude du marché afin d'impliquer l'ensemble des acteurs de l'entreprise et en particulier les directions métiers et ainsi favoriser la prévention des risques	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn** **15 min de présentation de la réalisation en groupe**	• Le candidat présente les modalités de communication qu'il juge pertinent dans le cadre de l'information sur les cybers menaces : • Il présente les outils de communication digitale tels que webinaire, google workspace… • Le candidat doit proposer des supports et des outils de communication qui favorisent l'inclusion numérique

A4.T2. Gestion des risques liés à la cybersécurité et accompagnement lors d'une cyberattaque		**15 min d'entretien individuel (questions en lien avec les compétences)**	
	A4C5. Analyser les risques de sécurité liés à l'introduction des nouvelles technologies en se basant sur une méthode d'analyse de risque optimisé afin d'atténuer les impacts sur le niveau de sécurité informatique d'une entreprise.	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat est capable de décrire un process d'analyse de risque des NTIC sur 6 niveaux • La sécurité organisationnelle • La sécurité physique • La continuité de service • L'organisation informatique • La sécurité logique et l'exploitation • La sécurité des applications Le candidat applique la méthodologie de l'analyse des risques de façon conforme. Le process proposé tient compte des préconisations de l'ANSSI. •
	A4C6. Assurer un appui opérationnel à la gestion de la cyber-crise avec les experts techniques, en cas d'incidents de sécurité majeurs, en coordonnant les équipes, afin d'agir de traiter tout actes malveillants impactant l'entreprise et mieux prévenir la cyber menace.	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn** **15 min de présentation de la réalisation en groupe**	Le candidat doit capable de • Documenter son analyse de la situation technique Il présente le déroulement de la cyber -attaque • Proposer des actions pour rétablir l'activité. • Rétablir le bon fonctionnement des systèmes • Coordonner des équipes variées (techniques, stratégiques, fonctionnelles) L'ensemble des actions proposées sont conformes à la stratégie SI.

		15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)	
	A4C7. Assurer la formation et l'entraînement des acteurs métiers et support susceptible d'intervenir en cas de crise de cybersécurité afin d'améliorer la capacité de l'organisation à réagir à une attaque	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn** **15 min de présentation de la réalisation en groupe** **15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)**	Le candidat doit être capable de proposer une démarche d'apprentissage progressive sous forme d'une présentation orale permettant de : • Sensibiliser les personnels aux problématiques cyber et d'entraîner ceux qui ont un rôle à jouer • Éprouver l'efficience des procédures mises en place dans le cadre de ce dispositif et de les améliorer • Rendre compte des efforts produits en matière de résilience cyber répondant ainsi à de potentielles exigences légales et attentes sociétales. Il décrit sa démarche, sa stratégie de formation, la typologie de son public et les objectifs pédagogiques
	A4C8. Animer la cellule de crise décisionnelle et les cellules de crise opérationnelles en impliquant chaque membre de l'équipe afin de s'assurer de leur capacité à agir et à traiter la crise de cybersécurité	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur**	Le candidat est capable de proposer une feuille de route claire et la présenter de façon précise La feuille de route présente un dispositif global de : • Gestion de crise des cybers menaces en détaillant son fonctionnement • Prises de décision majeures à la lumière des problèmes de sécurité remontés par les cellules opérationnelles

		Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn **15 min de présentation de la réalisation en groupe** **15 min d'entretien individuel (questions en lien avec les compétences)**	• L'ensemble des actions et recommandations de sécurité SI à mener en apportant de la transversalité à la réflexion
	A4C9. Piloter les actions de sensibilisation à la sécurité des SI et de conduite du changement auprès des utilisateurs en organisant des formations internes et externes dans le domaine de la sécurité des S.I afin de faire gagner en compétences les équipes internes en matière de cyber prévention et à terme faciliter la mise en place des nouveaux processus	**Epreuve IV Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur** **Phase II-Production écrite individuelle à réaliser**	Le candidat doit rédiger un argumentaire sur l'intérêt de la sensibilisation des équipes à la culture de la cybersécurité. • Le document présente une qualité rédactionnelle Les arguments présentés sont factuels et s'appuie sur études récentes établies par l'ANSSI par exemple

Modalités d'évaluation

Les modalités d'évaluation pour la certification Expert en cybersécurité et sécurité informatique est réalisée par le biais des mises en situation professionnelle (MSPR) et d'un dossier professionnel

1. Mises en situation professionnelle (MSPR) :

Chaque bloc de compétence est évalué par une mise en situation professionnelle reconstituée :

La préparation des MSPRs se fait par équipe de 3 maximum et donne lieu à :

Une production écrite individuelle

Une soutenance orale par équipe devant un jury de deux professionnels Experts dans le métier

Une évaluation individuelle par le jury à la suite d'un échange individuel avec le jury

2. Dossier Professionnel :

Le candidat doit mettre en avant les compétences acquises en entreprise durant le stage ou l'alternance et fait l'objet d'une production écrite individuelle de 50 à 60 pages et une soutenance individuelle orale devant un jury de deux professionnels et un représentant de l'organisme de certification

Bloc de compétences 1 : Epreuve I- Mise en situation professionnelle reconstituée (MSPR)
Analyse et conception d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur
Phase I- Préparation tutorée de la MSPR par équipe de 4 max.
- Durée de préparation : 21 h
Phase II-Production écrite individuelle à réaliser
Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn
15 min de présentation de la réalisation en groupe
15 min d'entretien individuel (questions en lien avec les compétences)

Bloc de compétence 2 : Epreuve II Mise en situation professionnelle reconstituée (MSPR)
Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur
Préparation tutorée de la MSPR par équipe de 4 max.
- Durée de préparation : 20 h
Phase II-Production écrite individuelle à réaliser
Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn
15 min de présentation de la réalisation en groupe
15 min d'entretien individuel (questions en lien avec les compétences)

Bloc de compétences 3 : Epreuve III Mise en situation professionnelle reconstituée (MSPR)
Déploiement d'une architecture ou solution de sécurité cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur
- Durée de préparation : 30 h
Phase II-Production écrite individuelle à réaliser
Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 30 mn
15 min de présentation de la réalisation en groupe
15 min de démonstration technique et entretien individuel (questions en lien avec les compétences)

Bloc de compétences 4 : Epreuve IV Mise en situation professionnelle reconstituée (MSPR)
Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur
Phase I- Préparation tutorée de la MSPR par équipe de 4 max.
- Durée de préparation : 20 h

Phase II-Production écrite individuelle à réaliser
Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn
15 min de présentation de la réalisation en groupe
15 min d'entretien individuel (questions en lien avec les compétences)

Adaptation des modalités d'évaluation pour les personnes à situation de handicap

Afin de garantir l'égalité de leurs chances avec les autres candidats, les candidats à la certification issus de l'établissement partenaire et présentant un handicap temporaire ou permanent peuvent bénéficier des aménagements rendus nécessaires par leur situation lors des modalités d'évaluation de compétences (soit leur de la réalisation et la soutenance des Mises en situation professionnelle reconstituée et du dossier professionnel)
Il appartient au candidat souhaitant bénéficier d'un aménagement ou bien à son médecin
d'en faire la demande écrite auprès du référent handicap de l'établissement partenaire .
(se référer à la partie VI du règlement de validation de la certification)