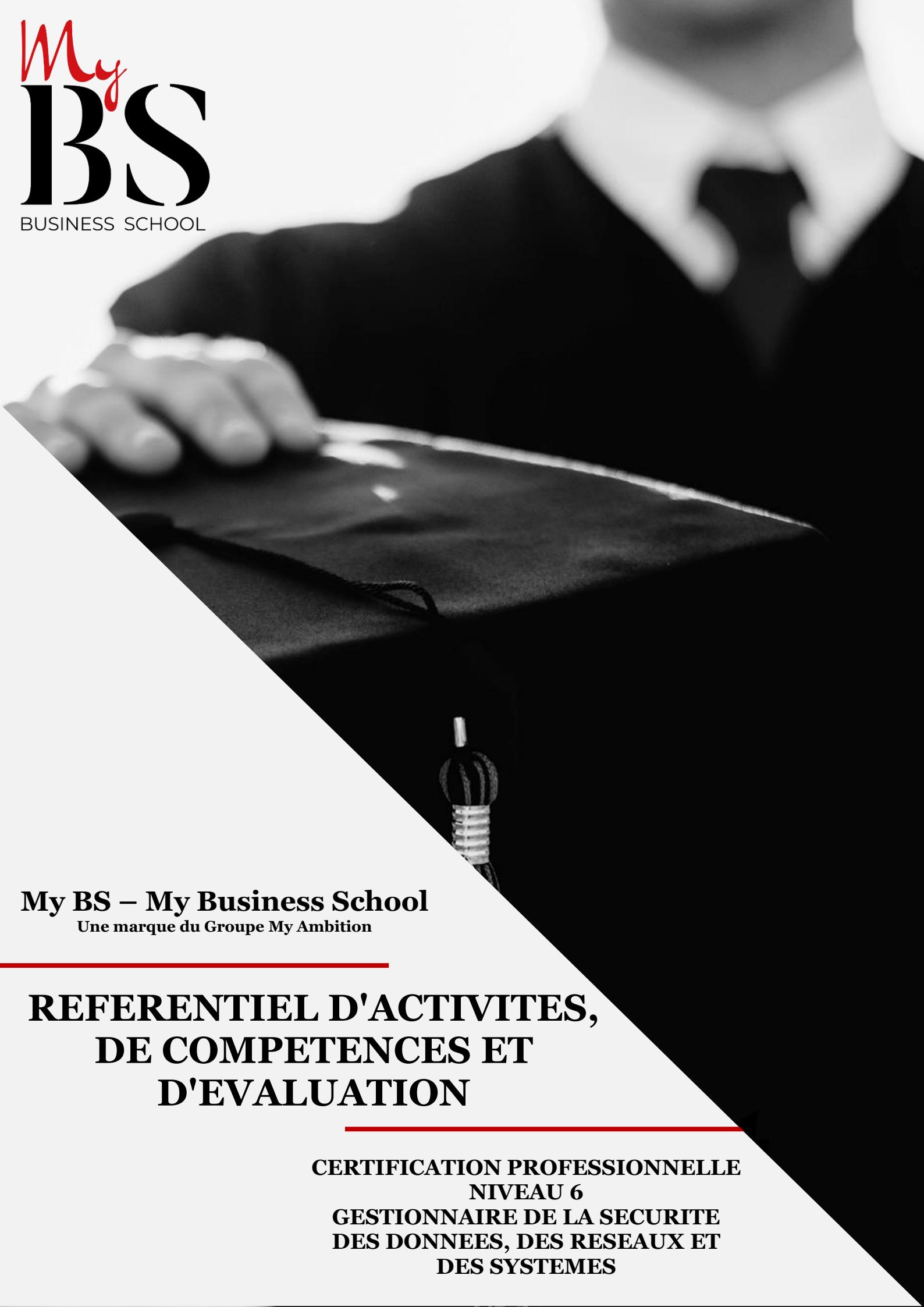

My BS – My Business School

Une marque du Groupe My Ambition

REFERENTIEL D'ACTIVITES, DE COMPETENCES ET D'EVALUATION

CERTIFICATION PROFESSIONNELLE
NIVEAU 6
GESTIONNAIRE DE LA SECURITE DES DONNEES, DES RESEAUX ET DES SYSTEMES

REFERENTIEL D'ACTIVITES *Décrit les situations de travail et les activités exercées, les métiers ou emplois visés.*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités.*	**REFERENTIEL D'EVALUATION*** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITES D'EVALUATION	**CRITERES D'EVALUATION**
BLOC 1 : CARTOGRAPHIER LES SYSTEMES D'INFORMATION			
A 1.1 : Identification des risques de sécurité des systèmes d'information : • Réalisation de l'inventaire des systèmes d'information, • Elaboration des vues cartographiques, • Anticipation des risques de traitement. **A 1.2 : Contrôle des accès aux systèmes d'information :** • Authentification des utilisateurs, • Contrôle des habilitations, • Qualification des accès critiques. **A 1.3 : Amélioration continue du processus de cartographie des systèmes d'information :** • Actualisation régulière et structurée de la cartographie, • Respect du cadre juridique et légal. • Organisation de la veille.	**C 1.1 :** Définir les objectifs et les enjeux du projet de cartographie pour répondre aux besoins opérationnels de sécurité numérique de l'organisation. **C 1.2 :** Réaliser un listing exhaustif des composantes du système d'information incluant notamment l'écosystème qui gravite autour du SI, les processus métiers de l'organisme avec les acteurs qui y participent, les périmètres et les niveaux de privilèges des utilisateurs/administrateurs, les logiciels et les équipements physiques utilisés, pour appréhender les risques potentiellement encourus par les systèmes d'information. **C 1.3 :** Réaliser une revue des droits d'accès pour identifier les accès obsolètes, incomplets ou non autorisés. **C 1.4 :** Déterminer par degré de criticité les accès sensibles, cibles privilégiées par les cyberattaquants, de sorte à prioriser les actions en matière de gestion des risques et de s'assurer que les accès aux éléments sensibles soient maitrisés. **C 1.5 :** Evaluer les risques engendrés par chaque traitement pour mesurer l'impact relatif que pourraient avoir ces menaces sur l'organisation.	**Etude de cas réel d'entreprise.** *Cartographie des SI.* *Production écrite.* Le candidat a, à sa disposition, une présentation littéraire et chiffrée de l'entreprise, de ses activités, des méthodes utilisées pour sécuriser les systèmes d'information ainsi, que des comptes rendus d'entretien des salariés de l'entreprise impliqués dans les services informatiques. Dans le respect du cadre juridique et légal relatif à la protection des systèmes d'information, le candidat doit à partir de ces informations : 1. Identifier les objectifs pour l'entreprise et analyser les besoins de sécurité, 2. Etablir une liste des ressources du système et identifier chaque partie prenante pouvant accéder à ce dernier. 3. Elaborer une cartographie du système d'information afin de recenser les vulnérabilités. 4. Identifier les scénarii de risques et leurs impacts sur l'organisation. 5. Classer par criticité les événements redoutés.	Les composants critiques susceptibles de servir de vecteur d'entrée à la cyberattaque sont identifiés et analysés. Les éléments de l'écosystème (ensemble des parties prenantes qui gravitent autour du produit ou du service et qui sont nécessaires à son fonctionnement), susceptibles de rendre possible ou de faciliter la réalisation de cyberattaque, sont listés exhaustivement. L'analyse menée permet d'identifier les besoins de durcissement du socle de sécurité et d'identifier des mesures complémentaires ad hoc liées aux conditions d'emploi du produit ou service, à ses processus métier, à son écosystème, etc. Les évènements redoutés sont décrits, sous la forme d'une *abuser story,* de nature intentionnelle ou d'origine accidentelle. La cotation de la gravité des impacts est effectuée sur la base de l'échelle suivante : 1- Mineur 2- Significative 3- Grave

	C 1.6 : Elaborer la cartographie des systèmes d'information dans une démarche d'amélioration continue, à la fois incrémentale (enrichissement par de nouvelles vues) et itérative (affinement des vues déjà constituées), pour identifier les systèmes les plus critiques et les plus exposés, anticiper les chemins d'attaque possibles sur ces systèmes et mettre en place des mesures adéquates pour assurer leur protection, réagir plus efficacement en cas d'incident, identifier les activités clés de l'organisme afin de définir un plan de continuité d'activité. **C 1.7 :** Maintenir la cartographie à jour pour garantir une synchronisation entre les évolutions du système d'information et leur représentation dans l'inventaire et les vues tout en veillant à la bonne conformité de l'organisation avec les nouvelles exigences en matière de sécurité numérique. **C 1.8 :** Mettre en œuvre les exigences réglementaires relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces datas, aux mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne, pour inscrire la sécurisation des données, des réseaux et des systèmes de l'entreprise dans le cadre légal et juridique. **C 1.9 :** Utiliser les outils de veille cybersécuritaire, juridique, technique, concurrentielle, stratégique et mobiliser les ressources expertes (ANSSI) pour maintenir à l'état de l'art sa connaissance relative à la sécurité des systèmes d'information.	6. Définir les mesures de sécurité permettant de limiter les risques.	4- Critique Les mesures de sécurité privilégiées sont de nature à réduire le niveau de menace. A travers sa production, le candidat met clairement en avant les objectifs stratégiques pour l'entreprise relatifs à cette cartographie, les besoins de sécurité, les sources de risques, les modes opératoires des attaquants, les composants du système, les impacts métier, les gravités, les mesures existantes et/ou prévues. Les tâches sont menées dans le respect du cadre juridique et légal. Le candidat fait notamment du lien avec le Règlement (UE) 2016/679, la Directive (UE) 2016/1148, la loi n° 2018-493 et le décret n'°2015-351 (liste non exhaustive). La connaissance de l'écosystème et des fondamentaux de sécurité recommandés, notamment par l'ANSSI, est démontrée.

BLOC 2 : SECURISER LES DONNEES, LES RESEAUX ET LES SYSTEMES

A 2.1 : Protection des données, des réseaux et des systèmes : • Homologation de sécurité, • Gestion de la sécurité des postes de travail, • Protection des locaux, • Fiabilisation de l'administration, • Sécurisation des serveurs et réseaux internes, • Protection des réseaux externes, • Sauvegarde et archivage de manière sécurisé. **A 2.2 : Maintien en condition de sécurité les données, les réseaux et les systèmes :** • Mise en œuvre d'une procédure de maintien en condition de sécurité des ressources matérielles et logicielles des systèmes d'information, • Amélioration continue.	**C 2.1 :** Mesurer le niveau de maîtrise des risques atteint en prenant en compte la sécurité numérique des services proposés afin d'adapter le niveau de risque résiduel accepté à un contexte donné. **C 2.2 :** Déployer le niveau de sécurité, défini par la Direction, sur l'ensemble du parc informatique et des locaux techniques de l'entreprise afin d'homogénéiser les politiques de sécurité s'appliquant à l'ensemble du parc pour sécuriser le système d'information. **C 2.3 :** Mettre en œuvre les mesures techniques (configuration de matériels et de logiciels, installation de micro-codes, de systèmes d'exploitation…) sur le système d'information d'administration et son écosystème pour protéger le SI d'administration de toutes tentatives d'intrusions et compromissions. **C 2.4 :** Cloisonner le système d'information par la mise en place de dispositifs de filtrage entre les différentes zones réseaux plus ou moins critiques pour minimiser la propagation d'informations infectieuses sur l'ensemble des systèmes de l'entreprise. **C 2.5 :** Contrôler les accès internet par la mise en place d'une passerelle internet sécurisée permettant de bloquer les flux illégitimes avec des relais applicatifs incontournables implémentant des fonctions de sécurité pour réduire les risques de sécurité.	**Mise en situation professionnelle en groupe de maximum quarte personnes.** *Serious Game.* *Production numérique / informatique.* Les équipes ont pour mission d'administrer deux machines qui hébergent des services de messagerie, des applications web et du partage de fichiers. Les serveurs ont vingt vulnérabilités (ex : un mot de passe faible, un problème de droits, etc). Chaque équipe gère un couple de machines et peut intervenir sur n'importe quelle partie du système, mais les services doivent rester accessibles, sous peine de pénalité. Les groupes ont à disposition une cartographie répertoriant les menaces, vulnérabilités et risques potentiels. En s'appuyant sur les différentes vues cartographiques, les équipes doivent mettre en œuvre un plan d'action pour : • Sécuriser les postes de travail, • Sécuriser l'administration, • Sécuriser le serveur, • Protéger le réseau interne, • Protéger le réseau externe, • Sauvegarder et archiver les composants critiques.	Les deux postes de travail sont sécurisés via l'installation d'un pare-feu logiciel (firewall). Les flux d'administration sont protégés dans un tunnel VPN IPsec. Un protocole assurant le chiffrement et l'authentification, type TLS, est mis en œuvre pour protéger le serveur. Le réseau est segmenté et un cloisonnement entre les différentes zones de ce dernier est mis en place pour favoriser une sécurité homogène du réseau. Une passerelle sécurisée d'accès à Internet est mise en œuvre. Elle comprend au minimum un pare-feu au plus près de l'accès Internet pour filtrer les connexions et un serveur mandataire (proxy) embarquant différents mécanismes de sécurité afin d'assurer notamment l'authentification des utilisateurs et la journalisation des requêtes. Les données présentes sont sauvegardées sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques, de manière déconnectée du système d'information pour prévenir leur chiffrement, afin de protéger les sauvegardes d'une infection des systèmes et de conserver les données critiques à la reprise d'activité.

	C 2.6 : Appliquer une politique de sauvegarde des composants critiques (liste des données jugées vitales pour l'organisme et les serveurs concernés, différents types de sauvegarde, fréquence des sauvegardes, procédure d'administration et d'exécution des sauvegardes, informations de stockage et restrictions d'accès aux sauvegardes, procédures de test de restauration, destruction des supports ayant contenu les sauvegardes) pour poursuivre l'activité en cas d'incident. **C 2.7 :** Maintenir le niveau de sécurité des systèmes d'information tout au long de leur cycle de vie, conformément à la politique de sécurité des réseaux et systèmes d'information de l'organisation, en raccourcissant le délai entre la publication d'une vulnérabilité et la mise en œuvre de mesures techniques ou organisationnelles pour la contrer. **C 2.8 :** Mettre en œuvre un plan d'amélioration continue de la sécurité pour garantir la montée en puissance et en maturité de la sécurité de l'entreprise et permettre une gestion dynamique des risques résiduels selon leur criticité.	L'exercice est hébergé sur une plateforme, type infrastructure de virtualisation, conçue à cet effet.	Le plan d'action privilégié répond aux exigences de la procédure de maintien en condition de sécurité et d'un processus d'amélioration continue.

BLOC 3 : GERER LE RISQUE NUMERIQUE

A 3.1 : Participation à la définition de la stratégie de sécurité des données, des réseaux et des systèmes : • Collaboration à l'élaboration stratégique, • Mise en œuvre de la sécurisation du système d'information. **A 3.2 : Management du risque numérique au sein de l'organisation :** • Gestion des accès aux locaux, • Fiabilisation des actions de maintenance, • Sécurisation des développements informatiques, • Supervision des journaux, • Contrôle des actions de sous-traitance, • Evaluation des dispositifs de sécurité. **A 3.3 : Traitement de cyberattaques :** • Gestion de cybercrise, • Investigation, • Remédiation, • Stabilisation.	**C 3.1 :** Contribuer à la définition du modèle de gouvernance de la politique de sécurité du système d'information afin que la Direction puisse élaborer la stratégie de protection des données, des réseaux et des systèmes. **C 3.2** : Déployer la stratégie de sécurité numérique de l'entreprise, préalablement définie par la Direction, dans le respect du cadre juridique et réglementaire, pour protéger le système d'information contre une large gamme de menaces. **C 3.3 :** Contrôler l'accès aux salles serveurs et aux locaux techniques afin de s'assurer que les mécanismes de sécurité physique ne puissent pas être contournés aisément par un attaquant. **C 3.4 :** Gérer la maintenance des données en garantissant la sécurité de ces dernières, à tout moment du cycle de vie des matériels et des logiciels, pour maîtriser l'accès aux données. **C 3.5 :** Encadrer les développements informatiques pour s'assurer et attester que le développement est effectué conformément aux exigences règlementaires et sécuritaires de l'organisation. **C 3.6 :** Mettre en place une supervision des incidents de sécurité informatique par une politique de journalisation sur les différentes ressources du système d'information afin de détecter une éventuelle compromission.	**ME 1 – Etude de cas réel d'entreprise** *Stratégie et plan d'action.* *Production écrite.* Le candidat dispose d'un rapport d'analyse, sous forme de cartographie, des systèmes d'informations de l'entreprise ainsi qu'un compte rendu de réunion de la Direction précisant la stratégie de sécurité numérique de l'organisation privilégiée. En s'appuyant sur ces deux documents, le Gestionnaire de la sécurité des données, des réseaux et des systèmes a pour mission d'apporter des préconisations à sa Direction afin de parfaire la stratégie de sécurité numérique. Dans un second temps, il rédige un plan d'action relatif au déploiement de la stratégie de sécurisation du système d'information préalablement préconisée.	**Pour ME 1 :** Les préconisations faites s'appuient sur le rapport d'analyse et spécifiquement sur la vraisemblance d'exploitation des chemins d'attaques et l'impact des pires scénarios sur l'organisation, la capacité des mesures de sécurité en place à empêcher la survenance des scénarios, les ressources financières, humaines et techniques disponibles. En tenant compte des critères supra, le candidat décline les options de traitement des risques à retenir telles que la mise en œuvre de mesures de sécurité, l'évolution des processus métiers ou encore le transfert contractuel des risques vers des tiers externes (sous-traitants, assurances, etc…). Le plan d'action comprend la définition des actions à mettre en œuvre, la planification des actions dans le temps, l'affectation des ressources humaines à la mise en œuvre des actions et le montant des investissements prévus. Le candidat est en mesure de définir les objectifs et les résultats attendus dans le cadre de la mise en œuvre du plan d'action. Il propose un ensemble de KPI mesurant l'efficacité des actions préconisées. Le cadre réglementaire est pris en compte et respecté.

	C 3.7 : Gérer la sous-traitance en prenant et documentant les moyens (contrôle de sécurité, visite des installations…), tout en tenant compte des situations de handicap le cas échéant, pour s'assurer l'effectivité des garanties offertes par le sous-traitant. **C 3.8 :** Déployer la stratégie de réponse aux cyberattaques associée au dispositif de gestion de crise, définie par anticipation par la Direction, en s'appuyant sur le contexte dans lequel s'inscrit l'attaque pour manager l'impact de cette dernière sur l'organisation et assurer la continuité d'activité puis son retour à un état normal. **C 3.9 :** Collecter et analyser les éléments techniques permettant de comprendre le chemin d'attaque utilisé par les cyberattaquants et les actions de ces derniers sur les systèmes infectés, restaurer les systèmes dans leur état initial en éjectant l'attaquant du système et améliorer la sécurité pour éviter une attaque similaire par l'application de mesures d'assainissement, améliorer la sécurité à plus long terme par la définition et l'application de mesures de sécurisation et l'amélioration de la supervision, afin de faire cesser les effets de la cyberattaque et éjecter l'attaquant en dehors des systèmes d'information infectés. **C 3.10 :** Procéder à des contrôles des dispositifs de sécurité en évaluant concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps pour assurer la protection des données, des systèmes et des réseaux de l'entreprise.	**ME 2 – Mise en situation professionnelle** en groupe de maximum quatre personnes. *Cyberattaque.* *Production écrite et présentation orale.* Les groupes sont réunis dans une pièce. Le formateur leur fait part des évènements majeurs de la cyberattaque : • Une attaque touchant le réseau bureautique provenant d'un vecteur logiciel lié à une faille propre à un sous-traitant et d'un vecteur physique provenant des locaux de la société. • Sa propagation sur au moins un autre site. • La médiatisation de l'attaque. • La publication par un groupe d'attaquants d'une partie des données exfiltrées afin de faire pression en vue du paiement d'une rançon. Le formateur leur transmet également la stratégie de réponse aux cyberattaques définie par la Direction. A partir de l'ensemble des éléments communiqués, les candidats analysent les données permettant de comprendre les chemins d'attaque utilisés puis mettent en œuvre des actions pour gérer la crise et assurer la continuité d'activité de l'entreprise puis son retour à l'état normal. Les groupes exposent en suite leurs actions et justifient leurs choix auprès	**Pour ME 2 :** Une main courante est ouverte permettant de tracer les actions et les évènements liés à l'incident comprenant l'heure et la date de l'évènement, le nom de la personne à l'origine de cette action ou ayant informé sur l'évènement, la description de l'évènement, pour renseigner les décideurs sur l'état d'avancement des actions entreprises. Les opérations de maintenance sont encadrées pour maitriser l'accès aux données par les prestataires par les précautions élémentaires suivantes : - Les interventions de maintenance sont enregistrées dans une main courante. - Une clause de sécurité est insérée dans les contrats de maintenance effectués par des prestataires. - Un responsable de l'organisme est désigné pour encadrer les interventions par des tiers. - Une procédure de suppression sécurisée des données est rédigée et mise en œuvre. - Les données des matériels sont supprimées de façon sécurisée avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin du contrat de location. La sécurité informatique avec les sous-traitants est encadrée par : - La communication de la politique de sécurité des systèmes

		d'un jury composé de deux membres qui joueront les rôles de : • Directeur Général ; • Responsable de la sécurité des systèmes d'information.	d'information en prenant compte d'éventuelles situations de handicap ; - Des garanties offertes par le sous-traitant en matière de protection des données ; - La rédaction d'un contrat avec les sous-traitants, qui définit notamment l'objet, la durée, la finalité du traitement et les obligations des parties. L'accès aux salles serveurs et aux locaux techniques est contrôlé et protégé par des propositions de prise de précautions comme l'installation d'alarmes anti-intrusion, un contrôle d'accès dédié pour la salle informatique, etc… Les exigences de sécurité informatique sont intégrées dès la conception des projets par des choix d'architecture, de fonctionnalités, de technologies, etc. La supervision des incidents de sécurité informatique est assurée par la mise en place d'une politique de journalisation sur les différentes ressources du système d'information (les serveurs d'infrastructure système, les postes d'administration et postes utilisateur, les serveurs métier et les équipements réseau et de sécurité situés en périphérie ou au cœur du système d'information). La stratégie de réponse proposée pour faire face à la cyberattaque s'appuie sur le contexte dans lequel celle-ci s'inscrit afin de manager son impact sur l'organisation et assurer la continuité

			d'activité puis son retour à un état normal. Les candidats évaluent l'efficacité de leurs actions via des indicateurs clés de performances.
		ME 3 – Mise en situation professionnelle *Contrôle de sécurité.* *Production numérique / informatique et écrite.* Le candidat se connecte à un espace informatique, conçu spécifiquement pour cette mise en situation, où il a la visibilité sur l'ensemble des dispositifs de sécurité de l'entreprise. Il contrôle que les règles pour assurer le maintien en conditions de sécurité sont mises en œuvre, respectées et efficaces. Il identifie les vulnérabilités et effectue des actions de remédiation. Dans un second temps, une fois avoir techniquement opéré, il rédige un compte rendu des actions menées à sa Direction.	**Pour ME 3 :** Les contrôles de sécurité mis en œuvre s'assurent que : - L'organisation et les processus choisis pour protéger les informations sont toujours au niveau défini ; - La sécurité mise en place sur les systèmes pour protéger les informations est toujours au niveau défini ; - Les systèmes sont bien protégés de toutes les failles techniques connues ; - Les risques identifiés ont bien été pris en compte et corrigés ; - L'élément humain de l'organisation respecte bien les politiques de sécurité et réagit correctement aux évènements pour protéger les informations. Les contrôles sont menés 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. Les actions de remédiation sont effectuées dans le respect du cadre réglementaire et optimisent la protection

			des données, des systèmes et des réseaux de l'entreprise. Le rapport recense l'ensemble des actions entreprises, met en évidence les vulnérabilités et les écarts constatés, évalue les risques de sécurité et leurs impacts sur les métiers.

BLOC 4 : DIFFUSER DES INFORMATIONS RELATIVES A LA SECURITE DES DONNEES, DES RESEAUX ET DES SYSTEMES

A 4.1 : Information, formation et assistance : • Diffusion de la politique de protection du système d'information, • Conseil et accompagnement, • Sensibilisation et formation. **A 4.2 : Communication d'alertes :** • Transmission d'informations à la Direction, • Information et conseil auprès des parties prenantes.	**C 4.1 :** Mener des actions de communication et de sensibilisation, en collaboration avec les éventuels services de l'organisation en charge de la communication et en tenant compte des situations de handicap le cas échéant, permettant au personnel de l'entreprise de développer une culture de protection des données en prenant appui sur les recommandations des autorités nationales (ANSSI, CNIL…). **C 4.2 :** Dispenser des conseils et assister les acteurs de l'entreprise sur les problématiques relatives à la protection des données, des réseaux et des systèmes, en adaptant sa posture aux besoins des personnes ayant un handicap, pour éviter toute sortie du cadre juridique et réglementaire tout en les invitant à signaler au service informatique de l'organisation des éléments suspects pour lutter contre la cybermenace. **C 4.3 :** Mettre en œuvre des programmes de formation du personnel, pouvant être suivi par tout public quel que soit son handicap, pour sensibiliser aux bonnes pratiques de sécurité numérique, faire naître ou renforcer certains réflexes, renforcer la responsabilité et la transparence de chacun. **C 4.4 :** Informer la Direction d'un risque de compromission du système d'information et rédiger un rapport d'analyse associé afin de leur permettre d'appréhender les menaces pesantes sur l'environnement et de prendre les décisions adéquates.	**ME 1 – Mise en situation professionnelle** *Note de vigilance et proposition d'accompagnement.* *Production écrite.* La Direction de l'entreprise a confié la mission au candidat d'adresser, via le système de messagerie interne de l'organisation, une note de vigilance à l'ensemble des collaborateurs sur une potentielle cybermenace (exemple : type rançongiciel). En retour, un membre de l'entreprise signale au Gestionnaire de la sécurité des données, des réseaux et des systèmes qu'il remarque une anomalie technique sur son ordinateur. Le candidat précise, en réponse, les actions à mettre en œuvre pour parer à la menace éventuelle. **ME 2 – Mise en situation professionnelle** *Conception de formation.* *Production écrite et présentation orale.* Le candidat reçoit un mail du Responsable Formation de l'entreprise indiquant un besoin en formation interne, pour huit collaborateurs, relatif à la sécurité des données, des réseaux et des systèmes.	**Pour ME 1 :** Le message communiqué est structuré, précis, audible et prend en compte les situations de handicap en rendant accessible l'information à tous les collaborateurs. La communication permet aux collaborateurs de prendre conscience de la valeur des données, des réseaux, des systèmes, d'accroitre leurs connaissances relatives à ces dernières et de la nécessité d'adopter les bonnes postures face au risque cyber. Les réponses apportées au collaborateur sont claires, justes et appropriés. Les éléments techniques de réponse respectent le cadre réglementaire et juridique de la protection des systèmes d'information. **Pour ME 2 :** Le programme de formation précise l'intitulé de la formation, le nombre de stagiaires, la durée, le nombre de jours, les horaires, les dates, le lieu, l'accessibilité du lieu aux personnes handicapées, les objectifs pédagogiques, les moyens et méthodes pédagogiques, les méthodes d'évaluation, la validation des acquis, le contenu détaillé et séquencé de la formation.

	C 4.5 : Alerter les parties prenantes (clients, fournisseurs, médias, autorités, etc.), en adaptant si nécessaire sa communication à un public ayant un handicap, d'un comportement inhabituel de la part d'un poste de travail ou d'un serveur, synonyme d'une potentielle intrusion, en spécifiant l'état de la compréhension de la menace, les hypothèses d'évolution de cette dernière et en préconisant des actions simples à mener dans l'attente de la réalisation d'opérations techniques pour limiter ou stopper la cybermenace.	Il conçoit un programme de formation de deux jours (quatorze heures). **ME 3 – Mise en situation professionnelle** *Communication d'alerte.* *Production écrite.* En pleine action de contrôle des dispositifs de sécurité, le candidat observe, sur son ordinateur portable, un risque de compromission du système d'information. Il informe alors sa direction, via un rapport d'analyse. Puis, dans un second temps, le candidat constate sur son PC un comportement inhabituel (connexion impossible, activité importante, activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation, multiples alertes de l'antivirus, etc.). Il rédige alors une note à l'ensemble des parties prenantes indiquant l'état de la compréhension de la menace, les hypothèses d'évolution de cette dernière et en préconisant des actions simples à mener.	La formation peut être suivie par toute personne, sans nécessiter d'adaptation ni de conception spéciale, et ce, quel que soit son handicap. **Pour ME 3 :** Le rapport d'analyse intègre une note de synthèse, le cadre de l'étude, le périmètre métier et technique, l'identification des évènements redoutés, les sources de risque et les objectifs visés par ces dernières, les scénarii de cyberattaque potentiels et des préconisations de traitement du risque. La note d'alerte à l'ensemble des parties-prenantes comprend bien l'état de la compréhension de la menace, des hypothèses d'évolution de cette dernière, des préconisations d'actions à effectuer et peut-être utilisée par toute personne quel que soit son handicap.

REFERENTIEL D'EVALUATION*

L'ensemble des mesures décrites ci-après visent à garantir le système d'évaluation des prétendants à la certification.

Les objectifs poursuivis sont multiples :

- Pertinence des modalités d'évaluation : permettent de faire le lien entre la théorie et la pratique. Elles développent notamment des compétences techniques mais aussi des aptitudes humaines propres à la complexité des prises de décisions terrain.
- Proportionnalité en fonction des objectifs d'évaluation poursuivis
- Equilibre dans les diverses situations d'évaluation
- Equité dans le traitement
- Expertise dans la création des supports
- Garantie d'indépendance des évaluations et certifications partielles par bloc de compétence
- Formation des acteurs aux situations d'évaluation spécifiques
- Contrôle des résultats et analyse des écarts
- Principes et voies de recours

I. PERTINENCE DES MODALITES D'EVALUATION

Les différentes situations d'évaluation, épreuves certificatrices globales ou partielles (bloc de compétences), contrôles continus en cours de formation, font l'objet d'un équilibre et d'un ajustement visant à offrir une variété de situations vécues où à vivre au travers de problématiques professionnelles réelles, fictives, individuelles, de groupe, ponctuelles ou de moyen / long terme. Elles font l'objet d'une sélection rigoureuse et d'un contrôle amont par l'encadrement pédagogique et les experts métiers.

II. PROPORTIONNALITE EN FONCTION DES OBJECTIFS D'EVALUATION POURSUIVIS

Les modalités d'évaluation diffèrent au regard des objectifs de contrôle de compétence poursuivis. En fonction de leur poids dans le référentiel, de leur complexité, technicité, de la multiplicité des expertises mobilisées, leur nombre, leur fréquence et leur durée est ajustée sous le contrôle de l'encadrement pédagogique.

III. EQUILIBRE DANS LES DIVERSES SITUATIONS D'EVALUATIONS

Le choix des types d'évaluation est échantillonné de manière à adapter les situations aux compétences à observer : écrits sous forme d'étude de cas réel, oraux individuels ou collectifs, serious game, cas pratiques, ou simple contrôle de connaissance ; la diversité des situations vise à transcrire la réalité de la mise en œuvre des compétences métiers, le plus souvent en situation « réelle ». L'équilibre recherché garantit la complexité des attitudes et compétences professionnelles éprouvées mais aussi, la recherche de la mise en œuvre des « soft kills » associés.

IV. EXPERTISE DANS LA CONSTRUCTION DES SITUATIONS ET SUPPORTS

La sélection experte des contenus, la construction des scénarii, la validation conjointe expert métier / pédagogique, garantit la qualité des contenus, leurs modalités, leur actualité et actualisation. La pluralité des expertises personnelles mobilisées vise la confrontation contradictoire et l'équilibre de traitement des problématiques professionnelles à observer dans la détermination des réponses attendues. La correction des épreuves se fait au moyen systématique de grilles d'évaluation croisées par compétence et niveau d'exercice attendu.
Il en va de même pour le jury final de validation des parcours de certification par le biais de la VAE.

V. INDEPENDANCE DES EVALUATIONS ET CERTIFICATION PARTIELLE PAR BLOC DE COMPETENCES

L'ensemble des modalités d'évaluation autorise la validation partielle de la certification par bloc de compétence. Ainsi, chaque bloc est évaluable indépendamment. Les compensations de notes au regard des parcours certifiants progressifs sont autorisées intra-bloc, pour les parcours globaux selon un système intra bloc et inter bloc.
La potentielle exigence d'un mémoire de fin d'étude garantit l'homogénéité des blocs de compétences validés par des parcours progressifs ou par le biais des Validations des Acquis de l'Expérience.

VI. FORMATION DES ACTEURS AUX SITUATIONS D'EVALUATION SPECIFIQUES

Les épreuves à visée certifiante, par bloc et globale mettent en œuvre une multiplicité de situations et de modalités spécifiques qui nécessitent une double expertise technique / pédagogique.
Aussi, les jurys sont-ils préalablement informés et formés sur celles-là. Le jury de validation des parcours de type VAE bénéficient de la même manière d'une formation préalable.

VII. CONTROLE DES RESULTATS ET ANALYSE DES ECARTS

Chaque session d'examen voit l'ensemble des résultats analysés sous un double objectif :

- Recherche des abandons de parcours, défaillances individuelles et collectives ;
- Performance des promotions annuelles, homogénéité dans le temps.

Les écarts ainsi observés au regard des résultats attendus ont pour objectif de garantir le niveau de maîtrise et d'exercice des compétences des différentes cohortes par la mise en œuvre d'actions à visée d'amélioration.

VIII. PRINCIPES ET VOIES DE RECOURS

Les échecs de parcours individuels au regard des exigences du règlement de certification sont ainsi, par nature, possibles sans toutefois être recherchés.

Aussi, le Jury de Délivrance de la Certification Professionnelle, qu'il analyse sous la forme globale de passage, la forme progressive ou par le biais de la VAE, est souverain dans l'appréciation des différents parcours au regard du règlement de certification.

Toutefois, chaque prétendant a la faculté de représenter :

- Une ou plusieurs épreuves par le biais de rattrapage(s) ponctuels
- Leur parcours ainsi consolidé à un Jury de Délivrance de la Certification Professionnelle ultérieur
- Une réclamation consistant en la consultation d'une copie corrigée, grille d'évaluation annotée et accès la correction type de l'évaluation.
- Une demande spécifique au regard de la situation personnelle, professionnelle et d'un écart minime versus la conjonction des exigences du règlement.