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**	
		Modalité d'évaluation	**Critères d'évaluation**
BLOC 1 : DEFINIR LA STRATEGIE DE CYBERSECURITE D'UNE ORGANISATION			
		Type d'évaluation : Mise en situation professionnelle réelle ou fictive **Attendus du candidat :** A partir d'une analyse d'organisation réelle ou fictive de son choix, le candidat propose une stratégie de cybersécurité. **Livrable attendu :** Le candidat remet au jury un dossier écrit comprenant :	
A1.1. Mener une veille en cybersécurité • Veille sur les produits de sécurité, les évolutions technologiques • Suivi des pratiques des autres organisations	C.1.1.1. Organiser et animer un système de veille technique et technologique en matière de Sécurité du Système d'Information (SSI) à l'aide de recherches documentaires, de plateformes de partage, de webinars, de participations à des salons, des forums, clubs (CLUSIF[1], CLUSIR[2], …etc.), afin d'être alerté des évolutions techniques, technologiques.	✓ La méthodologie de recherche des informations ✓ Les sources d'informations utilisées	✓ La méthodologie de veille est expliquée et justifiée. ✓ La sélection des sources d'informations est expliquée et justifiée.

[1] CLUSIF : Club de sécurité de l'information français
[2] CLUSIR : Club de la sécurité de l'information en réseau

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Veille règlementaire, légale et normative	C.1.1.2. Organiser et animer un système de veille réglementaire en matière de SSI en identifiant les sources de références du secteur de l'organisation afin de garantir la conformité de l'organisation à la réglementation.	✓ Les Sources d'informations utilisées ✓ Un exemple d'obligations réglementaires, légales et des préconisations normatives	✓ La sélection des sources d'informations est expliquée et justifiée. ✓ Les réglementations/lois applicables à l'organisation et à son secteur sont identifiées. ✓ Les normes relatives à la sécurité du SI sont présentées
• Veille sur les nouvelles menaces	C.1.1.3. Organiser et animer un système de veille concernant les nouvelles menaces à l'aide de recherche Web, CERT[3] afin d'être prévenu des alertes, vulnérabilités et menaces susceptibles d'impacter l'organisation.	✓ Les Sources d'informations utilisées ✓ Un exemple d'alerte, menace ou vulnérabilité	✓ La sélection des sources d'informations est expliquée et justifiée. ✓ Les menaces identifiées sont cohérentes avec le contexte technique et métier de l'organisation.
• Tri, analyse et intégration des informations	C.1.1.4. Traiter les informations recueillies en s'assurant de leur pertinence et véracité afin d'identifier les opportunités d'amélioration et obligations en matière de sécurité des données, des systèmes et des réseaux de l'organisation.	✓ La présentation d'une obligation de sécurité règlementaire et d'une opportunité d'amélioration	✓ La véracité des éléments de veille recueillis est justifiée par des éléments de preuve ✓ Les obligations réglementaires et légales auxquelles le SI de l'organisation doit se conforme sont justifiées. ✓ L'amélioration de sécurité du SI au regard de la veille réalisée est préconisée et justifiée.

[3] CERT : Computer Emergency Response Team

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**	
		Modalité d'évaluation	**Critères d'évaluation**
A1.2. Etude de l'écosystème de l'organisation : • Identification de l'architecture technique • Identification des parties prenantes et parties prenantes critiques • Identification des acteurs étatiques impliqués dans la sécurité du système d'information (SI).	C.1.2.1. Identifier les composants techniques et les différentes parties prenantes en étudiant l'écosystème afin d'établir la cartographie des informations, leur portée et les risques afférents.	✓ Une cartographie synthétique du SI	✓ Les principaux composants de l'architecture technique sont décrits. ✓ Les liens entre les différents composants techniques sont modélisés. ✓ Les parties prenantes internes et externes sont identifiées ✓ La liste des acteurs étatiques (ANSSI[4], DGSI[5], Cybermalveillance.gouv.fr,) concernant l'organisation ou son secteur est complète. ✓ Le rôle de chaque acteur est précisé.
A.1.3 Evaluation du niveau de sécurité de l'organisation et analyse du besoin de mise en conformité • Analyse de l'exposition numérique de l'organisation (OSINT).[6]	C.1.3. 1. Rédiger un état des lieux de l'exposition numérique de l'organisation à l'aide des données publiques disponibles sur internet afin d'identifier les risques en termes de sécurité et d'exigences réglementaires.	✓ Un état des lieux de l'exposition numérique	✓ L'état des lieux de l'exposition numérique comporte : - L'identification des données exposées - La preuve de leur exposition publique - L'analyse des risques inhérents d'un point de vue sécuritaire - L'analyse des risques d'un point de vue réglementaire

[4] ANSSI : Agence Nationale de la Sécurité de Systèmes d'Information
[5] DGSI : direction générale de la Sécurité intérieure
[6] OSINT : Open Source Intelligence terminologie métier qui signifie renseignement d'origine sources ouvertes.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Analyse des risques initiaux de sécurité • Hiérarchisation des risques par ordre de priorité	C.1.3.2. Réaliser une analyse des risques en identifiant les évènements pouvant affecter la sécurité du système d'information et en estimant les conséquences et les impacts potentiels afin de hiérarchiser les risques pouvant affecter le système d'information (SI).	✓ Une analyse de risque	✓ Le choix de la méthode d'analyse de risque est justifié (EBIOS, MARION, MEHARI.). ✓ L'étude des risques comprend : - les objectifs, - les sources de risques, - la justification des critères de risque choisis - la classification des niveaux de risque - le seuil d'acceptabilité du risque - l'estimation des risques
• Analyse des besoins métier • Détermination des actions de sécurité à mettre en œuvre.	C1.3.3 Evaluer les besoins métier en consultant les utilisateurs et en identifiant les exigences fonctionnelles afin de déterminer les actions de sécurité à mettre en œuvre.	✓ Une évaluation des besoins ✓ Un exemple d'action préventive à mettre en œuvre	✓ Les besoins métiers sont détaillés et évalués. ✓ L'action préventive proposée répond aux besoins métier.
• Documentation des résultats et synthèse managériale	C1.3.4. Concevoir et rédiger des solutions techniques en étudiant le système d'information (SI) et les procédures informatiques d'une organisation afin de formaliser les objectifs de la stratégie de cybersécurité.	✓ Un exemple d'objectif stratégique en matière de cybersécurité	✓ L'objectif présenté est : - conforme aux exigences légales et règlementaires - cohérent au regard du SI et des procédures informatiques existantes - techniquement réalisable.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
A.1.4. Elaboration de la politique de sécurité du système d'information (PSSI) • Définition de la PSSI ou de sa mise en conformité.	C.1.4.1 Définir la politique de sécurité du système d'information (PSSI) en tenant compte de l'analyse de risques, du périmètre et des objectifs stratégiques de sécurité afin de s'assurer que les risques pesant sur le périmètre défini soient bien couverts	✓ Une note de cadrage de la PSSI	✓ La note de cadrage de la PSSI comprend : - le périmètre, - les enjeux et les orientations stratégiques de sécurité du SI, - les aspects légaux et réglementaires, les normes ISO - la gestion des sous-traitants, - une échelle de besoins de sécurité, - les origines des menaces. ✓ Le document tient compte des préconisations du guide de l'ANSSI.
• Identification des moyens humains • Identification des contraintes et des moyens techniques	C.1.4.2. Identifier les moyens techniques et humains nécessaires à la mise en œuvre de la PSSI en prenant en compte la stratégie de l'organisation en termes de sécurité du SI afin de permettre une évaluation du coût de mise en œuvre de la PSSI.	✓ La présentation des moyens techniques et humains nécessaire pour la mise en œuvre de la PSSI	✓ Les moyens techniques et humains nécessaires sont décrits et justifiés au regard de la capacité de l'organisation.
• Etude des couvertures assurantielles existantes ou de l'opportunité d'une souscription en collaboration avec les services concernés • Estimation du budget de la mise en œuvre de la PSSI	C1.4.3. Estimer le coût de mise en œuvre de la PSSI en prenant en compte les différentes solutions possibles y compris assurantielles afin de permettre l'organisation de valider le déploiement des solutions.	✓ Une comparaison budgétaire de la mise en œuvre de la PSSI en fonction des différentes solutions	✓ Au moins 3 solutions dont une assurantielle sont détaillées et comparées. ✓ Les estimations sont détaillées par poste de dépenses. ✓ Les avantages et inconvénients de chaque solution sont exposés.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
A1.5. Définition des outils destinés à garantir la disponibilité des données et à faciliter la résilience du système en cas d'incidents • Elaboration du plan de sauvegarde • Elaboration du Plan de secours Informatique (PSI) • Elaboration d'un plan de reprise d'activité (PRA) • Elaboration d'un plan de continuité d'activités (PCA)	C.1.5.1 Elaborer les plans de sauvegarde, plan de secours informatique (PSI), plan de reprise d'activité (PRA), plan de continuité d'activité (PCA) en étudiant les processus et scénarios critiques afin de faciliter la résilience du système en cas d'incidents.	✓ Un Plan de sauvegarde ou Un Plan de Secours Informatique ou Un Plan de Reprise d'Activité ou Un Plan de continuité d'activité	✓ Les processus critiques et les scénarios critiques sont pris en compte. ✓ Les données critiques et sensibles du SI sont identifiées et prises en compte. ✓ Les ressources critiques sont identifiées et font l'objet d'un traitement spécifique. ✓ Les indicateurs fixés pour le plan sélectionné sont définis. (ex: RTO Recovery Time Objective[7], RPO Recovery Point objective[8]….) ✓ Les solutions techniques et organisationnelles sont adaptées aux besoins et aux moyens de l'organisation et permettent de répondre aux indicateurs fixés.
• Réalisation d'un processus de tests PRA, PSI, PCA, plan de sauvegarde	C.1.5.2 Réaliser un processus de tests des PCA, PRA, PSI et plan de sauvegarde en simulant un incident afin de vérifier la capacité de l'organisation à les mettre en œuv*re.*	✓ Un exemple de tests à effectuer pour chaque plan (PSA, PRA, PSI, plan de sauvegarde)	✓ Le bon déroulé des plans est couvert par les tests. ✓ Les objectifs fixés dans les différents plans font l'objet d'une vérification pendant les tests.

[7] RTO : Recovery Time Objective, terminologie métier qui signifie en français objectif de délai de restauration
[8] RPO : Recovery Point objective terminologie métier qui signifie en français objectif de temps de reprise

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Evaluation des coûts propres aux PCA, PRA, PSI, plan de sauvegarde	C.1.5.3. Estimer les coûts associés à la mise en œuvre des PCA, PRA, PSI et plan de sauvegarde en identifiant l'ensemble des postes de dépenses afin d'intégrer ces coûts dans le budget de l'organisation.	✓ Un macro-chiffrage / estimation des coûts de mise en œuvre des PCA, PRA, PSI et plan de sauvegarde	✓ La méthode utilisée pour réaliser l'estimation des différents plans est décrite et justifiée. ✓ L'estimation fait apparaitre le cout de mise en œuvre de chaque plan. ✓ Les propositions sont détaillées et font apparaitre les postes de dépenses. ✓ Chaque poste de dépenses est budgété

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**	
		Modalité d'évaluation	**Critères d'évaluation**
BLOC 2 : ELABORER ET PILOTER DES PROCESSUS DE CYBERSECURITE D'UNE ORGANISATION			
		Type d'évaluation : Mise en situation professionnelle réelle ou fictive. **Attendus du candidat :** Sur la base d'une stratégie de cybersécurité d'une organisation de son choix, le candidat présente l'élaboration et le pilotage de processus de cybersécurité. **Livrable attendu :** Sous la forme d'une soutenance orale, le candidat présente :	
A.2.1. Elaboration du plan d'actions de Sécurité • Déclinaison de la Politique de sécurité du système d'information (PSSI) en règles de sécurité et d'utilisation du système d'information (SI) • Analyse de l'impact sur l'organisation	C.2.1.1. Décliner la politique de sécurité du système d'information (PSSI) en actions et/ou règles de sécurité adaptées à la cible en prenant en compte l'état actuel du système d'information (SI) afin de déterminer les impacts sur l'organisation.	✓ Une action de sécurité résultant de la PSSI	✓ L'action proposée s'inscrit dans La PSSI. ✓ L'action de sécurité est applicable au regard de la cible. ✓ L'utilité de l'action est justifiée par rapport à la situation initiale. ✓ L'impact de l'action sur l'organisation est évalué.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Elaboration du plan d'actions correspondant	C.2.1.2 Elaborer le plan d'actions en priorisant les actions selon les enjeux de sécurité identifiés et en évaluant leurs coûts afin d'éclairer la prise de décision.	✓ Un plan d'actions	✓ Les actions sont priorisées au regard des enjeux de sécurité. ✓ La priorisation est justifiée ✓ Les coûts associés sont évalués
• Rédaction du corpus documentaire de de la Sécurité du Système d'Information	C2.1.3. Rédiger le corpus documentaire en tenant compte de la Politique de sécurité du système d'information (PSSI) afin d'encadrer l'utilisation /l'usage du système d'information (SI).	✓ Une liste des documents	✓ Les différents types de documents sont listés et pour chaque document sont précisés : - L'objectif au regard de la PSSI - Le périmètre de diffusion - La cible visée - Le niveau de criticité au regard des enjeux sécuritaires
A.2.2. Déploiement des solutions de protection du SI • Conception d'une architecture (fonctionnelle et réseau) sécurisée du système d'information (SI).	C.2.2.1. Concevoir une architecture sécurisée en utilisant les méthodes et solutions connues afin de garantir la sécurité du système d'information (SI).	✓ Un schéma d'architecture sécurisée	✓ Les contraintes et impératifs opérationnels sont pris en compte. ✓ L'état de l'art est respecté. ✓ Les méthodes et solutions de sécurité utilisées sont expliquées. ✓ L'architecture proposée répond aux exigences de sécurité de l'organisation.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Gestion des identités et contrôles des accès	C.2.2.2. Rationaliser les identités et les accès à l'aide de différents dispositifs de contrôle et d'alerte (électronique, physique et informatique) afin d'éviter les diffusions d'informations indues.	✓ Le processus de contrôle des accès	✓ Les moyens organisationnels et techniques sont mis en œuvre pour authentifier l'identité numérique des utilisateurs (ex : authentification multi facteur, gestion des mots de passe, contrôle de mot de passe...) ✓ Les droits et niveaux d'autorisation sont déterminés en fonction des profils des utilisateurs. ✓ Les ressources auxquelles les utilisateurs ont accès en fonction de leurs droits sont répertoriées. ✓ Les moyens d'attribution des droits sont décrits. ✓ Les moyens de contrôle et d'alerte permettent d'identifier les failles sécuritaires.
• Déploiement de solutions cryptographiques	C.2.2.3. Mettre en place les solutions potentielles de sécurité (VPN[12], chiffrement de portable, protection de fichiers, …) en identifiant les besoins (classification et usage) afin de renforcer la protection des informations contre les accès indus et risques de divulgation accidentelle ou malveillante.	✓ Un exemple de solution cryptographique	✓ Les besoins (classification et usage) sont identifiés. ✓ Les règles et recommandations issues du Référentiel Général de Sécurité sont listées. ✓ L'état de l'art est respecté. ✓ La solution cryptographique répond aux besoins sécuritaires et n'est pas un frein opérationnel

[12] VPN : virtual private network, terminologie métier pour désigner un réseau privé virtuel

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Application des référentiels normatifs et règlementaires en matière de sécurisation du SI (par ex : RGPD[9], ISO[10] 27001, ISO 27002, ISO 270003, SOC 1[11], SOC2, SOC3 …etc.)	C.2.2.4 Intégrer la sécurité dans l'organisation en appliquant les prérequis, les normes et les bonnes pratiques en matière de sécurisation du système d'information (SI) en vigueur, afin de garantir un niveau de sécurité en adéquation avec la politique de sécurité du système d'information (PSSI)	✓ Un exemple d'intégration de normes/réglementation	✓ Le choix du référentiel normatif ou réglementaire (RGPD, ISO 27001, ISO 27002, ISO 270003, SOC1, SOC2, SOC3 …etc.) est expliqué et justifié au regard de la PSSI de l'organisation. ✓ L'intégration dans l'organisation des grandes directives du référentiel choisi est décrite.
A.2.3 Déploiement des différents projets de sécurité conformément à la PSSI • Elaboration d'un processus de validation des changements	C.2.3.1. Définir un processus de validation des changements en évaluant la demande de changement, en analysant son impact et en accompagnant les parties prenantes aux changements afin de garantir la sécurité du système d'information (SI) dans le déploiement des projets.	✓ Le processus de validation des changements	✓ Les grandes étapes du processus de validation des changements sont décrites. ✓ Les modalités d'évaluation du changement permettent de couvrir la mesure de l'impact et les moyens d'accompagnement à mettre en place.

[9] RGPD : Règlement Général de la Protection des données
[10] ISO : International Organization for Standardization, terminologie métier pour désigner l'organisation internationale de normalisation
[11] SOC : System and Organization Control, terminologie métier pour indiquer un centre opérationnel de sécurité

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Définition du contenu fonctionnel d'un projet de sécurité (objectifs, ressources, démarche suivie, règlementation applicable, …)	C.2.3.2. Elaborer les spécifications fonctionnelles d'un projet de sécurité en tenant compte de l'exposition au risque, des ressources nécessaires et de la politique de sécurité du système d'information (PSSI) afin de définir les spécifications techniques	✓ Une note de cadrage du projet de sécurité	✓ Les objectifs du projet sont clairs, concis. ✓ Le cadre règlementaire du projet est présenté le cas échéant. ✓ La démarche de sécurité suivie est expliquée ✓ Le concept de développement durable est pris en compte le cas échéant. ✓ Les principales ressources nécessaires à la bonne réalisation du projet sont identifiées.
• Planification d'un projet de sécurité	C.2.3.3. Planifier un projet de sécurité du système d'information (SI) en tenant compte des ressources humaines, matérielles, financières nécessaires à l'exécution du projet afin de définir l'ordonnancement détaillé des tâches, clarifier les responsabilités des différents acteurs et assurer une bonne coordination.	✓ Un planning du projet	✓ Le choix de la méthodologie de gestion de projet (Agile, Lean…) est justifié ✓ Le planning est construit au moyen d'outils adaptés (ex : diagramme de Gantt, PERT, rétroplanning ...) ✓ La durée du projet est réaliste au regard de la taille du projet. ✓ Le planning du projet est découpé en phases, en tâches ou lots. ✓ Les jalons du projet sont établis selon les objectifs et livrables fixés

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**	
		Modalité d'évaluation	**Critères d'évaluation**
			✓ Les tâches sont assignées aux différents membres de l'équipe selon leurs compétences (matrice RACI[13], RASCI[14] ...) et tiennent compte des personnes en situation d'handicap. ✓ Les points de vigilance sont soulignés
• Pilotage tout au long d'un projet de la performance de la sécurité du système d'information (SI).	C.2.3.4. Piloter l'avancement d'un projet après avoir défini les outils de suivi adaptés, en assurant un suivi régulier de l'avancée, en communiquant sur les indicateurs clés afin de garantir la performance du projet dans le respect des délais, de la qualité et des coûts.	✓ La mise en œuvre du suivi de projet	✓ L'outil de suivi utilisé est en adéquation avec le projet et la méthodologie choisie. ✓ Les jalons de suivi sont présentés. ✓ L'outil de suivi permet de contrôler la performance du projet. ✓ Les tableaux de bord et les indicateurs sont clairs, lisibles et permettent de suivre l'avancement du projet (suivi des délais, suivi des couts…). ✓ Le choix des indicateurs qualitatifs et quantitatifs est argumenté et cohérent avec les enjeux du projet.

[13] RACI : la matrice RACI permet d'affecter les rôles et responsabilités de chacun (Responsible, Accountable, Consulted, Informed ou en français Réalisateur, Approbateur responsable, Consulté, Informé)
[14] RASCI : la matrice RASCI permet d'affecter les rôles et responsabilités de chacun (Responsible, Accountable, Support, Consulted, Informed ou en français Réalisateur, Approbateur responsable, Support, Consulté, Informé)

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Livraison d'un projet	C.2.3.5. Réaliser une campagne de tests conformément au cahier de recettes afin de s'assurer que le projet réponde aux attentes et spécifications définies.	✓ Un exemple de test pour s'assurer de la conformité du projet aux spécifications	✓ Le test présenté permet de mesurer la conformité du projet de sécurité par rapport aux objectifs de départ. ✓ Les indicateurs de performance sont cohérents avec les objectifs du test.
	C.2.3.6. Rédiger la documentation projet en tenant compte des spécificités du projet et son impact dans l'organisation du système d'information (SI) afin de permettre la livraison du projet	✓ La liste des documents à fournir dans le cadre de la livraison d'un projet	✓ La liste des documents accompagnant la livraison du projet est complète et adaptée à l'organisation. ✓ Les différents types de documents sont listés et pour chaque document sont précisés : - Le rôle du document - Le périmètre de diffusion - La cible visée

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**	
		Modalité d'évaluation	**Critères d'évaluation**
BLOC 3 : MAINTENIR LA SECURITE DU SYSTEME D'INFORMATION D'UNE ORGANISATION			
		Type d'évaluation : Mise en situation professionnelle réelle ou fictive. **Attendus du candidat :** Sur la base d'une analyse d'un système d'information d'une organisation de son choix, le candidat présente les éléments permettant de maintenir la sécurité du système d'information. **Livrable attendu :** A l'aide d'un support de présentation, le candidat présente oralement son analyse du système d'information et ses préconisations sur les éléments à mettre en place. La présentation comprendra :	
A3.1. Mise en place d'un processus de sensibilisation • Définition d'une politique de sensibilisation de cybersécurité dans l'organisation	C.3.1.1. Elaborer une politique de sensibilisation aux risques de cybersécurité en impliquant tous les collaborateurs afin de prévenir les incidents de cybersécurité au sein de l'organisation.	✓ La note de cadrage de la politique de sensibilisation	✓ Les objectifs sont précisés. ✓ La règlementation applicable à l'organisation est identifiée le cas échéant. ✓ Les parties prenantes visées (utilisateurs, contractants…) et leurs fonctions dans l'organisation sont identifiées

Référentiel d'activités **décrit les situations de travail et les activités exercées, les métiers ou emplois visés**	**Référentiel de compétences** **identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités**	**Référentiel d'évaluation** **définit les critères et les modalités d'évaluation des acquis**	
		Modalité d'évaluation	**Critères d'évaluation**
			✓ Les thèmes abordés en fonction du public visé sont décrits. ✓ Les moyens mis en œuvre (cours en ligne, présentations, simulations d'hameçonnage...) sont décrits. ✓ Les moyens d'évaluation des actions de sensibilisation sont déterminés et tiennent compte des personnes en situation de handicap ✓ Les fréquences d'actions de sensibilisation sont définies.
• Elaboration des supports de sensibilisation • Sensibilisation du personnel aux risques liés à l'usage des systèmes d'information	C.3.1.2. Déployer la politique de sensibilisation aux risques de cybersécurité en élaborant des supports et des méthodes de formation adaptés afin d'aider les utilisateurs du système d'information (SI) à s'approprier la culture de cybersécurité mise en place.	✓ Un exemple d'action de sensibilisation	✓ Le choix du type de support tient compte des personnes en situation de handicap ✓ Le message est clair et adapté aux parties prenantes visées. ✓ Les bonnes pratiques d'hygiène informatique (réglementations, PSSI ...) sont précisées L'objectif de l'action de sensibilisation est clairement formalisé

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**	
		Modalité d'évaluation	**Critères d'évaluation**
A3.2. Contrôle et Surveillance continue de la sécurité • Définition d'une politique de contrôle et de surveillance continue du système d'information (SI).	C.3.2.1. Mettre en place une politique de contrôle et de surveillance continue en tenant compte des menaces identifiées et de la PSSI afin de s'assurer de l'efficacité des mesures de protection.	✓ La note de cadrage de la politique de contrôle et surveillance	✓ Les menaces identifiées sont prises en compte dans la politique de contrôle et surveillance ✓ La liste des composants du SI à surveiller est précisée et justifiée. ✓ Les dispositifs permettant de surveiller la sécurité du SI sont déterminés (journalisation, système SIEM[15]…)
• Définition des Indicateurs de surveillance	C.3.2.2. Identifier, en étudiant le contexte du système d'information, les paramètres à connaitre et mesurer, qui permettent soit par leur valeur absolue, soit par leur variation d'évaluer le niveau de sécurité du système d'information	✓ La présentation d'un indicateur	✓ Le contexte du système est décrit. ✓ Le choix de l'indicateur est expliqué au regard des objectifs de contrôle et de surveillance. ✓ Les seuils d'alerte associés à cet indicateur sont décrits et justifiés.

[15] SIEM : Security Information and Event Management, terminologie métier qui désigne le système de gestion des informations et des événements de sécurité

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Mise en œuvre des moyens de surveillance et de contrôles	C.3.2.3. Mettre en place une surveillance et un contrôle à l'aide de dispositifs de sécurité et d'outils de supervision afin de s'assurer du fonctionnement continu et efficace des dispositifs de sécurité mis en place.	✓ Un exemple de moyen de surveillance et de contrôle	✓ Le moyen de surveillance et de contrôle est décrit. ✓ Le moyen de surveillance et de contrôle permet de s'assurer du bon fonctionnement de la ressource concernée.
• Détection et documentation des vulnérabilités	C.3.2.4. Documenter les vulnérabilités détectées par les moyens techniques de surveillance en analysant les risques associés afin de décrire les mesures à prendre.	✓ Une étude d'une vulnérabilité	✓ Le(s) moyen(s) de surveillance permettant de détecter la vulnérabilité est/sont précisé(s). ✓ Les critères de vulnérabilité sont analysés. ✓ Les risques associés sont déterminés.
• Traitement des vulnérabilités identifiées	C.3.2.5. Corriger les vulnérabilités identifiées en élaborant un plan d'actions approprié afin de restaurer la sécurité du système concerné	✓ Un plan d'actions de correction associé	✓ Les actions sont établies, attribuées et séquencées. ✓ Les parties prenantes et les ressources impactées sont identifiées ✓ Le plan d'action permet la correction de la vulnérabilité.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
A3.3. Réalisation d'audit de sécurité • Définition d'un plan d'audit • Réalisation d'audit de sécurité • Pilotage et coordination d'audits externes	C.3.3.1. Définir le plan d'audit en délimitant le périmètre à étudier et en prenant en compte les points critiques afin de s'assurer de la bonne application des politiques et procédures de sécurité.	✓ Un plan d'audit technique ou organisationnel au choix du candidat	✓ Le périmètre de l'audit est défini. ✓ Le référentiel applicable est identifié. ✓ Les objectifs de l'audit sont formalisés.
• Réalisation du rapport d'audit • Plan d'action des actions correctives à mettre en place (plan de remédiation)	C.3.3.2. Rédiger un rapport d'audit en précisant la démarche suivie, les actions entreprises les vulnérabilités détectées afin d'établir un plan de remédiation	✓ Un exemple de vulnérabilité identifiée lors d'un audit et sa solution de remédiation	✓ L'écart constaté par rapport aux configurations acceptables est clairement formalisé. ✓ La criticité de l'écart est déterminée en fonction de la vulnérabilité identifiée et de son risque associé ✓ Le référentiel de classification de l'écart est précisé. (CWE[16], CVSS[17]) ✓ La solution de remédiation proposée répond à la vulnérabilité identifiée.

[16] CWE : Common Weakness enumeration, terminologie métier qui désigne l'énumération des faiblesses communes
[17] CVSS : Common Vulnerability Scoring systeme, terminologie métier qui désigne un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Suivi des actions correctives (remédiation)	C.3.3.3. Suivre la mise en œuvre des actions correctives en vérifiant leur efficacité afin d'augmenter la sécurité de l'organisation	✓ La méthode d'évaluation de l'efficacité de l'action de remédiation	✓ La méthode d'évaluation de l'efficacité de l'action de remédiation est expliquée. ✓ L'efficacité de l'action de remédiation est démontrée.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
BLOC 4 : GERER LES INCIDENTS ET CRISES DE CYBERSECURITE D'UNE ORGANISATION			
		Type d'évaluation : Mise en situation professionnelle réelle ou fictive **Attendus du candidat :** A partir d'un cas d'organisation réel ou fictif de son choix, le candidat présente l'organisation mise en place afin de gérer les incidents et crise de cybersécurité en illustrant ses propos à l'aide d'un ou plusieurs exemples d'incidents. **Livrable attendu :** le candidat remet au jury un dossier comprenant les éléments suivants :	
A4.1. Analyse et qualification de l'incident : • Détection des incidents	C.4.1.1. Identifier les incidents de sécurité détectés à l'aide des outils de supervision au sein d'un Security Operations Center (SOC) afin de permettre leur analyse.	✓ Un processus de détection d'incident	✓ Les grandes étapes du processus sont détaillées. ✓ Les rôles des différents acteurs sont décrits. ✓ Les outils de détection sont décrits. (ex : SIEM[18], SIM[19] …etc.)

[18] SIEM ou Security Information and Event Management, terminologie métier qui désigne la gestion des informations et des événements de sécurité
[19] SIM ou Security Information Management, terminologie métier qui désigne la gestion des informations de sécurité

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**	
		Modalité d'évaluation	**Critères d'évaluation**
• Identification et analyse de l'incident • Analyse de l'impact de l'exploitation • Analyse de l'évènement déclencheur et du point d'entrée • Etude du déroulé étape par étape de l'incident (timeline)	C.4.1.2. Réaliser une analyse forensique de l'incident en collectant les preuves afin de permettre la présentation d'une synthèse destinée aux décideurs.	✓ Un rapport d'analyse forensique	✓ Les sources d'informations et les anomalies associées sont identifiées ✓ Le périmètre concerné est déterminé ✓ Les impacts sur l'organisation sont évalués. ✓ Les preuves de la cyberattaque sont collectées. ✓ L'évènement déclencheur est expliqué ✓ Le scénario de l'attaque (point d'entrée, timeline…) est reconstitué. ✓ L'ensemble des étapes réalisées qui ont permis de récupérer les preuves sont décrites. ✓ Le rapport est présenté sous forme chronologique pour faire concorder les hypothèses et les preuves datées

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**	
		Modalité d'évaluation	**Critères d'évaluation**
A4.2. Développement et mise en œuvre des activités appropriées pour bloquer ou atténuer une menace ou intrusion (action de sauvegarde) / remédiation • Blocage ou atténuation des menaces du système d'information ou du réseau • Adaptation des moyens mis en œuvre selon la menace ou l'intrusion • Mise en œuvre des solutions techniques pour préserver le système d'information.	C4.2.1. Utiliser des moyens d'atténuation, de réparation ou de récupération du système d'information (SI), en utilisant des outils dédiés afin d'assurer la continuité du bon fonctionnement du SI et la préservation des données.	✓ Présentation des moyens de blocage ou préservation mis en œuvre	✓ Les moyens de blogage ou préservation mis en œuvre sont détaillées. ✓ Les moyens de blogage ou préservation mis en œuvre répondent à la menace/intrusion.
• Application d'un protocole de tests pour vérifier le bon fonctionnement de la procédure mise en place	C4.2.2 Réaliser un protocole de tests afin de vérifier que les moyens et solutions techniques mis en œuvre permettent de corriger une faille informatique.	✓ Un exemple de test	✓ Le déroulé du test est expliqué ✓ Les résultats du test permettent de démontrer l'efficacité des moyens et solutions mis en œuvre.
• Mise en œuvre des plans de restauration	C4.2.3. Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de restaurer toutes les capacités ou les Services du système d'information (SI).	✓ Une description du plan de restauration du SI	✓ Les actions de restauration permettent la restauration des capacités du SI ✓ Les rôles des parties prenantes et les ressources impliquées sont décrits. ✓ Le séquençage des actions est justifié.

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**	
		Modalité d'évaluation	**Critères d'évaluation**
A4.3. Gestion des équipes en cas de crise • Encadrement de l'équipe de crise • Coordination des actions de maitrise du risque • Suivi et pilotage des opérations	C4.3.1 Donner des instructions et un plan d'actions détaillé pour répondre aux intrusions en maintenant la communication avec les équipes et la direction afin de piloter la gestion de crise.	✓ Un plan d'actions de gestion de crise	✓ Le plan d'actions de gestion de crise est clair, concis. ✓ Les rôles des parties prenantes et les ressources impliquées sont décrits. ✓ Le séquençage des actions est justifié.
A.4.4. Communication de crise avec les parties prenantes • Élaboration du plan de communication de crise interne et/ou externe • Information des parties prenantes • Communication aux organismes d'état si nécessaire	C.4.4.1. Définir un plan de communication de crise en identifiant les parties prenantes à informer et les canaux de communication à utiliser afin de réagir de manière efficace en cas de crise.	✓ Un plan de communication de crise	✓ Toutes les parties prenantes internes et externes y compris les organismes d'état sont identifiés ✓ Le niveau d'informations à communiquer est précisé pour chaque partie prenante ✓ Les délais à respecter sont établis
• Présentation d'une synthèse destinée aux décideurs • Adaptation des procédures du SI en tirant les conclusions de l'incident	C.4.4.2 Présenter une synthèse de l'incident à partir des éléments présents dans le rapport d'analyse forensique afin de faire valider les adaptations des procédures du système d'information (SI) à déployer.	✓ Une synthèse de l'incident	✓ L'incident est décrit. ✓ L'analyse de l'incident est détaillée. ✓ Les actions à mettre en œuvre pour éviter la répétition de l'incident sont décrites. ✓ La restitution de l'analyse de l'incident est adaptée à un public non technique.