Référentiel d'activités et de compétences

Cybersécurité et réseaux

CyActivités et tâches	Compétences professionnelles (associées aux activités et tâches)	Compétences ou capacités qui seront évaluées (aptitudes professionnelles)	Modalités d'évaluation	Critères d'évaluation
Activité 1. Audit de sécurité du système d'information				
A1T1. Analyse de la sécurité du système d'information d'une organisation	**A1T1C1.** Analyser les enjeux économiques et juridiques liés aux risques d'altération du système d'information pour comprendre la nécessité d'une politique de sécurité informatique efficiente. **A1T1C2.** Analyser la stratégie de cybersécurité de l'organisation et la politique de gestion des données et des traitements pour vérifier la conformité de l'organisation au regard de la loi (protection des données, loi défense, loi de programmation militaire, …). **A1T1C3.** Identifier et caractériser les menaces de dysfonctionnement du système d'information pour en analyser les causes, les impacts, estimer leur probabilité de survenance et dresser la cartographie des risques.	**A1T1Ce1.** Analyser les enjeux économiques et juridiques liés aux risques d'altération du système d'information pour comprendre la nécessité d'une politique de sécurité informatique efficiente. **A1T1Ce2.** Analyser la stratégie de cybersécurité de l'organisation et la politique de gestion des données et des traitements pour vérifier la conformité de l'organisation au regard de la loi (protection des données, loi défense, loi de programmation militaire, …). **A1T1Ce3.** Identifier et caractériser les menaces de dysfonctionnement du système d'information pour en analyser les causes, les impacts, estimer leur probabilité de survenance et dresser la cartographie des risques.	**A1Me1. Evaluation de l'activité 1** **Mode :** Etude de cas sur la conduite d'un audit de sécurité. **Durée :** 1 heure. **Modalités d'évaluation :** Il est remis au candidat une étude de cas dans laquelle sont présentés une organisation, son mode de fonctionnement et ses installations matérielles et logicielles. Il est demandé au candidat d'organiser un audit de sécurité et de rédiger un rapport en analysant l'existant,	**A1Cr1**. Les enjeux économiques et juridiques liés à la défaillance du système sont exposés. **A1Cr2**. L'analyse de la stratégie de cybersécurité du cas étudié est correcte.. **A1Cr3**. Le candidat caractérise les risques de dysfonctionnement et en justifie les causes. **A1Cr4**. L'analyse de la gestion des identités, des accès et des flux d'informations est correcte et complète.

Référentiel d'activités et de compétences

Cybersécurité et réseaux

A1T2. Définition des objectifs de fiabilité et de sécurité du système d'information.	**A1T1C4.** Analyser la gestion des identités et des accès et les flux d'informations critiques de l'activité d'un système d'information pour repérer les composants les plus sensibles à protéger. **A1T2C1.** Synthétiser les analyses liées à la vulnérabilité du système d'information pour fixer et hiérarchiser les objectifs en matière de cybersécurité du système d'information en tenant compte des enjeux économiques et juridiques liés à l'arrêt du système. **A1T2C2.** Définir les indicateurs de fiabilité du système d'information pour disposer d'éléments factuels à mesurer afin d'éclairer les choix stratégiques à opérer en matière de sécurité. **A1T2C3.** Rédiger le rapport d'audit de sécurité du système d'information (enjeux, cartographie des risques, cybermenaces) pour poser le cadre de référence et de réflexion pour améliorer la cybersécurité de l'organisation en s'appuyant sur des éléments tangibles.	**A1T1Ce4.** Analyser la gestion des identités et des accès et les flux d'informations critiques de l'activité d'un système d'information pour repérer les composants les plus sensibles à protéger. **A1T2Ce1.** Synthétiser les analyses liées à la vulnérabilité du système d'information pour fixer et hiérarchiser les objectifs en matière de cybersécurité du système d'information en tenant compte des enjeux économiques et juridiques liés à l'arrêt du système. **A1T2Ce2.** Définir les indicateurs de fiabilité du système d'information pour disposer d'éléments factuels à mesurer afin d'éclairer les choix stratégiques à opérer en matière de sécurité. **A1T2Ce3.** Rédiger le rapport d'audit de sécurité du système d'information (enjeux, cartographie des risques, cybermenaces) pour poser le cadre de référence et de réflexion pour améliorer la cybersécurité de l'organisation en s'appuyant sur des éléments tangibles.	caractérisant les cyber-menaces et en identifiant les composants les plus sensibles. Le candidat aura à livrer son rapport d'audit avec la cartographie des risques, les enjeux, les vulnérabilités et l'analyse des cyber-risques.	**A1Cr5**. L'analyse de l'existant est pertinente. **A1Cr6**. Les menaces sont identifiées dans leur intégralité. **A1Cr7**. Les composants les plus sensibles sont identifiés. **A1Cr8**. La cartographie des risques est complète. **A1Cr9**. Le rapport d'audit est exhaustif et complet.

Référentiel d'activités et de compétences

Cybersécurité et réseaux

Activités et tâches	Compétences professionnelles (associées aux activités et tâches)	Compétences ou capacités qui seront évaluées (aptitudes professionnelles)	Modalités d'évaluation	Critères d'évaluation
Activité 2. Élaboration et déploiement d'une politique de sécurité du système d'information				
A2T1. Elaboration de la politique de sécurité du système d'information	**A2T1C1.** Exploiter le rapport d'audit de l'organisation pour identifier les axes correctifs à rechercher et proposer des solutions de protection du système d'information. **A2T1C2**. Caractériser les solutions et les outils du marché pour la gestion des process de sécurité afin de sélectionner les réponses et les produits adéquats. **A2T1C3**. Elaborer la politique de sécurité du système d'information pour répondre aux exigences de l'audit en préconisant et en validant les solutions de sécurité les plus pertinentes. **A2T1C4**. Evaluer les ressources humaines et matérielles à mobiliser pour concevoir le plan de déploiement de la politique de sécurité et préparer	**A2T1Ce1.** Exploiter le rapport d'audit de l'organisation pour identifier les axes correctifs à rechercher et proposer des solutions de protection du système d'information. **A2T1Ce2**. Caractériser les solutions et les outils du marché pour la gestion des process de sécurité afin de sélectionner les réponses et les produits adéquats. **A2T1Ce3**. Elaborer la politique de sécurité du système d'information pour répondre aux exigences de l'audit en préconisant et en validant les solutions de sécurité les plus pertinentes. **A2T1Ce4**. Evaluer les ressources humaines et matérielles à mobiliser pour concevoir le plan de déploiement de la politique de sécurité et préparer	**A2Me1. Evaluation de l'activité 2** **Mode :** Etude de cas sur un rapport d'audit à exploiter pour en dégager des solutions et une politique de sécurité. **Durée :** 1 heure d'écrit et 20 minutes de soutenance orale **Modalités d'évaluation :** Il est remis au candidat un rapport d'audit à exploiter. Le candidat est chargé de l'analyser pour élaborer une nouvelle politique de sécurité. Le candidat aura à rechercher des solutions de prévention et	**A2Cr1**. L'exploitation du rapport d'audit est correcte. **A2Cr2**. Les axes d'amélioration à rechercher sont identifiés. **A2Cr3.** La recherche de solutions et de produits de sécurisation est constatée. **A2Cr4.** Les solutions proposées sont pertinentes. **A2Cr5.** Le candidat propose une politique de sécurité cohérente

A2T2. Déploiement de la politique de sécurité	sa mise en œuvre. **A2T2C1**. Déployer les solutions techniques retenues pour répondre aux exigences de la politique de sécurité décidée afin de protéger l'organisation face aux menaces identifiées. **A2T2C2**. Analyser les différents protocoles réseaux (IP, IMCP, UDP, TCP, …) pour concevoir des architectures sécurisées. **A2T2C3**. S'approprier les techniques et l'ingénierie de la cryptographie pour élaborer un protocole cryptographique de protection des données en s'appuyant sur une méthode formelle. **A2T2C4**. Mettre en place les pare-feux client/serveur des applications web pour détecter et bloquer les trafics anormaux afin de protéger les serveurs web contre les cyber-attaques. **A2T2C5**. Mettre en place les contrats de maintenance et de backup des	sa mise en œuvre. **A2T2Ce1**. Déployer les solutions techniques retenues pour répondre aux exigences de la politique de sécurité décidée afin de protéger l'organisation face aux menaces identifiées. **A2T2Ce2**. Analyser les différents protocoles réseaux (IP, IMCP, UDP, TCP, …) pour concevoir des architectures sécurisées. **A2T2Ce3**. S'approprier les techniques et l'ingénierie de la cryptographie pour élaborer un protocole cryptographique de protection des données en s'appuyant sur une méthode formelle. **A2T2Ce4**. Mettre en place les pare-feux client/serveur des applications web pour détecter et bloquer les trafics anormaux afin de protéger les serveurs web contre les cyber-attaques. **A2T2Ce5**. Mettre en place les contrats de maintenance et de backup des	de protection en tenant compte de l'existant et des vulnérabilités identifiées. Il aura à évaluer les ressources humaines et matérielles à mettre en regard des mesures préconisées. Le candidat sera interrogé à l'oral sur les protocoles réseaux et de cryptographie, les firewalls et les procédures de back-up et de PCA/PRA à mettre en place.	et adaptée au cas étudié. **A2Cr6.** L'évaluation des ressources matérielles et humaines est correcte. **A2Cr7**. Les protocoles réseaux sont connus. **A2Cr8**. L'ingénierie de cryptographie est acquise. **A2Cr9**. Le candidat est en capacité de gérer des firewall adaptés au système d'information présenté. **A2Cr10**. La description des procédures de back-up, de PCA et de PRA est conforme aux attendus et en cohérence avec la

	matériels pour assurer l'actualisation du système d'information et prévenir la perte accidentelle de données. **A2T2C6.** Concevoir les procédures en cas d'interruption de service pour organiser les plans de continuité et de reprise d'activité (PCA et PRA) permettant de minimiser les préjudices sur l'activité et les services de l'organisation.	matériels pour assurer l'actualisation du système d'information et prévenir la perte accidentelle de données. **A2T2Ce6.** Concevoir les procédures en cas d'interruption de service pour organiser les plans de continuité et de reprise d'activité (PCA et PRA) permettant de minimiser les préjudices sur l'activité et les services de l'organisation.		politique de sécurité préconisée.

Activités et tâches	**Compétences professionnelles** (associées aux activités et tâches)	**Compétences ou capacités qui seront évaluées** (aptitudes professionnelles)	**Modalités d'évaluation**	**Critères d'évaluation**
Activité 3. Pilotage et suivi de la politique de sécurité du système d'information				
A3T1. Accompagnement des équipes dans la mise en œuvre de la politique de sécurité du système	**A3T1C1.** Identifier un référent interne et expliciter ses missions pour garantir la bonne gestion de la politique de sécurité et accompagner l'organisation dans la durée. **A3T1C2.** Mettre en place et animer les instances de pilotage pour superviser le	**A3T1Ce1.** Identifier un référent interne et expliciter ses missions pour garantir la bonne gestion de la politique de sécurité et accompagner l'organisation dans la durée. **A3T1Ce2.** Mettre en place et animer les instances de pilotage pour superviser le	**A3Me1. Evaluation de l'activité 3** **Mode :** Evaluation orale sur la gestion du déploiement de la politique de sécurité et son suivi. **Durée :** 20 minutes de	**A3Cr1**.Les conditions de réussite pour la gestion et le suivi d'un projet de sécurisation sont identifiées. **A3Cr2**. L'intérêt de sensibiliser les acteurs (collaborateurs) aux

d'information.	déploiement, son planning et le respect des objectifs au regard de la politique de sécurité de l'organisation. **A3T1C3.** Informer et sensibiliser l'ensemble des collaborateurs à la politique de sécurité de l'organisation pour diffuser la culture de la vigilance face aux cyber-risques et transmettre les bonnes pratiques en matière d'utilisation du système d'information.	déploiement, son planning et le respect des objectifs au regard de la politique de sécurité de l'organisation. **A3T1Ce3.** Informer et sensibiliser l'ensemble des collaborateurs à la politique de sécurité de l'organisation pour diffuser la culture de la vigilance face aux cyber-risques et transmettre les bonnes pratiques en matière d'utilisation du système d'information.	préparation et 30 minutes d'évaluation orale. **Modalités d'évaluation :** Il est demandé au candidat de présenter à l'oral les conditions de réussite d'une gestion et d'un suivi efficaces en matière de politique de sécurité. Le candidat précise les activités et les objectifs des instances de pilotage. Il explique l'intérêt d'informer et de sensibiliser les collaborateurs sur la vigilance sécuritaire continue à exercer. Le candidat montre sa capacité à mettre en place des audits internes et à assurer la continuité de l'activité en cas d'incident. Il est en mesure d'assurer une veille technologique sur le	bonnes pratiques est compris. **A3Cr3.** Les activités et les objectifs des instances de pilotage sont acquis. **A3Cr4**. Le candidat montre sa capacité à mettre en place des audits internes et à mettre à l'épreuve ses solutions pour en vérifier la pertinence et les limites. **A3Cr5.** Les plans de continuité de service exposés sont adaptés. **A3Cr6.** Le candidat est en mesure d'assurer une veille permanente pour améliorer ses connaissances et proposer des améliorations continues en matière
A3T2. Suivi et pilotage de la politique de sécurité de l'organisation	**A3T2C1.** Concevoir les protocoles d'audits internes et les planifier pour vérifier l'adéquation des solutions aux exigences définies par la loi et aux normes de sécurisation attendues par l'organisation. **A3T2C2.** Mettre en place le système de contrôle et les procédures de traitement des incidents pour remédier rapidement à toute anomalie détectée en veillant à assurer leur traçabilité. **A3T2C3.** Concevoir des mises à	**A3T2Ce1.** Concevoir les protocoles d'audits internes et les planifier pour vérifier l'adéquation des solutions aux exigences définies par la loi et aux normes de sécurisation attendues par l'organisation. **A3T2Ce2.** Mettre en place le système de contrôle et les procédures de traitement des incidents pour remédier rapidement à toute anomalie détectée en veillant à assurer leur traçabilité. **A3T2Ce3.** Concevoir des mises à		

	l'épreuve de la politique de sécurité pour améliorer, si besoin, les solutions techniques et les procédures organisationnelles déployées. **A3T2C4.** Mettre à jour les composants techniques du système pour intégrer les évolutions fonctionnelles et techniques (architecture, logiciels, nouveaux services, ...) en veillant à la cohérence avec la politique de sécurité. **A3T2C5.** Assurer une veille technologique sur l'évolution des cyber-risques pour être en capacité d'actualiser ses compétences et d'en faire bénéficier l'organisation.	l'épreuve de la politique de sécurité pour améliorer, si besoin, les solutions techniques et les procédures organisationnelles déployées. **A3T2Ce4.** Mettre à jour les composants techniques du système pour intégrer les évolutions fonctionnelles et techniques (architecture, logiciels, nouveaux services, ...) en veillant à la cohérence avec la politique de sécurité. **A3T2Ce5.** Assurer une veille technologique sur l'évolution des cyber-risques pour être en capacité d'actualiser ses compétences et d'en faire bénéficier l'organisation.	secteur de la cybersécurité et de proposer des améliorations au sein d'une organisation.	de sécurité des systèmes d'information.