RESPONSABLE DE LA SECURITE DES SYSTEMES D'INFORMATION DE SANTE (DU)

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*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
Bloc I : Définition, planification et mise en place d'une organisation et d'un système de management de la sécurité de l'information			
I.1 Définir le périmètre et les enjeux du Système de Management des SI de Santé	**Compétence I.1** : Identifier les réglementations relatives à la cybersécurité et s'appliquant à la protection des données de santé en France en utilisant les informations mises à disposition (plateforme institutionnelle, plateforme de veille active,…)	Mise en situation pratique : L'évaluation proposée sous forme d'une épreuve mobilisant l'ensemble des compétences du bloc sera axée sur l'étude d'une situation réelle ou simulée relative à la mise en place d'un système de management de la sécurité de l'information dans une organisation de santé. Épreuve individuelle écrite : La restitution sous forme d'un écrit individuel permet d'évaluer le niveau de maitrise du référentiel d'implémentation d'un système de management de la sécurité de l'information ISO27001. Elle prendra la forme de questions à choix multiples et de questions ouvertes. Épreuve individuelle orale : La restitution sous forme orale individuelle permet au futur RSSIS d'évaluer sa capacité à convaincre à la fois un spécialiste et un auditoire constitué de ces pairs, de l'efficience de sa démarche.	Le candidat doit être en capacité de rédiger une documentation de synthèse, démontrant : - qu'il a identifié et qu'il s'est approprié la réglementation relative à la sécurité de l'information sur les SI en santé, - qu'il a compris les enjeux et qu'il maitrise la définition, la planification et l'implémentation d'un Système de Management de la sécurité de l'information à travers la formalisation des documents requis dans la norme ISO27001. - qu'il est en mesure d'assurer la conformité réglementaire de son SI en pilotant le SMSI à travers l'établissement de plan projets, de plan d'actions, de tableaux de bords et indicateurs. Lors de la présentation orale, le candidat est évalué selon : - la qualité de son analyse de la situation étudiée (auprès d'un spécialiste) sur des problématiques de sécurité de l'information, - la cohérence de ses recommandations sur l'implémentation du SMSI en argumentant sur les enjeux pour l'organisation ou l'établissement - la pertinence des solutions techniques et organisationnelles proposées
	Compétence I.2 : Déterminer le rôle et planifier les missions des référents métier de l'organisme, en étant attentif au personnel de statut RQTH, pour organiser efficacement la gestion et la mise en œuvre des mesures de sécurité de l'information		
I.2 Documenter le Système de Management des SI de santé	**Compétence I.3 :** Rédiger et communiquer la politique de sécurité des systèmes d'information (PSSI), les procédures de sécurité et les guides composant le Système de Management de la Sécurité de l'Information en respectant le formalisme et le mode de transmission requis par la norme ISO27001.		
I.3 Piloter le Système de Management des SI de santé	**Compétence I.4 :** Définir et piloter les activités, les projets et l'ensemble des moyens humains, organisationnels, financiers, et techniques nécessaires à assurer la sécurité du SI de santé telle que décrit dans la norme ISO27001.		

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*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
	Compétence I.5 : Animer des réunions avec une ou plusieurs équipes projet pour le déploiement des mesures de sécurité organisationnelles et techniques (en collaboration avec des spécialistes comme les informaticiens, juristes, services généraux…)		
	Compétence I.6 : Rédiger un cahier des charges techniques et fonctionnelles (CCTP) ou une demande de proposition (Appel d'offres) afin de trouver les fournisseurs adaptés pour maitriser les risques de sécurité de l'information		
I.4 Assurer le suivi de la performance et l'amélioration du Système de Management des SI de Santé	**Compétence I.7 :** Construire, alimenter et mettre à jour des tableaux de bord pour assurer le suivi de la performance du système de management de la sécurité de l'information de santé.		
	Compétence I.8 : Évaluer le niveau de sécurité du système d'information sur la base de rapports et résultats d'audits techniques interne ou externe et des solutions de sécurité en place.		
Bloc II : Recensement, analyse et traitement des risques liés à la sécurité du SI de santé			
II.1 Recenser les risques pesant sur les systèmes d'information de santé	**Compétence II.1** : Préparer et conduire des audits par rapport à des référentiels internes ou externes relatifs à la sécurité de l'information.	<u>Étude d'un cas réel ou reconstitué</u> : L'évaluation proposée mobilisant l'ensemble des compétences du bloc sera axée sur la gestion des risques SI à partir d'une situation réelle ou reconstituée survenue dans une organisation, un établissement ou un service en santé.	Le candidat doit être en mesure de rédiger une documentation de synthèse, démontrant : - qu'il s'est bien approprié la démarche de cartographie et d'analyse de risques informationnels selon la méthode EBIOS RM.
	Compétence II.2 : Animer des interviews avec les référents métiers, en étant attentif au personnel de statut RQTH, afin de recueillir les besoins de sécurité et identifier les écarts aux obligations		

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*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
	requises par l'ANSSI, en prenant en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire).	Restitution écrite et orale : La restitution donne lieu à la production d'une synthèse écrite réalisée en groupes. ↳ Ce travail d'analyse, de réflexion et de formalisation permet de placer le futur RSSI en Santé dans une situation de réaliser une analyse de risques du SI d'un organisme de santé et de la confronter ensuite avec les solutions mises en œuvre dans les conditions réelles. ↳ La restitution orale de ce travail sera réalisée individuellement pour permettre de tester les futurs managers sur leur capacité à contextualiser, synthétiser et argumenter les résultats et les recommandations (plan d'action) à l'issue d'une analyse de risques SI.	- qu'il a pris des décisions pertinentes en justifiant ses choix d'une manière convaincante pour établir son plan de traitement des risques - que ses livrables présentent une démarche d'analyse de risques cohérente, reproductible et comparable. - que ses résultats et plans d'action sont bien alignés avec les enjeux de l'étude. - qu'il a su communiquer les risques et les bonnes pratiques de sécurité aux différentes parties prenantes et utilisateurs du système d'information. La soutenance orale consiste en une restitution contradictoire individuelle des différentes solutions envisagées sur un cas identique. Les candidats seront évalués selon : – Leur capacité à faire un compte rendu complet et synthétique de leur analyse des risques sur le SI dans le cadre de la confrontation à une situation identique, – La cohérence des solutions envisagées et leur capacité à convaincre sur leur bien-fondé par rapport aux enjeux pour l'organisation ou l'établissement.
	Compétence II.3 : Rédiger un rapport d'audit proposant des actions d'améliorations organisationnelles et techniques afin de sécuriser le SI de santé.		
II.2 Identifier les risques pesant sur les systèmes d'information de santé	**Compétence II.4 :** Identifier et analyser les risques pesant sur les systèmes d'information de santé en appliquant la méthode d'analyse de risques de l'ANSSI, Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS).		
II.3 Évaluer les risques pesant sur les systèmes d'information de santé	**Compétence II.5 :** Évaluer les risques pesant sur les systèmes d'information de santé en prenant en compte leur probabilité d'occurrence et les impacts en termes de disponibilité, intégrité et confidentialité sur les informations de santé.		
	Compétence II.6 : Prioriser les risques et proposer des solutions organisationnelles et techniques pour traiter les risques conformément à la méthode d'analyse de risques EBIOS.		
II.4 Etablir un plan de traitement des risques pesant sur les systèmes d'information de santé	**Compétence II.7 :** Rédiger les documents synthétisant les besoins de sécurité, les menaces, les objectifs de sécurité ainsi que le plan de traitement des risques en respectant les attendus de la méthode EBIOS.		
	Compétence II.8 : Organiser et animer des réunions pour présenter les résultats de l'analyse de risques à des décideurs non experts en sécurité de l'information afin de		

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*	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
	les convaincre d'investir dans la sécurisation des systèmes d'information de santé (direction de l'établissement, partenaires…).		
II.5 Sensibiliser les parties prenantes à la sécurité et la protection des données de santé.	**Compétence II.9 :** Piloter un programme de sensibilisation à la cybersécurité et de conduite du changement auprès des utilisateurs finaux pour favoriser l'adoption des bonnes pratiques et améliorer la culture de sécurité de l'organisme.		

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*	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
Bloc III : Prévenir et gérer les incidents de sécurité de l'information			
III.1 Prévenir les incidents de sécurité de l'information	**Compétence III.1 :** Réaliser une veille technologique du SI sur les dernières vulnérabilités, les menaces et une veille technique relative aux solutions de sécurité.	Épreuve individuelle écrite : L'évaluation est proposée sous forme d'une épreuve écrite mobilisant l'ensemble des compétences du bloc. Elle portera sur la maitrise des réflexes et bonnes pratiques en termes de gestion des incidents de sécurité de l'information impactant la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données de santé.	Le candidat doit être en capacité de rédiger une documentation de synthèse, démontrant : - Son aptitude à faire face à la découverte d'un Incident de sécurité en élaborant des procédures et des tableaux de bord de gestion des incidents accompagnés de fiches action/reflexe. - Son aptitude à faire face à la survenue d'une situation de crise en élaborant des procédures (Plan de reprise d'activité, plan de sauvegarde...), et la réalisation d'un plan de communication de crise. - La pertinence de la démarche et des solutions qu'il propose (réactivité, flexibilité, niveau de protection, mode dégradé et reprise d'activité). - L'adaptation de son discours sur la gestion des incidents au niveau de compréhension des différents interlocuteurs.
	Compétence III.2 : Élaborer une méthodologie de réponse à incident pour faire face aux risques de sécurité physique ou numérique et réagir rapidement et efficacement en cas d'attaques.		
	Compétence III.3 : Établir les procédures relatives à la prévention et réactions à un incident de sécurité telles que la procédure de gestion des incidents, le plan de reprise d'activité ou le plan de sauvegarde du système d'information de santé		
	Compétence III.4 : Assurer la formation et l'entraînement des référents métiers, en étant attentif au personnel de statut RQTH, afin d'améliorer la capacité de l'organisme de santé à réagir à une cyberattaque et limiter les impacts de celle-ci.		
III.2 Gérer les incidents de sécurité et organiser la gestion de crise liée à la sécurité de l'information.	**Compétence III.5 :** Définir un processus d'escalade et une organisation de crise afin de traiter les incidents urgents de sécurité conformément à la réglementation en vigueur concernant les systèmes d'information de santé.		
	Compétence III.6 : Communiquer les étapes de résolution de l'incident aux parties intéressées		
	Compétence III.7 : Organiser des retours d'expériences afin de capitaliser sur les incidents passés et améliorer le traitement		

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*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
	des incidents à venir (clients, managers, direction générale, institutions…)		