

Responsable de la sécurité des systèmes d'information de santé (DU)

RNCP37767 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31045, 31008, 42881
Code(s) ROME	M1801
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	19/07/2023
Date d'échéance	19/07/2026

Certificateur(s)

UNIVERSITE D'ANGERS · SIRET : 19490970100303

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le Responsable de la Sécurité des Systèmes d'Information de Santé assure le pilotage de la démarche de sécurité de l'information au sein de l'organisation de santé. Il définit ou décline, selon la taille de l'organisation et les résultats de l'analyse de risques, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des référents métiers et/ou de la direction de l'organisme. Il s'assure de la mise en place des solutions de sécurité en prenant en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) pour garantir la protection des données et le niveau de sécurité des systèmes informatiques en santé.

À ce titre, le RSSI santé doit être capable de conseiller ou de convaincre les décideurs et les référents métiers, des spécialistes informatiques, des utilisateurs du SI de l'importance et de la nécessité des mesures de sécurité. Il doit savoir formaliser les documents relatifs au système de management de la sécurité de l'information et conduire des démarches et plans pour atteindre un niveau de protection acceptable.

ACTIVITÉS VISÉES

Bloc 1 : Définition, planification et mise en place d'une organisation et d'un système de management de la sécurité de l'information

- Définir le périmètre et les enjeux du Système de Management des SI de Santé
- Documenter le Système de Management des SI de santé
- Piloter le Système de Management des SI de santé
- Assurer le suivi de la performance et l'amélioration du Système de Management des SI de Santé

Bloc 2 : Recensement, analyse et traitement des risques liés à la sécurité du SI de santé

- Recenser les risques pesant sur les systèmes d'information de santé
- Identifier les risques pesant sur les systèmes d'information de santé
- Évaluer les risques pesant sur les systèmes d'information de santé
- Etablir un plan de traitement des risques pesant sur les systèmes d'information de santé
- Sensibiliser les parties prenantes à la sécurité et la protection des données de santé

Bloc 3 : Prévention et gestion des incidents de sécurité de l'information

- Prévenir les incidents de sécurité de l'information

- Gérer les incidents de sécurité et organiser la gestion de crise liée à la sécurité de l'information

COMPÉTENCES ATTESTÉES

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,...)

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

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.

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.

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...)

Rédiger un cahier des charges techniques et fonctionnelles (CCTP) ou une demande de proposition (Appel d'offres) afin de trouver les fournisseurs adaptés pour maîtriser les risques de sécurité de l'information

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.

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.

Préparer et conduire des audits par rapport à des référentiels internes ou externes relatifs à la sécurité de l'information.

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 requises par l'ANSSI, en prenant en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire).

Rédiger un rapport d'audit proposant des actions d'améliorations organisationnelles et techniques afin de sécuriser le SI de santé.

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).

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.

Prioriser les risques et proposer des solutions organisationnelles et techniques pour traiter les risques conformément à la méthode d'analyse de risques EBIOS.

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.

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 les convaincre d'investir dans la sécurisation des systèmes d'information de santé (direction de l'établissement, partenaires...).

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.

Réaliser une veille technologique du SI sur les dernières vulnérabilités, les menaces et une veille technique relative aux solutions de sécurité.

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.

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

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.

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.

Communiquer les étapes de résolution de l'incident aux parties intéressées

Organiser des retours d'expériences afin de capitaliser sur les incidents passés et améliorer le traitement des incidents à venir (clients, managers, direction générale, institutions...)

Blocs de compétences

RNCP37767BC01 — Définition, planification et mise en place d'une organisation et d'un système de management de la sécurité de l'information

LISTE DE COMPÉTENCES

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,...)

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

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.

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.

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...)

Rédiger un cahier des charges techniques et fonctionnelles (CCTP) ou une demande de proposition (Appel d'offres) afin de trouver les fournisseurs adaptés pour maîtriser les risques de sécurité de l'information

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.

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.

MODALITÉS D'ÉVALUATION

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 maîtrise 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'efficacité de sa démarche.

RNCP37767BC02 — Recensement, analyse et traitement des risques liés à la sécurité du SI de santé

LISTE DE COMPÉTENCES

Préparer et conduire des audits par rapport à des référentiels internes ou externes relatifs à la sécurité de l'information.

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 requises par l'ANSSI, en prenant en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire).

Rédiger un rapport d'audit proposant des actions d'améliorations organisationnelles et techniques afin de sécuriser le SI de santé.

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).

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.

Prioriser les risques et proposer des solutions organisationnelles et techniques pour traiter les risques conformément à la méthode d'analyse de risques EBIOS.

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.

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 les convaincre d'investir dans la sécurisation des systèmes d'information de santé (direction de l'établissement, partenaires...).

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.

MODALITÉS D'ÉVALUATION

Étude d'un cas réel ou reconstitué : 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.

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.

RNCP37767BC03 — Prévention et gestion des incidents de sécurité de l'information

LISTE DE COMPÉTENCES

Réaliser une veille technologique du SI sur les dernières vulnérabilités, les menaces et une veille technique relative aux solutions de sécurité.

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.

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

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.

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.

Communiquer les étapes de résolution de l'incident aux parties intéressées

Organiser des retours d'expériences afin de capitaliser sur les incidents passés et améliorer le traitement des incidents à venir (clients, managers, direction générale, institutions...)

MODALITÉS D'ÉVALUATION

Épreuve individuelle écrite : L'évaluation est proposée sous forme d'une épreuve écrite mobilisant l'ensemble des compétences du bloc. Elle portera sur la maîtrise 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.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Dans le secteur Santé, le RSSI exerce au sein de :

- Établissements de santé publics et privés (CHRU, hôpitaux, cliniques, laboratoires, maison de santé, EHPAD, ...)
- Groupements Hospitaliers de Territoire (GHT) ou Groupements d'Intérêt Public (GIP) en Santé
- Agence du Numérique en Santé (ANS) ou Agence Régionale de Santé (ARS)
- Industrie pharmaceutique, cosmétique / bien-être
- Service (éditeur logiciel, télémedecine, ...)
- Structures de conseil ou d'audit en Santé

La taille des organisations concernées peut aller de la Très Petite Entreprise (TPE) au grand groupe international. Il peut s'agir d'un organisme public ou privé.

TYPE D'EMPLOIS ACCESSIBLES

- Responsable Sécurité des SI dans un Groupement de Coopération Sanitaire ou un Groupement Hospitalier de Territoire
- Responsable de la sécurité de systèmes d'information (RSSI) ou Référent Sécurité de l'Information (RSI)
- Gestionnaire de la sécurité des données, des réseaux et des systèmes
- Expert(e) sécurité informatique
- Administrateur(trice) sécurité informatique
- Consultant(e) ou auditeur(trice) en sécurité de l'information de santé

RÉGLEMENTATIONS D'ACTIVITÉ

L'exercice du métier de RSSI de Santé ne nécessite pas de détention d'une habilitation ou d'une certification spécifique. Cependant les établissements de santé peuvent être soumis, dans certaines conditions, à des réglementations spécifiques tels que le NIS pour les Organismes d'Importance Vitales (OIV) ou les Organismes de Services Essentiels (OSE). es réglementations sont intégrées à la certification professionnelle. Et en étant sur le territoire européen et traitant de données personnelles de citoyens européens, les organismes dans lesquels exerceront les candidats seront soumis au Règlement Général sur la Protection des Données (RGPD), ce dont tient compte le contenu du référentiel de compétences, qui est également aligné avec les attentes de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et répond aux attentes des organismes de santé à travers l'intégration des standards ISO27001, ISO27002 et ISO27005/EBIOS RM. Enfin les réglementations spécifiques au domaine de la santé telles que la certification HAS des établissements de santé ou la certification HDS pour les organismes qui hébergent ou traitent des données de santé pour le compte d'établissements sont également intégrées à la certification professionnelle.

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Modérée (3/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 4 sur 5.
Facteurs principaux	Intensité d'embauche, Inadéquation géographique
Salaire médian (mensuel)	2 419 €
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée)
Projets de recrutement (BMO 2026)	9 549
Jugés difficiles à recruter	46 %
Emplois saisonniers	3 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le public visé par le dispositif concerne les professionnels suivants (liste non exhaustive) :

- Responsables qualité (RAQ)
- Gestionnaire de risques (RM)
- Chefs de projet informatique systèmes/applications/data manager
- Directeurs de systèmes d'information
- Médecins (Département d'information médicale ...)

Pour accéder à la formation, les candidats doivent être au moins titulaire d'un diplôme de niveau 6 en lien avec le domaine concerné par la certification et présenter un projet professionnel motivé en lien avec le diplôme (CV détaillé et lettre de motivation).

Les candidats ne justifiant pas d'une qualification de niveau 6, doivent justifier d'une qualification de niveau 5 et

présenter une expérience professionnelle significative avec le domaine concerné par la certification (CV détaillé et lettre de motivation).

Toutes les candidatures sont soumises à une commission de recrutement, présidée par le responsable de la formation/certification, et les candidats seront conviés à un entretien de sélection. Les décisions motivées de la commission sont formalisées sur un procès-verbal rédigé par le responsable de la formation/certification.

PRÉREQUIS À LA VALIDATION

Pour valider la certification, le candidat doit avoir validé l'ensemble des blocs de compétences par capitalisation ou par validation des acquis de l'expérience (VAE).

COMPOSITION DU JURY — FORMATION CONTINUE, VAE

- Le responsable de la certification RSSIS, président du jury : PAST à l'Université d'Angers et Chief Information Security Officer (CISO)
- Un enseignant-chercheur d'une autre formation : Responsable de la formation professionnelle de Polytech Angers
- Deux professionnels qualifiés, extérieurs à l'équipe pédagogique et exerçant dans le domaine de la sécurité de l'information en Santé :
 - o Référent régional Sécurité des Systèmes d'Information de Santé
 - o Responsable Sécurité des Systèmes d'Information dans un Groupement Hospitalier de Territoire (GHT)

Base légale

Date de décision	19/07/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	19/07/2026
Date de dernière délivrance possible	19/07/2030

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37767/>

Entrées et sorties de formation

Entrées en formation	3
Parcours menés à terme	3
Taux d'achèvement	100 %
Période	03/2026 – 07/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	3
Montant total engagé	9 762 €
Coût moyen par dossier	3 254 €
Durée moyenne	43 h
Période	03/2026
France compétences	95 %
France Travail	3 %

Reste à charge titulaire

2 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.