

Expert en sécurité des systèmes d'information

RNCP34342 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326m
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	16/12/2019
Date d'échéance	16/12/2024

Certificateur(s)

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION · SIRET : 13000766900018

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ECOLE SUP INFORMATIQUE ELECTRON AUTOMAT	31134913800017	Former et organiser l'évaluation
INSTITUT MINES TELECOM - TELECOM SUDPARIS	18009202500055	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'expert en sécurité des systèmes d'information (ESSI) doit garantir la sécurité des systèmes d'information tout au long de leur cycle de vie, en intervenant aux différentes étapes : depuis l'expression de besoin jusqu'à l'exploitation, en passant par le développement.

À ce titre, l'ESSI doit notamment être conscient des enjeux de la sécurité et prendre en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) de la problématique SSI. Il doit être capable de conseiller ou de convaincre, en tant qu'interlocuteur des décideurs et acteurs d'un projet, des spécialistes informatiques, des administrateurs et des responsables de la sécurité des systèmes d'information (RSSI). Il doit savoir formaliser les documents relatifs à la SSI et élaborer et conduire des démarches et plans, notamment pour l'audit ou l'homologation de systèmes.

ACTIVITÉS VISÉES

L'ESSI exerce les activités suivantes :

- Formaliser les besoins de sécurité en en prenant en compte toutes les dimensions ;
- Élaborer des dispositifs techniques de sécurité correspondant aux besoins de sécurité des systèmes d'information ;
- Estimer ou faire estimer le niveau de sécurité d'un système d'information ;
- Gérer la sécurité d'un système d'information (notamment en réagissant aux incidents de sécurité pendant la phase d'exploitation, pour en réduire les impacts).

COMPÉTENCES ATTESTÉES

Compétences attestées :

- Identifier et collecter les enjeux de la sécurité d'un système d'information en prenant en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) de la problématique SSI ;

- Mener, de manière formelle, l'analyse de risque d'un système d'information complexe afin d'identifier les besoins en sécurité, les menaces et les risques et d'en déduire les objectifs de sécurité ;
- Conseiller ou convaincre un donneur d'ordre dans le domaine de la SSI ;
- Identifier et préciser les risques liés à un système d'information. Analyser les forces et faiblesses des produits de sécurité, notamment ceux mettant en œuvre des mécanismes cryptographiques ;
- Établir une architecture et définir un ensemble de solutions techniques pour protéger un système d'information selon des besoins en sécurité connus et selon les grands axes de la défense en profondeur ;
- Estimer soi-même le niveau de sécurité d'un système d'information ;
- Diriger et préparer un audit ; prendre en compte les résultats, élaborer et conduire un plan d'action ;
- Élaborer une démarche d'homologation et bien la conduire ;
- Contribuer à maintenir la sécurité d'un système, en relation avec les acteurs du projet, les spécialistes informatiques, les administrateurs et les RSSI ;
- Veiller sur les dernières vulnérabilités, menaces et produits de sécurité et les analyser. Évaluer les impacts d'une vulnérabilité ou d'une menace ;
- Gérer un incident de sécurité.

Blocs de compétences

RNCP34342BC01 — Définir et formaliser les besoins de sécurité des systèmes d'information

LISTE DE COMPÉTENCES

- Identifier et collecter les enjeux de la sécurité d'un système d'information en prenant en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) de la problématique SSI.
- Mener, de manière formelle, l'analyse de risque d'un projet relatif à un système d'information complexe afin d'identifier les besoins en sécurité, les menaces et les risques, et d'en déduire les objectifs de sécurité.
- Conseiller ou convaincre un donneur d'ordre (autorité, chef de projet, chef DSI...) dans le domaine de la SSI.

MODALITÉS D'ÉVALUATION

Exercices (écrits ou oraux) qui portent sur les enjeux de sécurité d'un système d'information.

Évaluation du candidat sous la forme d'une mise en situation d'analyse de risque (réalisée en groupe) avec restitution des résultats (sous forme orale).

Enfin, le candidat effectue une mise en situation professionnelle (sur plusieurs mois) sur un sujet SSI, dont la problématique contient une composante technique importante, et donnant lieu à la rédaction d'un mémoire et d'une soutenance orale devant un jury. Ce dernier est composé d'experts SSI, de représentants de divers ministères, et de responsables de la formation.

RNCP34342BC02 — Élaborer un dispositif technique correspondant aux besoins de sécurité

LISTE DE COMPÉTENCES

- Identifier et préciser les risques liés à un système d'information. Analyser les forces et faiblesses des produits de sécurité, notamment ceux mettant en œuvre des mécanismes cryptographiques.
- Établir une architecture et définir un ensemble de solutions techniques pour protéger un système d'information selon des besoins de sécurité connus et selon les grands axes de la défense en profondeur. Faire des recommandations relatives à la SSI auprès d'un spécialiste technique d'un système d'information.

MODALITÉS D'ÉVALUATION

Le candidat est évalué sur ses compétences en cryptographie, sécurité des systèmes, et des réseaux au moyen d'examens écrits et de questions orales portant sur des sujets techniques en SSI.

Le candidat effectue également un mini-projet en sécurité logicielle.

Enfin le candidat effectue une mise en situation professionnelle (sur plusieurs mois) sur un sujet SSI, dont la problématique contient une composante technique importante, et donnant lieu à la rédaction d'un mémoire et d'une soutenance orale devant un jury.

RNCP34342BC03 — Estimer ou faire estimer le niveau de sécurité d'un système d'information

LISTE DE COMPÉTENCES

- Estimer soi-même le niveau de sécurité d'un système d'information.
- Diriger et préparer un audit. Prendre en compte les résultats d'un audit. Élaborer et conduire un plan d'action.
- Élaborer une démarche d'homologation et bien la conduire.

MODALITÉS D'ÉVALUATION

Réalisation d'audits sous forme de travaux pratiques. L'objectif est de superviser la réalisation d'un audit technique, d'organiser et choisir différentes prestations d'audit (type de prestation, contour retenu, etc.).

Les candidats doivent ensuite appliquer la méthodologie d'audit, ainsi que des méthodes plus détaillées selon les domaines.

On évalue également les candidats par le biais de la réalisation d'un mini-projet sur une étude de cas portant sur une analyse de risque et une homologation (avec restitution orale).

RNCP34342BC04 — Gérer la sécurité d'un système d'information

LISTE DE COMPÉTENCES

- Contribuer à maintenir la sécurité d'un système, en relation avec les acteurs du projet, les spécialistes informatiques, les administrateurs et les RSSI.
- Veiller sur les dernières vulnérabilités, menaces et produits de sécurité et les analyser. Évaluer les impacts d'une vulnérabilité ou d'une menace.
- Gérer un incident de sécurité.

MODALITÉS D'ÉVALUATION

Le candidat est évalué sur la réalisation d'un mini-projet sur le thème « management de la sécurité » et sa restitution orale.

Le candidat doit écrire et soutenir à l'oral une étude bibliographique sur une vulnérabilité liée à la SSI, identifiée par des articles scientifiques et/ou grand public (les sources d'information sont majoritairement en anglais).

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Fonction publique et assimilé (établissements publics par exemple), entreprises privées concernées par le domaine des systèmes d'information (secteurs défense, informatique, télécommunications) ou ayant de forts enjeux en SSI (opérateurs d'importance vitale en particulier).

TYPE D'EMPLOIS ACCESSIBLES

L'expert en sécurité des systèmes d'information (ESSI) est destiné à occuper un emploi dans le domaine de la sécurité des systèmes d'information, par exemple en tant qu'architecte SSI au sein d'une équipe de maîtrise d'ouvrage, responsable de la sécurité des systèmes d'information, responsable de SOC, analyste de la menace, intégrateur de sécurité ou encore conseiller SSI pour des décideurs. De manière plus spécifique à l'administration, un ESSI a vocation à occuper des postes dans le domaine de la maîtrise d'ouvrage de projets à forte composante SSI ou d'officier de programme, de chef d'équipe SSI, ou encore de fonctionnaire de sécurité des systèmes d'information (FSSI) dans un ministère.

RÈGLEMENTATIONS D'ACTIVITÉ

L'exercice de l'activité peut nécessiter des habilitations particulières selon les secteurs (par exemple, habilitation de niveau Confidentiel Défense ou supérieur, conformément aux dispositions de l'instruction ministérielle 1300).

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour intégrer la formation délivrée par l'ANSSI, il est nécessaire d'obtenir un résultat satisfaisant au test d'admission (sur la base d'un questionnaire (voir le document 2018_01_09_RESSI_submission_cyberfizzbuzz.pdf sur le site

internet de la conférence RESSI) avec entretien oral (environ deux à trois heures) portant sur des questions scientifiques et techniques, sur le parcours professionnel... Ce questionnaire permet de valider les prérequis scientifiques et techniques dans les domaines des mathématiques, des réseaux, des systèmes, des langages (C essentiellement), etc. ; travailler dans la fonction publique (fonctionnaire ou contractuel), un OIV ou OSE (sous conditions) ; être habilité au niveau "Confidentiel défense" minimum ; être de nationalité française ; avoir le soutien écrit de sa hiérarchie et l'accord du HFDS du ministère d'appartenance ou de tutelle.

COMPOSITION DU JURY — FORMATION INITIALE, CANDIDATURE INDIVIDUELLE, VAE

Au minimum : le directeur général de l'ANSSI, deux représentants des sous-directions de l'ANSSI, deux représentants des ministères (dont le ministère des armées), un représentant du corps enseignant externe à l'ANSSI, un représentant du CFSSI, au moins un représentant d'un établissement partenaire ESSI, un représentant industriel, un représentant ESSI en activité.

COMPOSITION DU JURY — FORMATION CONTINUE

Au minimum : le directeur général de l'ANSSI, deux représentants des sous-directions de l'ANSSI, deux représentants des ministères (dont le ministère des armées), un représentant du corps enseignant externe à l'ANSSI, un représentant du CFSSI, au moins un représentant d'un établissement partenaire ESSI, un représentant industriel, un représentant ESSI en activité.

Base légale

Date de décision	16/12/2019
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	16/12/2024

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2017	10	1	100 %	70 %
2016	10	2	100 %	80 %
2015	9	1	100 %	80 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP4245

NOUVELLE(S) CERTIFICATION(S)

RNCP42504

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.ssi.gouv.fr/entreprise/formations/titre-essi/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/34342/>

Entrées et sorties de formation

Entrées en formation	5
Parcours menés à terme	6

Taux d'achèvement	120 %
Période	04/2022 – 08/2025

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

Demande CPF — formations engagées

Dossiers CPF engagés	6
Montant total engagé	42 885 €
Coût moyen par dossier	7 148 €
Durée moyenne	1527 h
Période	06/2021 – 09/2024
France compétences	58 %
Reste à charge titulaire	36 %
Entreprise	7 %

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