

La certification s'adresse aux RSI Responsables des Systèmes d'Information, RSSI Responsables de la Sécurité des Systèmes d'information, Consultants en Cybersécurité ou en Sécurité de l'Information, Administrateurs Systèmes et réseaux sécurité qui, dans le cadre d'une évolution de leurs pratiques ou missions, sont amenés à réaliser des audits de systèmes de management de la sécurité de l'information conformes à la norme ISO/CEI 27001.

Afin de garantir la sécurité des systèmes de l'information, les entreprises sont amenées à mettre en place un système de management de la sécurité de l'information conforme à la norme ISO 27001.

Pour contrôler la bonne mise en œuvre de cette conformité au sein des organisations, la certification "Audit de systèmes de management de la sécurité de l'information (ISO/CEI 27001 Lead Auditor)" permet aux professionnels évoluant dans le domaine de la sécurité de l'information ou ayant déjà réalisé des audits d'attester :

- qu'ils possèdent les connaissances et compétences complémentaires, nécessaires à la pratique de l'audit de systèmes de management de la sécurité de l'information conformes à la norme ISO/CEI 27001 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences », en tant que membre d'équipe d'audit ou seul.
- et qu'ils possèdent le savoir-faire nécessaire à la conduite d'un audit, défini dans la norme ISO/CEI 19011 « Lignes directrices pour l'audit des systèmes de management » et dans les guides associés (ISO, IAF, EA).

Prérequis :

- Maîtriser les connaissances de base des Systèmes de l'Information et de leurs systèmes de sécurité.
- Avoir au minimum 1 an d'expérience dans son poste ou métier (en lien avec les Systèmes de l'Information et systèmes de sécurité)

Candidat en situation de handicap : Tout candidat peut saisir le référent handicap du certificateur pour aménager les modalités d'évaluation et obtenir l'assistance d'un tiers lors de l'évaluation. Les supports et le matériel nécessaires à la réalisation des évaluations pourront être adaptés. Sur le conseil du référent Handicap et dans le respect des spécifications du référentiel, le format de la modalité pourra être adapté.

REFERENTIEL DE COMPETENCES	REFERENTIEL D'ÉVALUATION	
	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
Audit de systèmes de management de la sécurité de l'information (ISO/CEI 27001 Lead Auditor)		
<p>C1. Analyser les menaces, vulnérabilités et risques du système d'information, y compris ceux liés à l'utilisation de l'IA, en prenant en considération les aspects humains, organisationnels et technologiques de l'organisation, et en s'appuyant sur la documentation et les processus liés, afin de définir le périmètre et les points de contrôle de l'audit selon ISO 27001.</p>	<p><u>Mise en situation professionnelle reconstituée, sous la forme d'une étude de cas écrite, complétée par une séquence orale de questionnement du jury d'évaluation</u></p> <p>Mise en situation professionnelle Cette mise en situation se rapporte à un cas réel anonymisé d'une organisation qui prévoit un audit de sécurité de son système d'information en adéquation avec les normes ISO 27001 et les normes associées (1) et ISO 19011. Le cas d'entreprise décrit et présente le contexte spécifique, les particularités, les enjeux et le système d'information de l'entreprise. Dans l'étude de cas, à l'écrit, il est demandé au candidat de :</p> <ul style="list-style-type: none"> - Analyser les menaces, vulnérabilités et risques du système d'information, y compris ceux liés à l'utilisation de l'IA (en lien avec C1) - Constituer une équipe d'audit et élaborer un plan d'audit structuré (en lien avec C2) - Évaluer la conformité du Système de Management de la Sécurité de l'Information (en lien avec C3) - Formaliser et suivre les recommandations issues de l'audit (en lien avec C4) <p>La production réalisée par le candidat durant l'étude de cas sera transmis au jury d'évaluation en amont de la session orale de questionnement.</p>	<p>Cr1.1. Les informations collectées par le candidat sont factuelles et documentées, issues de sources fiables internes et externes comprenant la documentation et les processus liés.</p> <p>Cr1.2. Le candidat identifie et explicite les menaces et vulnérabilité plausibles du système d'information : celles-ci sont décrites, différenciées et mises en lien avec le secteur d'activité et les aspects humains, organisationnels et technologiques de l'organisation de l'organisation par le candidat. Les menaces et vulnérabilités liées à l'utilisation de l'IA le cas échéant sont prises en compte.</p> <p>Cr1.3. Le candidat caractérise les risques du système d'information de façon conforme :</p> <ul style="list-style-type: none"> - il fait le lien avec le système de sécurité de l'information de l'organisation ; - il relie les risques avec les vulnérabilités et les menaces préalablement identifiées ; - il prend en compte les risques d'audit ; - il formule les points critiques (non-conformités majeures et mineures) <p>Cr1.4. Le candidat définit le périmètre de l'audit et liste les points de contrôle en faisant le lien avec les clauses et annexes de la norme ISO 27001.</p>

C2. Organiser l'audit du Système de Management de la Sécurité de l'Information (SMSI), en constituant une équipe d'audit pluridisciplinaire adaptée aux points de contrôle identifiés et en élaborant un plan d'audit structuré à partir des normes ISO 19011, ISO 27007 et ISO 27008 et intégrant des modalités d'interaction adaptés pour les personnes en situation de handicap, **afin d'en assurer une conduite conforme, inclusive et couvrant l'ensemble des activités du périmètre défini.**

Questionnement du jury d'évaluation

A l'oral, il est demandé au candidat de répondre aux questions du jury d'évaluation portant notamment sur les éléments de l'étude de cas réalisée pouvant nécessiter des approfondissements, des éclairages ou des justifications.

(1) les normes associées sont les normes de la famille des ISO 27000 (27001, 27002, 27003, 27004, 27005, 27006, 27007, 27008) et la norme ISO 19011.

Cr2.1. Le candidat compose une équipe d'audit pluridisciplinaire d'au moins 2 personnes au profil complémentaire en veillant à l'absence de conflit d'intérêt. Il justifie ses choix notamment en faisant explicitement le lien entre les compétences de l'auditeur, les points de contrôle préalablement identifiés et les exigences de la norme ISO 19011.

Cr2.2. Le plan d'audit élaboré par le candidat est structuré selon les normes ISO 19011 et ISO 27007. Celui-ci comprend au minimum 4 de ces éléments :

- l'approche d'audit,
- l'identification des parties prenantes
- le rôle de chaque partie prenante
- la définition des objectifs et la mise en lien des objectifs avec les points de contrôles à effectuer
- les techniques et outils à mobiliser

Cr2.3. Le candidat justifie sa sélection d'outils et de techniques en s'appuyant sur la norme ISO 27008.

Cr2.4. Les modalités d'interaction et d'accessibilité pour les personnes en situation de handicap sollicitées au cours de l'audit sont prévues par le candidat (par exemple supports adaptés, communication inclusive...)

C3. Évaluer la conformité du Système de Management de la Sécurité de l'Information, en mettant en œuvre le plan d'audit, en identifiant et en caractérisant les non-conformités, tout en s'appuyant sur les preuves disponibles et les outils et méthodes spécifiques, **afin de proposer des actions correctives conformes à la norme ISO/CEI 27001.**

Cr3.1. Le candidat détaille et explicite de manière exhaustive et précise les non-conformités relevées lors de la mise en œuvre du plan d'audit. Celles-ci sont caractérisées et classées par degré de non-conformité (majeure/mineure).

Cr3.2. Les preuves d'audit sont collectées et documentées par le candidat. La mobilisation des outils et techniques spécifiques sélectionnés est décrite et justifiée.

		<p>Cr3.3. Des actions correctives sont proposées par le candidat pour chaque non-conformité et issues des 114 mesures liées à la sécurité de l'information en conformité avec la norme ISO/CEI 27001. Leur alignement avec les écarts constatés et leur applicabilité est justifié par le candidat.</p>
<p>C4. Formaliser et suivre les recommandations issues de l'audit, en rédigeant un rapport final structuré selon la norme 19011, accessible aux utilisateurs en situation de handicap, intégrant une priorisation des mesures à appliquer, et en établissant un plan de suivi des actions opérationnel, afin de faciliter et de contrôler la mise en œuvre et le niveau de réalisation des actions de mise en conformité du SMSI selon la norme ISO 27001.</p>		<p>Cr4.1. Le rapport d'audit formalisé par le candidat est structuré selon la norme 19011. Celui-ci comprend au minimum ces éléments : faits observés, preuves recueillies, conformités, non-conformités caractérisées, points forts, actions correctives. L'ordre des actions à appliquer en fonction de l'importance de la non-conformité y est défini par le candidat.</p> <p>Cr4.2. Le candidat propose un plan de suivi des actions opérationnel incluant : une formalisation des actions à appliquer, une échelle du niveau d'avancement et des échéances de rappels et de contrôle. Le candidat y sélectionne des actions systématiques à réaliser dans une démarche d'amélioration continue.</p> <p>Cr4.3. Le rapport d'audit intègre au moins 2 éléments ou adaptations d'accessibilité pour les utilisateurs en situation de handicap. Par exemple : format alternatif, police de caractère accessible, structure spécifique, ajout de pictogrammes...</p>