RÉFÉRENTIELS DE COMPÉTENCES ET D'ÉVALUATION
ISO/CEI 27001 Lead Auditor

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 ISO 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 et les qualités personnelles nécessaires à la conduite d'un audit, définies dans la norme ISO/CEI 19011 « Lignes directrices pour l'audit des systèmes de management » et dans les guides associés (ISO, IAF, EA).

Les activités en lien avec cette certification sont :
- Concevoir un audit du Système de Management de la Sécurité de l'Information avec une approche holistique, qui permette une analyse ciblée et précise
- Réaliser un audit en mobilisant les parties prenantes et en explorant les preuves disponibles pour identifier des actions correctives
- Élaborer un rapport final qui priorise les actions à réaliser et favorise l'engagement des parties prenantes
- Apprécier la mise en œuvre et le niveau de réalisation des actions pour pérenniser les résultats obtenus

Référentiel de compétences	Référentiel d'évaluation	
Compétences	**Modalités d'évaluation**	**Critères d'évaluation**
C1. Caractériser les menaces et vulnérabilités qui pèsent sur le système d'information de l'organisation, en prenant en considération les aspects humains, organisationnels et technologiques pour cibler le périmètre d'audit selon ISO 27001	L'évaluation se fait à travers une mise en situation professionnelle reconstituée. **Cette mise en situation se rapporte à un cas réel anonymisé d'une organisation qui prévoit un audit** de sécurité du 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. **Le candidat prépare une présentation sous forme de diaporama** du projet d'audit d'un système de management de la sécurité d'information selon ISO 27001 en distinguant 2	**Cr1. Critères pour la compétence C1** Le candidat identifie les menaces et vulnérabilité plausibles conformément à la norme ISO 27005 : - il détermine les menaces et vulnérabilités en les décrivant, les différenciant et en les mettant en lien avec le secteur d'activités de l'organisation - il identifie les points de contrôle en faisant le lien avec les clauses et annexes de la norme ISO 27001 - il choisit les outils et méthodes appropriées en s'appuyant sur les normes pertinentes (19011, 27007, 27008)

C2. Déterminer les risques en analysant la documentation et les processus de l'organisation afin de définir les points de contrôles de l'audit selon ISO 27001	de la sécurité d'information selon ISO 27001 en distinguant 2 parties : - Partie 1 : Présentation du plan d'audit élaboré conformément à la norme ISO 27001 et la norme ISO 19011 (C1 à C4) - Partie 2 : Présentation des rapports de non conformité et proposition d'actions correctives associées aux non-conformités et applicables au cas présenté (niveau de priorité, échéances, personnes référentes…) (C5 à C7) **Le candidat présente ce document au jury de certification comme s'il le défendait devant un comité de direction**. Lors de cette soutenance un accent particulier est mis sur les compétences de savoir agir en situation.	**Cr2. Critères pour la compétence C2** Le candidat caractérise les risques de façon conforme : - il relie les risques au système de sécurité de l'information de l'organisation ; - il relie les risques avec les vulnérabilités et les menaces préalablement identifiés ; - il prend en compte les risques d'audit ; - il formule les points critiques (non conformités majeures et mineures)
C3. Composer une équipe d'audit pluridisciplinaire en fonction du périmètre et des points de contrôles définis afin de réaliser un audit conforme à la norme ISO 19011		**Cr3. Critères pour la compétence C3** Le candidat compose l'équipe d'audit de manière appropriée : - il relie les compétences de l'auditeur avec les exigences de la norme ISO 19011 ; - il anticipe les conflits d'intérêts ; - il définit les rôles de chaque membre de l'équipe et veille à leur complémentarité ;
C4. Concevoir un plan d'audit en s'appuyant sur les outils et méthodes d'audit pertinents selon ISO 19011, ISO 27007 et 27008 afin de couvrir l'ensemble des activités du périmètre d'audit		**Cr4. Critères pour la compétence C4** Le candidat formalise un plan d'audit conformément aux normes ISO 19011 et ISO 27007 : - il décrit l'approche d'audit ; - il identifie les parties prenantes et leur rôle ; - il définit les objectifs clairement définis et les met en lien avec les points de contrôles à effectuer ; - il sélectionne les techniques et outils à intégrer dans l'audit en conformité avec ISO 27008 ;
C5. Identifier et apprécier les non conformités en mettant en œuvre le plan d'audit et en utilisant les outils de communication et d'audit pertinents pour proposer des actions correctives en conformité avec la norme ISO 27001		**Cr5. Critères pour la compétence C5** Le candidat détaille de manière exhaustive les non-conformités : - il décrit les non-conformités de façon précises ; - il classe les non-conformités par degré de non conformité (majeure/mineure) ; - il identifie les actions correctives pertinentes parmi les 114 mesures liées à la sécurité de l'information en conformité avec la norme ISO 27001 ;

C6. Formaliser ses recommandations dans un rapport final en priorisant les actions à mener afin de favoriser l'engagement des parties prenantes		**Cr6. Critères pour la compétence C6** Pour formaliser les actions correctives, le candidat structure ses recommandations pour les intégrer dans un rapport final : - définit l'ordre des actions à mettre en œuvre en fonction de l'importance de la non-conformité ; - cite les différentes parties qui structure le dossier de manière conforme avec la norme 19011 ;
C7. Établir un plan de suivi des actions en s'appuyant sur le rapport final afin de contrôler la mise en œuvre et le niveau de réalisation des actions		**Cr7. Critères pour la compétence C7** Le candidat propose un plan de suivi des actions opérationnel : - il formalise les actions à faire sous forme de plan ; - il sélectionne des actions systématiques à réaliser dans une démarche d'amélioration continue ; - il établit une échelle du niveau d'avancement des actions ; - il prévoit des échéances de rappel ;
(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.		