RÉFÉRENTIELS DE COMPETENCES ET D'EVALUATION
ISO/CEI 27001 Lead Implementer

La mise en place d'un système de management du système d'information (SMSI) de l'entreprise garantit la protection des fonctions et informations de l'entreprise de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique. La norme ISO/CEI 27001 énumère un ensemble de points de contrôle à respecter pour s'assurer de la pertinence du SMSI, permettre de l'exploiter et de le faire évoluer.
Cette certification valide les compétences de professionnels capables d'élaborer et piloter la mise en œuvre un système de management de la sécurité de l'information d'une organisation selon la norme ISO/CEI 27001 qui tienne compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation.

Elle s'adresse aux professionnels évoluant dans le domaine de la sécurité de l'information, de la gestion des systèmes d'information souhaitant démontrer qu'ils maîtrisent des compétences complémentaires leur permettant de préparer et piloter la mise en œuvre des projets d'implémentation de systèmes de gestion de la sécurité de l'information en conformité avec la norme ISO/CEI 27001.

Les activités concernées sont :
- Réaliser un diagnostic de la situation en terme de sécurité de l'information de l'entreprise, afin de définir les objectifs du projet de mise en œuvre d'un SMSI
- Définir et planifier l'ensemble des activités nécessaires à l'implémentation du SMSI afin obtenir l'approbation de la direction de l'entreprise
- Implémenter le SMSI en coordonnant l'ensemble des parties prenantes afin d'atteindre les objectifs ciblés
- Mettre en œuvre une démarche d'amélioration continue afin de garantir le niveau de performance du SMSI

Référentiel de compétences	Référentiel d'évaluation	
Compétences	**Modalités d'évaluation**	**Critères d'évaluation**
C1. Collecter et analyser les données existantes en s'appuyant sur la documentation obligatoire et non obligatoire de l'entreprise et des entretiens de personnes ressources telles que définis dans la norme ISO 27001 afin d'établir un état des lieux concernant la sécurité de l'information	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 souhaitant élaborer et mettre en œuvre un projet d'implementation d'un système de management de la sécurité de l'information en conformité avec la norme ISO 27001 et les autres normes ISO associées (1). Le cas d'entreprise décrit et présente le contexte spécifique, les particularités, les enjeux et le système d'information de l'entreprise.	**Cr1. Critères pour la compétence C1** Le candidat s'assure que : - les informations collectées sont factuelles et documentées - il produit une analyse qui s'appuie sur ces données et se réfère aux recommandations de la norme - il propose des axes de progrès pertinents en matière de système de management de la sécurité de l'information
C2. Définir les objectifs du système de management de la sécurité de l'information en s'appuyant sur l'état des lieux réalisés et la norme ISO 27001 afin de préciser le périmètre du projet de mise en œuvre		**Cr2. Critères pour la compétence C2** Le candidat formule des objectifs réalistes : - il définit des objectifs mesurables, évaluables, reliés aux exigences et aux mesures de la norme ISO 27001.

C.3 Formaliser le domaine d'application et le business case en utilisant une approche projet établie en vue de permettre la décision de lancement du projet de mise en œuvre	**Le candidat prépare une présentation sous forme de diaporama** de son projet d'implementation d'un système de management selon ISO 27001 en distinguant 3 parties : - Partie 1 : justification du choix du périmètre (compétence C1 à C3) - Partie 2 : description du projet d'implementation qu'il a conçu (politique et principales mesures) (compétence C4 à C6) - Partie 3 : formalisation de sa démarche d'accompagnement à la mise en place (principaux enjeux humains et actions/positionnement envisagées) (C7 à C9) **Le candidat présente son diaporama au jury de certification comme s'il défendait son projet d'implémentation devant un comité de direction d'une organisation**. Lors de cette soutenance un accent particulier est mis sur les compétences de savoir agir en situation.	**Cr3. Critères pour la compétence C3** Le candidat définit le domaine d'application et le business case de façon conforme : - il établit le périmètre en respectant les objectifs définis - il identifie les risques majeurs - il évalue des investissements réalistes - il identifie clairement les liens avec la stratégie de l'organisation - il propose une approche adaptée aux capacités de l'entreprise
C4. Constituer une équipe projet en définissant les rôles et responsabilités en lien avec la norme afin d'optimiser la mise en œuvre du SMSI		**Cr4. Critères pour la compétence C4** Le candidat compose une équipe cohérente avec les enjeux : - il définit l'ensemble des rôles et responsabilités nécessaires à la mise en place des exigences du projet SMSI ; - il vérifie que les personnes sélectionnées ont les compétences requises par rapport aux profils définis.
C5. Concevoir un plan de projet d'implémentation du SMSI en s'appuyant sur les parties prenantes du projet afin de garantir le succès de sa mise en œuvre		**Cr5. Critères pour la compétence C5** Le candidat conçoit un projet réaliste et argumentée : - il définit les activités au bon niveau de précision - il évalue les moyens et les risques - il définit les coûts, délais et le périmètre de manière cohérente
C6. Élaborer la Politique de sécurité de l'information et la Déclaration d'applicabilité en prenant en compte les contraintes de l'organisation afin d'obtenir l'approbation de la direction		**Cr6. Critères pour la compétence C6** Afin d'accompagner la prise de décision du démarrage du projets le candidat : - met en avant les points importants de la politique de sécurité au regard des enjeux de l'organisation et de ses objectifs - complète la Déclaration d'applicabilité pour la faire correspondre aux exigences de la norme
C7. Exécuter le plan de projet en créant, documentant les dispositifs, l'organisation et les mesures de sécurité spécifiques pour augmenter la maturité de l'entreprise concernant la sécurité de l'information		**Cr7. Critères pour la compétence C7** Le candidat formalise/préconise un dispositif ou une organisation et des mesures de sécurité pour réduire les vulnérabilités Il explique comment il accompagne les responsables de processus pour qu'ils conduisent la réalisation des processus et valident ces derniers conformément au plan de projet

C8. Faciliter l'appropriation du SMSI en s'appuyant sur une démarche d'accompagnement au changement afin d'obtenir l'engagement des parties prenantes		**Cr8. Critères pour la compétence C8** Le candidat propose un plan d'accompagnement au changement adapté : - il définit les besoins des bénéficiaires - il présente au moins une action de communication ou de sensibilisation ou de formation adaptée au contexte - il propose la structuration et la mise à disposition de la documentation du SMSI
C9. Mettre en œuvre une démarche de contrôle et d'amélioration continu du SMSI afin de garantir le niveau de performance du SMSI souhaité		**Cr9. Critères pour la compétence C9** Pour formaliser sa démarche d'accompagnement de la mise en œuvre du projet d'implémentation le candidat détermine et justifie : - l'utilisation des outils de contrôie et d'amélioration adaptés conforme à la norme (revue de direction, plan d'action pour traiter les non conformités, suivi des changements, audits internes…) - l'utilisation des indicateurs de suivi de la performance opérationnelle

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