Évaluer et traiter les risques de sécurité de l'information
en s'appuyant sur la norme NF ISO 27005
(ISO/CEI 27005 - Security Risk Manager)

Toutes les informations détenues par une entreprise sont exposées à des menaces d'attaques, d'erreur, d'événements naturels et sont exposées à des vulnérabilités inhérentes à leur utilisation.
Afin d'apporter une réponse adaptée, les organisations ont la possibilité développer des démarches de préservation de leur système d'information telle que l'analyse des risques portée par la norme NF ISO 27005. Pour cela, elles doivent pouvoir disposer de personnel formé et certifié capable d'analyser les risques potentiels susceptibles d'affecter leur dispositif de sécurité de l'information.
La certification s'adresse à tout professionnel en lien avec le management de la sécurité de l'information de l'entreprise souhaitant attester qu'il possède de manière complémentaire les connaissances et les compétences nécessaires pour identifier, évaluer et traiter les risques auxquels est soumis le Système d'Information de façon à préserver les activités essentielles de l'entreprise en s'appuyant sur l'ISO 27005.
Les activités en lien avec cette certification sont :
- Définir le périmètre de l'analyse des risques
- Apprécier les risques
- Traiter les risques
- Garantir que la gestion des risques est une des activités essentielles de l'entreprise

Référentiel de compétences	Référentiel d'évaluation	
Compétences	**Modalités d'évaluation**	**Critères d'évaluation**
C1. Identifier les processus métiers sensibles et stratégiques et leur système d'information associé en s'appuyant sur une analyse SWOT de l'environnement et de l'entreprise afin de garantir la cohérence des décisions de traitements des risques avec la stratégie de l'entreprise	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 mettre en place une démarche d'analyse des risques du système d'information visant la préservation des activités essentielles de l'organisation s'appuyant sur la norme ISO 27005. 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** de sa démarche d'analyse des risques selon ISO 27005 en distinguant : - Partie 1 : établissement de la stratégie d'évaluation et de traitement des risques en faisant références aux exigences de la norme ISO 27005 et aux données fournies dans le cas (compétence C1 et C2) - Partie 2 : proposition des plans de traitement des risques et de leur analyse comparée au regard des ressources mobilisées (compétence C3 et C4)	**Cr1.Critères pour la compétence C1** Le candidat choisit des processus en justifiant son choix : - il décrit les caractéristiques de l'environnement sur les plans humain, sociétal, technique ou physique en terme de menaces et opportunités ; - il relie clairement les processus métiers à leur système d'information ; - il repère les personnes ressources pertinentes devant être associées dans la démarche d'évaluation des risques du système d'information
C2. Délimiter le domaine d'application (périmètre d'action) sur lequel s'exerce l'analyse de risque en synthétisant toutes les informations collectées issus de groupes de travail collaboratifs et de la documentation de l'entreprise afin de définir la stratégie d'évaluation et de traitement des risques		**Cr2. Critères pour la compétence C2** Le candidat détermine les systèmes d'information : - il précise le périmètre d'action en identifiant clairement les actifs informatiques soutenant les processus métiers et stratégiques ; - il justifie ses choix en les liant avec les priorités de l'entreprise ; - il établit des échelles de mesure des risques sur la base de critères qualitatifs et quantitatifs ;
C3. Construire et hiérarchiser par criticité des scenarii de dysfonctionnement ou d'agression en s'appuyant sur les personnes ressources compétentes afin de retenir les scénarii les plus critiques en fonction de leur probabilité et de leurs impacts		**Cr3. Critères pour la compétences C3** Le candidat retient des scenarii pertinents : - il associe clairement les scénarii à des risques ; - il repère de manière exhaustive les risques cohérents avec les enjeux des métiers ; - il propose une évaluation chiffrée des impacts et de leur probabilité

C4. Elaborer les plans de traitement des risques (intégrant l'impact, la probabilité et les risques résiduels) en s'appuyant sur l'analyse des scenarii afin de permettre à la direction de l'entreprise de choisir les plus pertinents au regard de la stratégie de l'entreprise	- Partie 3 : conception d'un programme de mise en oeuvre d'un plan de traitement systématique et pérenne précisant les ressources nécessaires à mobiliser (compétence C5 et C6) **Le candidat présente son diaporama au jury de certification comme s'il défendait son analyse de risque 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.	**Cr4. Critères pour la compétence C4** Le candidat s'assure qu'ils sont complets et efficaces : - il propose des plans de traitement des risques qui couvrent complètement les enjeux de l'organisation ; - il propose des solutions réalistes, articulées entre elles, pratiques au niveau technique, organisationnel et comportemental ; - il hiérarchise les solutions en fonction de la criticité du risque et du nombre de risques couverts ; - il choisit des indicateurs de performance limités à 10 ; - il prévoit des seuils et les actions à déclencher en cas de franchissement de ces seuils
C5. Accompagner l'entreprise dans la mise en œuvre du plan de traitement en s'appuyant sur des indicateurs de suivi des dysfonctionnements et en collectant de retours d'expérience afin de s'assurer de son efficacité dans le temps		**Cr5. Critères pour la compétence C5** Le candidat structure son accompagnement : - il planifie les mesures correctrices et prévoit de mesurer leur efficacité (contrôles systématiques) ; - il propose des actions de formation ou d'information formalisées ; - il identifie les outils de communication et de suivi pertinents (tableaux de bord, documentation, fiches pratiques, bulletins d'information, brieffing…) ;
C6. Favoriser une culture de la gestion du risque lié au système d'information dans l'organisation en facilitant les remontées d'incidents de sécurité de l'information et leur analyse afin de pérenniser les bénéfices obtenus de la démarche		**Cr6. Critères pour la compétence C6** Le candidat développe une culture de gestion des risques : - il propose des actions qui responsabilise les salariés pour qu'ils soient proactifs et qu'ils rendent compte des dysfonctionnements et incidents évités; - il préconise une organisation humaine qui permet d'intégrer la gestion des risques dans les processus métiers de l'entreprise ;