CQP – Manager de la Sécurité et des Risques de l'Information (MSRI)

Référence : **CQPMSRI** Durée : **75 jours** Certification : **Oui - Jury**

CONNAISSANCES PREALABLES & PROFIL DES STAGIAIRES

• Titulaires d'un diplôme ou d'un titre de niveau I (bac + 5) selon la nomenclature des niveaux de formation de 1969 (ou expérience équivalente) issus d'un cursus scientifique, de commerce, de management ou juridique et avec une expérience professionnelle de 5 années minimum, soit dans le domaine de la Sécurité, soit de la Production ou des études informatiques, soit d'une Direction des risques / de la qualité, ou encore ayant un poste de management au sein d'une Direction métier.
• Les candidats doivent également justifier d'une maîtrise de l'anglais en contexte professionnel. Ce niveau peut être apprécié par l'apport d'une attestation de type TOIEC (entre 605 et 780) ou équivalent ou bien par la réalisation d'un test d'entrée

OBJECTIFS

• Le Manager de la Sécurité et des Risques de l'Information (MSRI) est en charge de la définition de la politique de gestion des risques liés à l'information dans l'entreprise, du déploiement et de l'animation du dispositif de gestion des risques. Ce dispositif intègre des actions anticipatrices de pesée des vulnérabilités et des actions correctrices de défaut de sécurité de l'information.
• Il est le garant de la mise en place de bonnes pratiques au sein de l'organisation dans un souci permanent de sensibilisation du personnel (interne ou de l'entreprise élargie) aux risques

METHODES PEDAGOGIQUES

Méthodes pédagogiques
• Storytelling
• Jeux de prise de conscience
• Analyse de situations
• Mise en situation
• Etudes de cas

Moyens pédagogiques
• Diaporamas spécifiques
• Supports de cours
• Exemples de chartes sécurité
• Liens des sites de veille
• Bibliographie

FORMATEUR

Consultant-Formateur expert des technologies enseignées

EVALUATIONS

• Chaque bloc donne lieu à une étude de cas qui permet d'évaluer la compréhension, l'appropriation et la restitution des éléments présentés en formation. Cette étude de cas est tutorée et elle est évaluée par un binôme d'évaluateurs.
• L'évaluation finale du CQP est constituée de deux éléments : la rédaction d'une note de synthèse (partiellement tutorée) et le passage devant un jury professionnel.

CONTENU DU COURS

BLOC 1 : Définir et organiser la gouvernance des risques liés à l'information au sein de l'entreprise et de l'entreprise élargie

UNITÉ 1 : LES ENJEUX DE LA SECURITE ET DES RISQUES DE L'INFORMATION

- Comprendre les enjeux de la sécurité et des risques de l'information, et définir une politique alignée avec ces enjeux.

- Disposer d'un panorama des référentiels, normes et méthodes de gestion des risques.
- Appréhender les principaux risques liés à l'information.

S1 – Les enjeux et les objectifs en matière d'information digitale

- Recenser les enjeux et objectifs en matière d'information, alignés avec ceux de l'entreprise.
- Identifier, caractériser et évaluer les informations manipulées.

• Les objectifs et enjeux métiers: identification, importance et utilisation
• La stratégie et la gouvernance d'entreprise : définition et objectifs …
• L'organisation de l'entreprise
• Les informations, bien essentiel de l'entreprise
• Les flux d'informations dans les processus et d'un processus à l'autre
• Le système d'information et le système informatique
• La raison (POURQUOI ?) de la SSI
• Le but (POUR QUOI ?) de la SSI
• Les objectifs et la stratégie de sécurité de l'information
• Les objectifs et la stratégie TIC et son alignement avec la stratégie d'entreprise et la stratégie de sécurité (introduction)
• La classification des actifs (informations, processus et biens support)
• Architecture (cartographie) informationnelle et des processus

S2 - Les exigences réglementaires et les instances officielles

- Appréhender les aspects liés au droit de l'informatique pour appliquer la réglementation en vigueur, afin de gérer les aspects contractuels, les spécificités liées à la fraude, à la sécurité, à la protection de l'information.
- Rappel des prérequis réglementaires et normatifs (SOX, ISO 27001, PCI-DSS, etc.) en matière de gestion des risques.
- Recenser les acteurs et instances officielles des filières risque et sécurité (internationale, européenne, nationale, gouvernementale, etc.).

• Exigences légales nationales et supranationales… Identification des risques juridiques liés à l'information (la conformité à ces exigences est un des enjeux majeurs)
• Les responsabilités civile et pénale.
• Les instances officielles et reconnues en matière de sécurité de l'information
• La charte informatique et la charte sécurité: deux documents essentiels dans l'arsenal juridique de l'entreprise
• La criminalité liée à l'information et à l'informatique
• Comment réagir en cas ce cyber attaque : débrancher ou pas ?
• Identification des 'exigences externes' à prendre en compte dans l'entreprise (autres que légales et règlementaires)
• Les 'sources' d'exigences normatives en matière de sécurité de l'information
• Importance de la veille sécuritaire

S3 – Le panorama des référentiels, normes et méthodes

- Appréhender les référentiels, modèles et normes en matière d'information, de management du système d'information, de gestion des risques, et de gouvernance de la sécurité de l'information.

• Référentiels SSI
• Référentiels risques SSI (présentation générale)
• Référentiels TIC
• Référentiels de certification
• Le référentiel ISO/IEC 27002 et ses 'satellites: 27010, 27011, 27017 et 27018: leur structure.
• Le NIST Cybersecurity Framework (structure + la 'Response chain')

S4 – Le panorama des risques et l'état de l'art des solutions

- Fournir une synthèse des dernières enquêtes sur la situation de la gestion des risques liés à l'information et aux usages numériques.
- Disposer d'un panorama des vulnérabilités, des menaces et des risques induits par les nouvelles pratiques en matière de management de l'information, incluant les cybermenaces, les risques sur la mobilité et le cloud.

• Le risque
• Les menaces pesant sur les informations et les TIC
• Les vulnérabilités connues des biens essentiels et support
• Les vulnérabilités des TIC
• Les 'nouveaux risques' apportés par la technologie
• Les solutions et mesures de sécurité

S5 – La stratégie et la politique générale de sécurité et des risques de l'information

- Disposer d'une démarche pour mettre en place une politique générale de sécurité et des risques liés à l'information.
- Associer la gestion des risques liés à l'information aux enjeux de l'entreprise.

• Le cadre documentaire SSI
• Comment ce cadre s'adapte à la taille de l'entreprise
• Les exigences 'documentaires' de la norme ISO/IEC 27001
• La problématique de la non-conformité… et ses solutions
• Les différents Tableaux de bord à prendre en compte

UNITÉ 2 : LA GOUVERNANCE DE LA SECURITE ET DES RISQUES DE L'INFORMATION

- Comprendre les métiers de la filière sécurité et risques liés à l'information.
- Établir et mettre en œuvre un modèle de gestion et d'amélioration continue de la sécurité et des risques liés à l'information où les rôles et les responsabilités sont clairement attribués à tous les niveaux de l'organisation.

S6 - Les métiers de la filière sécurité et risque

- Appréhender les métiers de la filière sécurité et risques liés à l'information.
- La maturité des entreprises en SSI.

• Les différents rôles et responsabilités de sécurité
• Les 'métiers' de la sécurité
• La maturité de la sécurité

S7 - L'organisation de la gouvernance des risques

- Appréhender l'organisation de la gouvernance de la sécurité et des risques liés à l'information :
- Liens entre la Sécurité des Systèmes d'Information, le Management, la DSI, les Directions Métiers, la Direction des risques, la Direction Générale.
- Principales instances opérationnelles, de pilotage et décisionnaires.

• La différence entre risques et insécurité d'une part et mesures et sécurité d'autre part
• La gouvernance de la SSI
• Les instances de gouvernance et de management de la SSI
• La hiérarchie des rôles de sécurité; proposition d'une organisation SSI
• L'indispensable lien entre les risques métiers et les risques SSI
• Introduction à l'aspect systémique du SI et de la SSI
• Les risques de l'entreprise

S8 - Les politiques opérationnelles

- Appréhender l'ensemble des piliers à adresser par les politiques opérationnelles de gestion de la sécurité et des risques liés à l'information :
  - organisation des ressources humaines,
  - gestion des identités et des droits,
  - sécurité physique et logique, etc.
- Proposer pour chaque pilier l'ensemble des exigences fines en matière de sécurité et de risques liés à l'information, alignés avec la politique générale de sécurité.

• Les 9 domaines de la Sécurité de l'Information + rappel ISO 27002
• Les catégories de solutions et mesures de sécurité (2 versions)
• Les caractéristiques des mesures de sécurité
• La 'systémique' des mesures de sécurité (hiérarchie et interactions)
• La classification des actifs : pourquoi et comment
• Comment écrire une politique de sécurité

S9 - Le système de management des risques

- Appréhender les modèles de gestion de risques et les systèmes de management. Classifier les différentes natures de risques (physique, logique, humain, etc.) et les différents types de risques (opérationnels, de sécurité, de non-conformité, de non qualité, financier, etc.).
- Définir une méthodologie commune adaptée à tous les types de risques.
- Comment tendre vers une méthodologie commune à tous les types de risques.

• Le processus de gestion des risques
• Les raisons et conditions de la gestion des risques
• Rappels : les formules et le cycle du risque
• Les méthodes (top 5) : MEHARI, EBIOS, OCTAVE, CRAMM, etc.
• Gestion du risque - Phase 1: Etude du contexte
• Que faire en cas de complexité ?
• EBIOS Etape 1

EVALUATION DU BLOC

L'évaluation porte sur la réalisation individuelle d'une étude de cas basée sur un cas fictif contextualisé.
Le livrable produit et présenté oralement devant un binôme d'évaluateurs sur :
• la définition des grandes lignes d'une politique de gestion des risques et de la sécurité liés à l'information
• l'élaboration du processus de management des risques et de la sécurité liés à l'information

BLOC 2 : Définir et piloter le dispositif de maîtrise des risques liés à l'information

UNITÉ 3 : LA GESTION DE LA SECURITE ET DES RISQUES LIES A L'INFORMATION

- Identifier les risques liés à l'information, les évaluer et disposer d'une cartographie.
- Définir un plan de traitement des risques, le mettre en œuvre et le suivre.

S10 - L'identification et l'évaluation des risques

- Appréhender l'ensemble des risques (menaces, vulnérabilités, etc.) liés à l'information de l'entreprise et faire une première évaluation qualitative.
- Disposer des techniques d'évaluation des risques (par exemple via la norme ISO 31010).
- Evaluer les risques bruts intrinsèques, et estimer les conséquences des risques avérés (financières, juridiques, humaines, métier, etc.).

• L'informatique d'entreprise
• Retour sur le système d'information
• Gérer la complexité de l'évaluation des risques
• Evaluation des risques (ISO 27005)
• Responsabilités face aux risques
• Que décider face aux risques ?
• EBIOS Etapes 2, 3 et 4

S11 - Le traitement et la réduction des risques

- Appréhender les stratégies de traitement des risques (prévention, protection, évitement, mutualisation, externalisation, transfert)
- Définir les niveaux de risque acceptable, et proposer un plan adapté de traitement des risques.
- Développer les modalités de traitement des risques et suivre le plan de traitement des risques. Identifier le type de traitement des risques optimal entre réduction et partage.

- Proposer des cas exceptionnels d'évitement ou de refus.

• Les options de traitement
• Le choix de l'option et la détermination des exigences pour couvrir le risque inacceptable
• Détermination des objectifs à atteindre pour réaliser les exigences
• Choisir des 'solutions de sécurité', besoin de pragmatisme
• Le Statement of Applicability (Déclaration d'Applicabilité) de l'ISO 27001
• La sélection des solutions de sécurité
• Mesurer l'efficacité des solutions de sécurité
• Préparer le Plan d'Actions Sécurité
• Les risques propres au Plan d'Actions

EVALUATION DU BLOC

L'évaluation porte sur la réalisation individuelle d'une étude de cas basée sur un cas fictif contextualisé.
Le livrable produit et présenté oralement devant un binôme d'évaluateurs sur :
• La réalisation d'une cartographie des risques et une fiche de risque par type,
• L'élaboration d'un plan de traitement des risques (avec des fiches « actions » « contrôle ») en tenant compte des aspects budgétaires.

BLOC 3 : Définir et superviser le dispositif de gestion des incidents et des crises

UNITE N°4 : LA GESTION DES INCIDENTS ET LA GESTION DE CRISE

- Comprendre le processus de gestion des incidents, et les principes d'escalade associés.
- Comprendre le processus de gestion de crise, et les dispositifs à mettre en œuvre.

S12 - La gestion des incidents

- Appréhender le processus de gestion des incidents (processus classique ou incident de sécurité).
- Appréhender les dysfonctionnements correspondant à des risques avérés.
- Evaluer leur conséquence et réévaluer les risques, en disposant d'une base de capitalisation s'enrichissant des événements du passé.

• Pourquoi gérer les incidents?
• Ce qu'est un incident
• C'est quoi, gérer un incident?
• Rôles et Responsabilités
• Retour sur la Response Chain (Nist Cybersecyrity framework)
• Les références
• La Capacité de réponse
• La détection et le signalement
• Le Plan de réponse
• La conduite de la réponse
• La 'mesure' de la réponse
• Apprendre la leçon de l'incident
• La communication lors de l'incident

S13 - La gestion des crises

- Définir la crise et ses éléments déclencheurs.
- Appréhender le processus de gestion de crise dans sa globalité : procédures, acteurs, critères.
- Constituer la gestion de crise.
- Définir le plan de gestion de crise et les critères d'activation du plan de secours.
- Définir le plan de désactivation de la crise et le plan de retour à la normale.

• C'est quoi, une crise?
• Différences entre la Plan de Secours informatique et le Plan de secours Sécurité de l'Information
• Rôles et Responsabilités
• Comment passer de la gestion d'incident à la gestion de crise ?
• La Capacité de gestion de crise

• Le PCA, le PRA et le Plan de Secours
• Retour sur la gestion des risques
• Les exigences des solutions de secours
• Référentiels (CobIT, ISO 22301,etc.)
• Le PCA
• Le PRA
• Le retour à la normale
• Apprendre les leçons de la crise
• La communication de crise

S14 - Les mesures correctives

- Proposer un aperçu des mesures correctives à mettre en place lors d'un risque avéré (dysfonctionnement ou incident).
- Définir les mesures correctives et les suivre.

• Que faut-il améliorer ?
• Comment agir
• Dans quels délais agir
• Le système de sanctions positives et négatives
• Suivre les actions et proposer les indicateurs de qualité et d'avancement

S15 – La communication de crise

- Anticiper la crise, et identifier les publics impactés et leur réaction potentielle en cas de crise.
- Communiquer lors d'une situation de crise, en ajustant les messages en interne et en externe.
- Analyser les effets de la crise et restaurer la confiance.

• A qui communiquer ? les parties prenantes (parties intéressées) chacune a son rôle, ses responsabilités, ses capacités et ses compétences
• Le Plan de communication et le PCC : plan de communication de crise
• Que communiquer – le message
• Quand et comment communiquer
• Comment communiquer – le mode de communication
• Anticiper la réaction des audiences
• Apprendre les leçons de la communication

EVALUATION DU BLOC

L'évaluation porte sur la réalisation individuelle d'une étude de cas basée sur un cas fictif contextualisé.
Le livrable produit et présenté oralement devant un binôme d'évaluateurs sur :

• L'élaboration de deux procédures relatives respectivement à la gestion des incidents et à la gestion de crise
• La réalisation d'un tableau de bord de gestion des incidents et des fiches actions

BLOC 4 : Evaluer régulièrement le dispositif de gestion des risques liés à l'information

UNITE N°5 : LE CONTROLE INTERNE ET L'AMELIORATION

- Mettre en place des mécanismes de contrôle interne et assurer le pilotage des risques liés à l'information

S16 - Le contrôle interne (permanent et audit)

- Effectuer des revues et réexamens régulier des processus et des risques liés à l'information afin de s'assurer du respect de la politique de sécurité et des risques liés à l'information, de la fiabilité et de l'intégrité des informations, de l'efficience et de l'efficacité des processus et opérations, de la protection des actifs informationnels, du respect des lois, règlements, règles, procédures et contrats.
- Effectuer des audits ponctuels de sécurité et des risques liés à l'information.

• Rôles et Responsabilités dans le contrôle interne
• Référentiels
• Terminologie
• Les contrôles par le RSSI
• Audit interne
• Audit externe
• Introduction à l'audit
• Les techniques et procédures d'audit
• L'application à la SSI
• Les non-coformités, qu'est-ce ?

S17 - Les actions d'amélioration

- Proposer des actions d'amélioration suite aux revues des processus et des risques, et les suivre.

➜ Corrections et améliorations en cas de faiblesse ou d'inconsistance
➜ Gestion du risque
➜ Cadre documentaire SSI
➜ Clauses de sécurité dans les contrats
➜ Efficacité et de l'efficience des solutions, services, contrôles et mesures de sécurité
➜ Plans de Traitement du risque
➜ Plans de communication
➜ Plans de correction (voir Plan de Traitement des risques)
➜ Plan de Diffusion de la culture de sécurité
➜ Gestion de projets SSI

S18 - Le référentiel de pilotage des risques

- Consolider le suivi des risques dans un tableau de bord permettant de fournir une vision globale de l'exposition de l'entreprise aux risques liés à l'information.
- Fournir un outil communiquant, permettant d'informer, de diriger, de gérer et de piloter la gestion des risques liés à l'information.

• Les rapports 'source'
• Retour sur les tableaux de bord
• Les indicateurs et les métriques : KGI et KPI de sécurité
• Référentiels
• La collecte et l'exploitation des données
• Faire rapport
• Retour sur les plans de correction et d'amélioration

EVALUATION DU BLOC

L'évaluation porte sur la réalisation individuelle d'une étude de cas basée sur un cas fictif contextualisé.
Le livrable produit et présenté oralement devant un binôme d'évaluateurs mettra l'accent sur:
• La réalisation d'une analyse des risques (basée sur une revue de processus et des audits)
• L'élaboration d'un plan d'actions correctrices dont on appréciera la pertinence, la lisibilité et la conformité des modalités de suivi.

BLOC 5 : Diffuser la culture de prévention des risques liés à l'information

UNITE N°6 : LA DIFFUSION DE LA CULTURE DE PREVENTION DES RISQUES

- Structurer et organiser la culture de prévention des risques liés à l'information

S19 – La définition de la culture de prévention des risques

- A partir des risques identifiés et des acteurs concernés, proposer des messages et des comportements permettant de faire progresser la culture risque dans l'entreprise.
- Permettre d'acquérir les règles de conduite et les réflexes afin d'améliorer l'efficacité de la prévention et de la protection.
- Faire émerger toute une série de comportements adaptés lorsqu'un événement majeur survient.

• Les bases de la culture de sécurité : connaissance, motivation, confiance et savoir-faire
• Connaître la situation et identifier les conséquences
• Créer la motivation pour atteindre les objectifs de l'entreprise
• Gérer la confiance dans le comportement des personnes
• Le savoir-faire : faire acquérir les comportements et les habitudes 'en ligne' avec les objectifs

S20 – La diffusion de la culture de prévention des risques

- Déployer le plan de communication au sein de l'entreprise, et s'assurer que les interlocuteurs ont compris et adhèrent aux messages.

• Les 4 axes de la culture de sécurité
• Les programmes et les plans

• Informer (pour tous) – montrer ce qui est important, créer le 'désir' et la motivation, CONSCIENTISER
• Sensibilisation – préparer aux habitudes, construire les connaissances de base et RESPONSABILISER et ENGAGER
• Formation pour ceux qui ont un rôle spécifique à réaliser – créer les savoir-faire nécessaires, CREER LES COMPETENCES
• Education pour ceux qui doivent connaître 'le fond de la question' – faire 'comprendre' les tenants et aboutissants, les moyens et les concepts de la sécurité
• Le système de sanctions…

EVALUATION DU BLOC

L'évaluation porte sur la réalisation individuelle d'une étude de cas basée sur un cas fictif contextualisé.
Le livrable produit et présenté oralement devant un binôme d'évaluateurs mettra l'accent sur:
➜ La réalisation d'un plan de communication et d'un plan de présentation pour une population d'utilisateurs.

COMPETENCES TRANSVERSES A L'ENSEMBLE DES BLOCS : Manager la gestion des risques et de la sécurité liés à l'information au sein de l'entreprise et dans l'entreprise élargie

UNITE 0 : UNITE TRANSVERSE

- Comprendre la gestion de projet, et l'appliquer à des cas concrets.
- Maitriser les techniques de communication et de management.
- Gérer son stress, résoudre les conflits et travailler en équipe.

S21 : La gestion de projet ou d'activité (gestion financière et comptable -notion de finance d'entreprise - et assurance)

- Identifier les actions majeures à entreprendre pour être en mesure de suivre les différentes étapes de la vie d'un projet / d'une action.
- Participer à l'estimation financière et à l'évaluation de la charge et de la durée nécessaire.
- Mettre en place une organisation permettant de capitaliser l'expérience acquise sur le projet.
- Disposer des facteurs clés associés à la mise en œuvre de plans d'action.

• Elaborer un plan projet
• Gérer les charges et les coûts
• Fonction et responsabilités
• Les outils

S22 : Les techniques de communication et de management

- Adopter une stratégie de communication selon les acteurs en présence, le thème à aborder, et la forme de l'échange visé.
- Apprendre à être explicite, tant dans la rédaction de documents (guide, plan lié à la cartographie, …) que dans l'expression orale.
- Appliquer les méthodes et les connaissances liées à la communication dans la réalisation du mémoire de mise en application, et dans la présentation orale de celui-ci.

• Stratégie de Communication
• Se faire comprendre
• Méthodes de préparation et présentation

S23 : Les techniques pour résoudre des situations de tension

- Mieux communiquer pour faire passer les messages.
- Résoudre les situations conflictuelles.
- Réagir au mieux en situation de stress.
- Faire face à l'agressivité par des techniques comportementales.

• Les biais de la communication interpersonnelle
• Gérer les conflits
• Gérer son émotionnel et celui de ses interlocuteurs

EVALUATION FINALE DU CQP

L'évaluation finale porte sur la rédaction et la soutenance par le stagiaire devant un jury délégué de professionnels du métier habilité par le CPNEFP, d'une note de synthèse qui porte sur l'analyse globale de gestion des risques et de la sécurité à partir d'une situation d'entreprise fictive.

		BLOC 1		BLOC 2	BLOC 3	BLOC 4	BLOC 5	Unité 0
		Unité 1	Unité 2	Unité 3	Unité 4	Unité 5	Unité 6	
Formation	Nb jours	**8**	**7**	**3**	**4**	**4**	**2**	**6**
	Nb heures	**56**	**49**	**21**	**28**	**28**	**14**	**42**
Préparation des évaluations	Nb jours	**4**		**5**	**3**	**3**	**2**	**1**
	Nb heures	**28**		**35**	**21**	**21**	**14**	**7**