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

Référence : **CQP-MSRI** Durée : **52 jours** Certification : **MSRI**

Eligible CPF : Oui

CONNAISSANCES PREALABLES

• Le niveau demandé à l'entrée en formation de ce CQP MANAGER DE LA SECURITE ET DES RISQUES DE L'INFORMATION est celui d'un titre, d'un diplôme ou d'un niveau Bac+5 dans un cursus scientifique, commerce, management et juridique.

PROFIL DES STAGIAIRES

• Jeunes de moins de 26 ans issus du système scolaire. • Les salariés des entreprises de la Branche (numérique, de l'ingénierie, du conseil, des études et des métiers de l'événement). • Les demandeurs d'emploi de plus de 25 ans souhaitant reprendre une activité professionnelle liée au secteur du numérique, de l'ingénierie, des études, du conseil et de l'événement.

OBJECTIFS

• Définir et organiser la gouvernance des risques liés à l'information au sein de l'entreprise et de l'entreprise élargie • Définir et piloter le dispositif de maîtrise des risques liés à l'information • Définir et superviser le dispositif de gestion des incidents et des crises • Evaluer régulièrement le dispositif de gestion des risques liés à l'information • Diffuser la culture de prévention des risques liés à l'information.

CERTIFICATION PREPAREE

• CQP Manager de la Sécurité et des Risques de l'Information.

METHODES PEDAGOGIQUES

• Storytelling. • Jeux de prise de conscience. • Analyse de situation. • Mise en situation. •Etude de cas.

FORMATEUR

Consultant-Formateur expert Sécurité

METHODE D'EVALUATION DES ACQUIS

- 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 en grande 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 : DEFINIR ET ORGANISER LA GOUVERNANCE DES RISQUES LIES A L'INFORMATION AU SEIN DE L'ENTREPRISE ET DE L'ENTREPRISE ELARGIE – 15 jours/105h

UNITE 1 : LES ENJEUX DE LA SECURITE ET DES RISQUES DE L'INFORMATION – *8 jours/56h*

Enjeux et objectifs en matière d'information digitale

- 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

Les exigences réglementaires et les instances officielles

- 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

Panorama des référentiels, normes et méthodes

- 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')

Panorama des risques et état de l'art des solutions

- 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

Stratégie et politique générale de sécurité et des risques de l'information

- 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

UNITE 2 : : LA GOUVERNANCE DE LA SECURITE ET DES RISQUES DE L'INFORMATION – *7 jours/49h*

Les métiers de la filière sécurité et risque 3

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

L'organisation de la gouvernance des risques

- 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

Les politiques opérationnelles

- 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

Le système de management des 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

BLOC 2 : DEFINIR ET PILOTER LE DISPOSITIF DE MAITRISE DES RISQUES LIES A L'INFORMATION – 3 jours/21h

UNITE 3 : LA GESTION DE LA SECURITE ET DES RISQUES LIES A L'INFORMATION *3 jours/21h*

L'identification et l'évaluation des risques

- 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

Le traitement et la réduction des risques

- 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

BLOC 3 : DEFINIR ET SUPERVISER LE DISPISITIF DE GESTION DES INCIDENTS ET DES CRISES – 4 jours/28h

UNITE 4 : LA GESTION DES INCIDENTS ET LA GESTION DE CRISE – *4 jours/28h*

La gestion des incidents

- 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

La gestion des crises

- 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
- Référentiels (CobIT, ISO 22301, etc.)
- Le PCA
- Le PRA
- Le retour à la normale
- Apprendre les leçons de la crise
- La communication de crise

Les mesures correctives

- 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

Communication de crise

- 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

BLOC 4 : EVALUER REGULIEREMENT LE DISPOSITIF DE GESTION DES RISQUES LIES A L'INFORMATION- 4 jours/28h

UNITE 5 : LE CONTROLE INTERNE ET L'AMELIORATION – *4 jours/28h*

Le contrôle interne (permanent et audit)

- 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-conformités, qu'est-ce ?

Les actions d'amélioration

- 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

Le référentiel de pilotage des risques

- 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

BLOC 5 : DIFFUSER LA CULTURE DE PREVENTION DES RISQUES LIES A L'INFORMATION – 2 jours/14h

UNITE 6 : LA DIFFUSION DE LA CULTURE DE PREVENTION DES RISQUES
2 jours/14h

Définir la culture de prévention des risques
- 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

Diffuser de la culture de prévention des risques
- 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…

UNITE TRANSVERSE – *6 jours/42h*

La gestion de projet ou d'activité (gestion financière et comptable -notion de finance d'entreprise - et assurance)
- Elaborer un plan projet
- Gérer les charges et les coûts
- Fonction et responsabilités
- Les outils

Les techniques de communication et de management
- Stratégie de Communication
- Se faire comprendre
- Méthodes de préparation et présentation

Les techniques pour résoudre des situations de tension
- Les biais de la communication interpersonnelle
- Gérer les conflits
- Gérer son émotionnel et celui de ses interlocuteurs