SUJET 2 - ÉVALUATION ET CONTRÔLES DES RISQUES

Déterminer les risques d'interruption (événements ou environnement externe) qui peuvent affecter défavorablement l'organisation et ses ressources (par exemple, les personnes, les installations, les technologies); les pertes potentielles que ces événements peuvent entraîner et les contrôles requis pour prévenir ou atténuer les conséquences de ces risques. Comme résultat de ce qui précède, une analyse coût bénéfices sera requise pour justifier les investissements dans des contrôles.

A. LE RÔLE DU PROFESSIONNEL EST DE :

A.1 Obtenir de la direction les informations sur la tolérance aux risques de l'organisation

A.2 Identifier et mettre en œuvre les activités de collecte d'information

A.3 Identifier les menaces/risques potentiels à l'organisation selon des catégories de risque

A.4 Qualifier et catégoriser les menaces identifiées selon leur importance

A.5 Identifier les contrôles et mesures de protection pour prévnir et atténuer les conséquences de perte potentielles

A.6 Évaluer l'efficacité des contrôles et mesures de protection

A.7 Documenter et présenter l'évaluation de risques à la direction générale pour approbation

B. LE PROFESSIONNEL DEVRAIT DÉMONTRER DES CONNAISSANCES PRATIQUES DANS LES DOMAINES SUIVANTS :

B.1 Obtenir de la direction les informations sur la tolérance aux risques de l'organisation

B.1.a Interroger le conseil juridique et tout autre domaine (tels que la direction financière, la direction des opérations, le responsable de gestion de risques, etc.) pour identifier toutes les préoccupations en matière de risques.

B.1.b Travailler avec la direction pour choisir le modèle d'analyse coût bénéfices adéquat

B.1.c Établir les critères de mesure nécessaires pour quantifier la tolérance aux risques

B.2 Identifier et mettre en œuvre les activités de collecte d'information

B.2.a Déterminer les méthodes de collecte d'information
- (i) Déterminer les sources d'information
- (ii) Déterminer la crédibilité des sources d'information

B.2.b Développer une stratégie de collecte d'information cohérente avec les préoccupations d'affaires et les politiques de l'organisation

B.2.c Développer une stratégie de collecte d'information qui peut s'appliquer à travers les divisions et emplacements d'affaires de l'organisation

B.2.d Concevoir des méthodes de collecte d'information et de distribution à l'échelle de l'entreprise

(i) Formulaires et questionnaires

(ii) Entrevues

(iii) Réunions

(iv) Revue de documentation

(v) Analyse

B.3 Identifier les menaces/risques potentiels à l'organisation selon des catégories de risque

B.3.a Identifier les catégories de risques associées au processus d'analyse de risques. Les catégories de risques comprennent, sans s'y limiter :

(i) Risques aux installations

(ii) Risques de sécurité (tant physique qu'informationnelle)

(iii) Réputation

(iv) Administrative

(v) Technologie de l'information (incluant l'infrastructure opérationnelle)

(vi) Humain

(vii) Chaîne d'approvisionnement (incluant l'impartition)

(viii) Conformité

B.3.b Identifier les sources d'exposition tant de l'interne qu'à l'externe. Les sources internes et externes comprennent, sans s'y limiter :

(i) naturelle, humaine ou technologique

(ii) accidentelle vs intentionnelle

(iii) interne vs externe

(iv) menace/risque contrôlable vs hors du contrôle de l'organisation

(v) Événements avec alerte préalable vs ceux sans avertissement

B.4 Qualifier et prioriser les menaces identifiées

B.4.a Élaborer une méthode quantifiable pour évaluer les menaces/risques en termes de probabilité et de sévérité

B.4.b Identifier d'autres méthodologies et outils d'analyse de risques

(i) méthodes quantitatives et qualificatives

(ii) avantages et inconvénients

(iii) facteurs de fiabilité / confiance

(iv) bases des formules mathématiques utilisées

B.4.c Choisir la méthodologie et les outils adéquats pour une mise en œuvre à l'échelle de l'entreprise

b.4.d Évaluer les risques et les catégoriser selon des critères pertinents, incluant sans s'y limiter :

(i) risques sous le contrôle de l'organisation

(ii) risques hors du contrôle de l'organisation

(iii) menaces avec alerte préalable (tels que les tornades et les ouragans)

(iv) menaces sans avertissement (tels que les séismes)

B.4.e Évaluer les impacts des risques ou menaces en fonction de facteurs essentiels à la conduite des affaires :

(i) disponibilité du personnel

(ii) disponibilité des technologies de l'information

(iii) disponibilité des technologies de communication

(iv) état des infrastructures (incluant le transport), etc.

B.5 Identifier les contrôles et mesures de protection pour prévenir et atténuer les conséquences de perte potentielles

Considérant : Les actions prises pour réduire la probabilité d'occurrence des incidents pouvant diminuer la capacité de poursuivre les activités

B.5.a Protection physique

(i) Identifier le besoin de restreindre les accès à tous les niveaux pertinents (i.e. immeubles, salles, etc.)

(ii) Investiguer la nécessité de barrières et structures renforcées pour distinguer les entrées volontaires, accidentelles ou non autorisées

(iii) Emplacement : construction physique, situation géographique, voisinage corporatif, infrastructure des installations, infrastructure communautaire.

(iv) Identifier la nécessité de faire appel à du personnel spécialisé pour vérifier les points d'entrée stratégiques

(v) Évaluer le besoin de surveillance humaine ou d'équipement de surveillance enregistrée pour contrôler les points d'entrée et les aires à accès restreints, incluant la détection, la notification et la suppression (i.e. détecteurs, alarmes, gicleurs)

(vi) Réviser la sécurité et les contrôles d'accès, la couverture d'assurance, les baux de location.

B.5.b Protection logique

(i) Évaluer le besoin de systèmes automatisés de protection des données entreposées, en traitement ou en transfert ; copies de sauvegarde et de protection

(ii) Évaluer la sécurité de l'information : surveillance du matériel, des logiciels, des données et des réseaux (i.e. détection, notifications, etc.)

B.5.c Emplacement des actifs

(i) Évaluer la protection inhérente accordée aux actifs clés selon leur emplacement par rapport aux sources de risques

(ii) Procédures pour le personnel

(iii) Maintenance préventive et entente de service selon les besoins

(iv) Services publics : duplication des services publics, redondance intégrée (télécommunications, alimentation électrique, eau, etc.)

(v) Interface avec des agences externes (fournisseurs, services d'impartition, etc.)

B.5.d Identifier les menaces ou risques potentiels à la sécurité de l'organisation, incluant mais sans s'y limiter :

(i) sécurité physique de tous les actifs (installations, équipement, etc.)

(ii) sécurité de l'information - salles d'ordinateurs et d'entreposage des médias

(iii) sécurité des communications – voix et données

(iv) sécurité des réseaux – intranet, internet

(v) sécurité du personnel

B.5.e Développer des options de prévention et avant planification (de continuité)

(i) coûts/ bénéfices

(ii) priorités, procédures et contrôle de la mise en place

(iii) Test/exercice

(iv) Fonctions et responsabilités d'audit

(v) Comprendre les options pour la gestion des risques et la sélection des mesures adéquates ou efficientes (par exemple, élimination, transfert ou acceptation du risque)

B.6 Évaluer l'efficacité des contrôles et mesures de protection

B.6.a Évaluer le processus de communication en matière de sécurité avec les autres secteurs internes et fournisseurs de service externes

B.6.b Évaluer les ententes de niveaux de service en matière de continuité d'activités avec les fournisseurs et les clients tant à l'interne qu'à l'extérieur de l'organisation

B.6.c Évaluer les contrôles et recommander des changements, au besoin, pour réduire les impacts dus aux risques et aux menaces

(i) Contrôles pour empêcher l'impact des menaces : contrôles préventifs (comme des mots de passe, détecteurs de fumée et pare-feu)

(ii) Contrôles pour compenser l'impact des menaces : contrôles réactifs (comme des sites de relève équipés)

B.6.d Établir des scénarios de sinistre basés sur les risques auxquels l'organisation est vulnérable. Les scénarios de sinistre devraient être basés sur ces situations graves, se produisant au pire moment possible, ayant pour résultat de perturber gravement la capacité de poursuivre les activités de l'organisation

B.6.e Recommander des mesures de protection réalisables et rentables pour prévenir ou réduire les risques et menaces ayant trait à la sécurité

B.6.f Établir un soutien continu au processus d'évaluation

B.7 Documenter et présenter l'évaluation de risques à la direction générale pour approbation

B.7.a Prépare un rapport d'évaluation des risques

B.7.b Présenter les résultats de l'évaluation des risques

(i) Contrôles satisfaisants

(ii) Recommander de nouveaux contrôles

(iii) Recommander des améliorations à des contrôles

(iv) Considérer les domaines adéquats pour transférer le risque

(v) Documenter les domaines pour lesquels la direction accepte le risque

B.7.c Déterminer les prochaines étapes pour amorcer le développement des stratégies de continuité d'activités

(i) Tenir compte des impacts identifiés dans le BIA

(ii) Tenir compte des menaces et risques identifiés dans l'analyse de risques