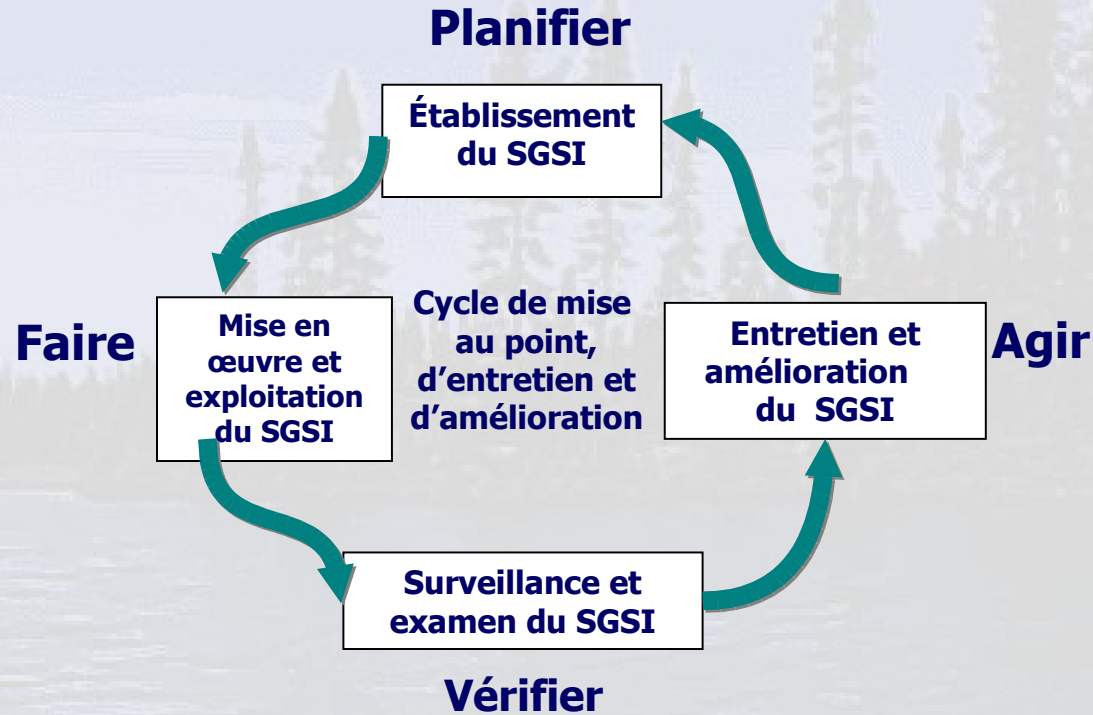


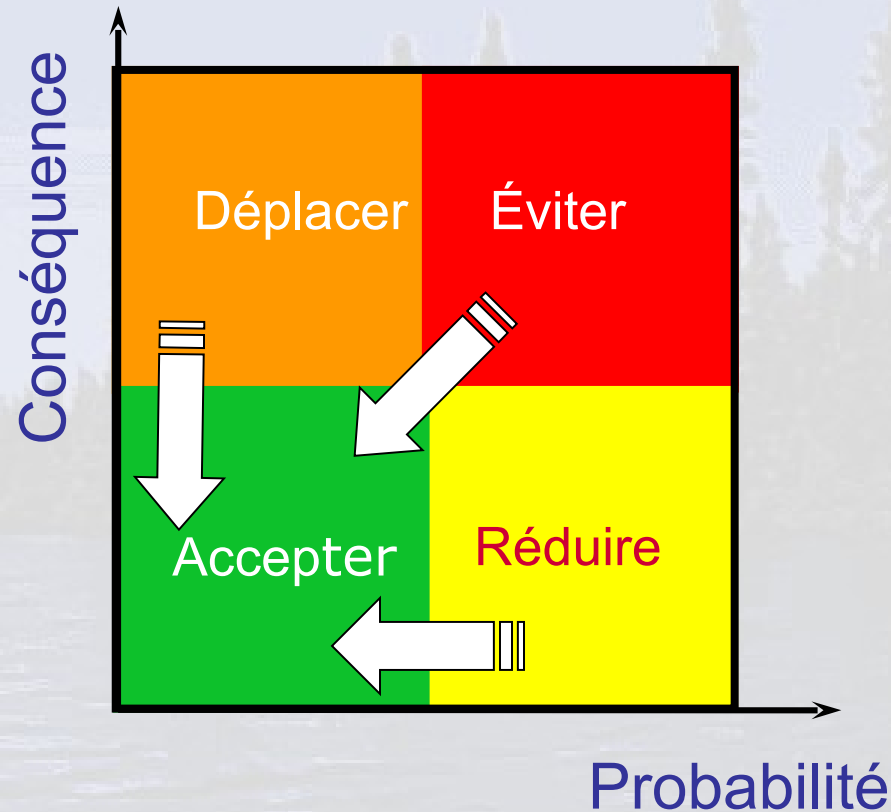
# Cours 8

## SYSTÈME DE GESTION DE LA SÉCURITÉ DE L'INFORMATION SGSI

# Systeme de gestion de la sécurité de l'information – SGSI



# Gestion et évaluation du risque SGSI

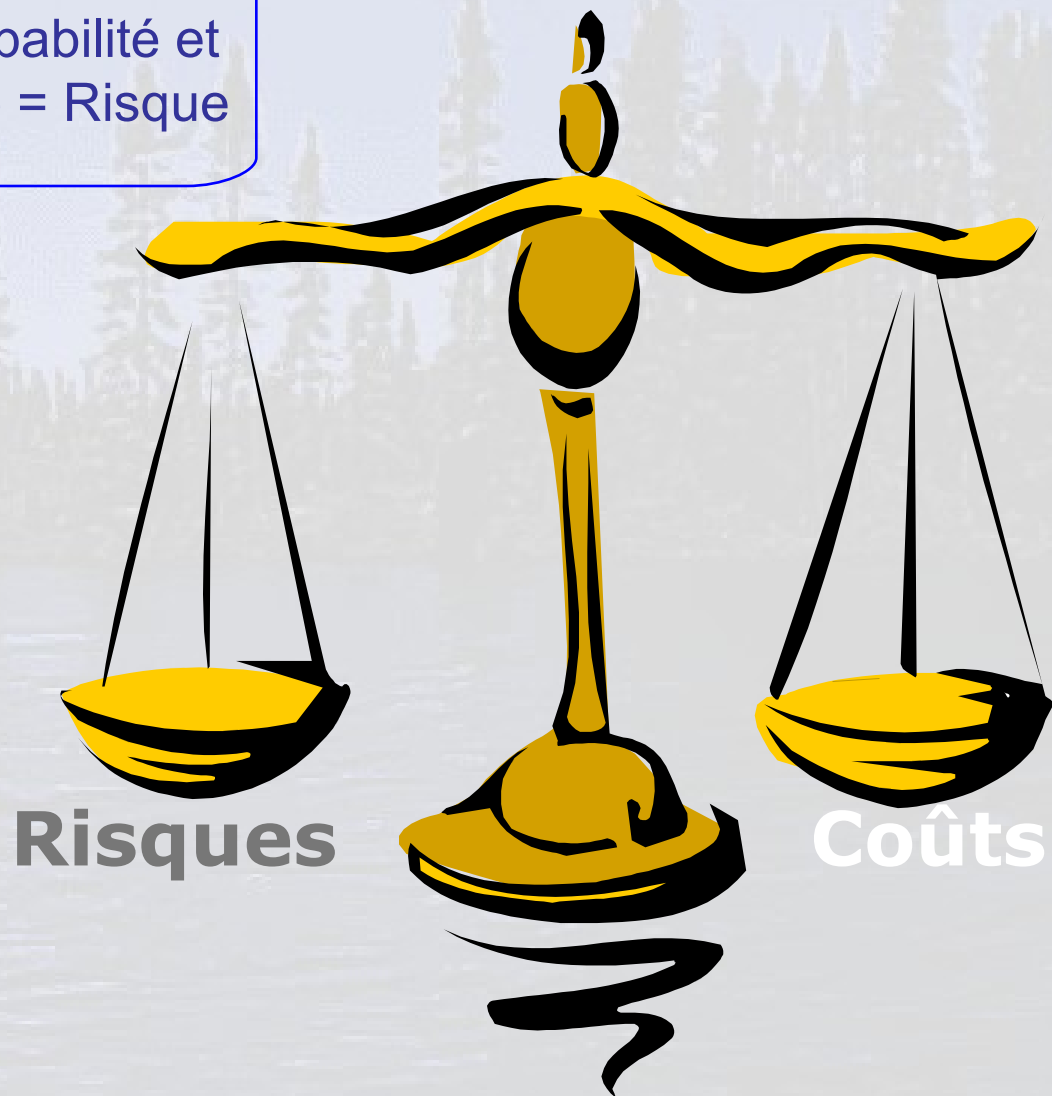


# Exigences du SGSI

Besoins de l'entreprise

Menace, probabilité et conséquence = Risque

Besoin de protection



# Mise en œuvre du SGSI

## Planifier

### Établissement du SGSI

- a) Définir la portée du SGSI
- b) Définir une politique du SGSI
- c) Définir une approche systématique d'évaluation du risque
- d) Déterminer les risques
- e) Évaluer les risques
- f) Identifier et évaluer les options pour le traitement des risques
- g) Sélectionner objectifs et contrôles pour le traitement des risques
- h) Préparer une déclaration d'applicabilité

# Mise en œuvre du SGSI



## Mise en œuvre et exploitation du SGSI

- a) Formuler un plan de traitement des risques
- b) Mettre en œuvre le plan de traitement des risques
- c) Mettre en œuvre les contrôles
- d) Mettre en œuvre les programmes de formation et de sensibilisation
- e) Gérer les opérations
- f) Gérer les ressources
- g) Mettre en œuvre les procédures et les autres contrôles pour la gestion des incidents

# Mise en œuvre du SGSI



**Planifier**

Établir le SGSI

**Faire**

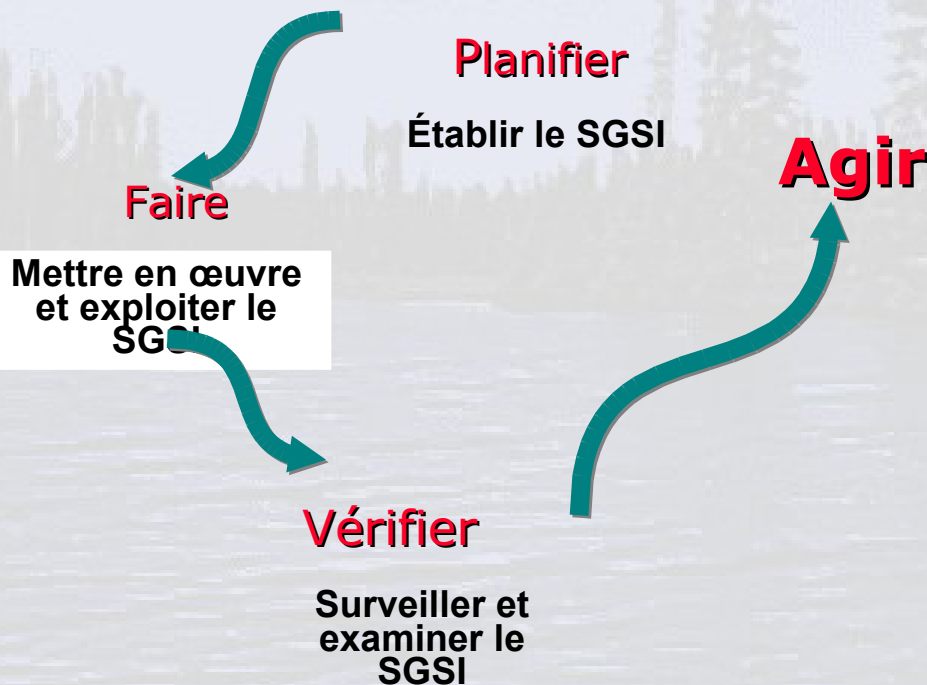
Mettre en œuvre  
et exploiter le  
SGSI

**Vérifier**

## **Surveillance et examen du SGSI**

- a) Exécuter les procédures de surveillance et les autres contrôles
- b) Examiner régulièrement l'efficacité du SGSI
- c) Examiner le degré de risque résiduel et de risque acceptable
- d) Effectuer des vérifications internes du SGSI
- e) Examiner la gestion du SGSI
- f) Enregistrer les mesures et les événements susceptibles d'avoir un effet sur l'efficacité du SGSI et sur son rendement

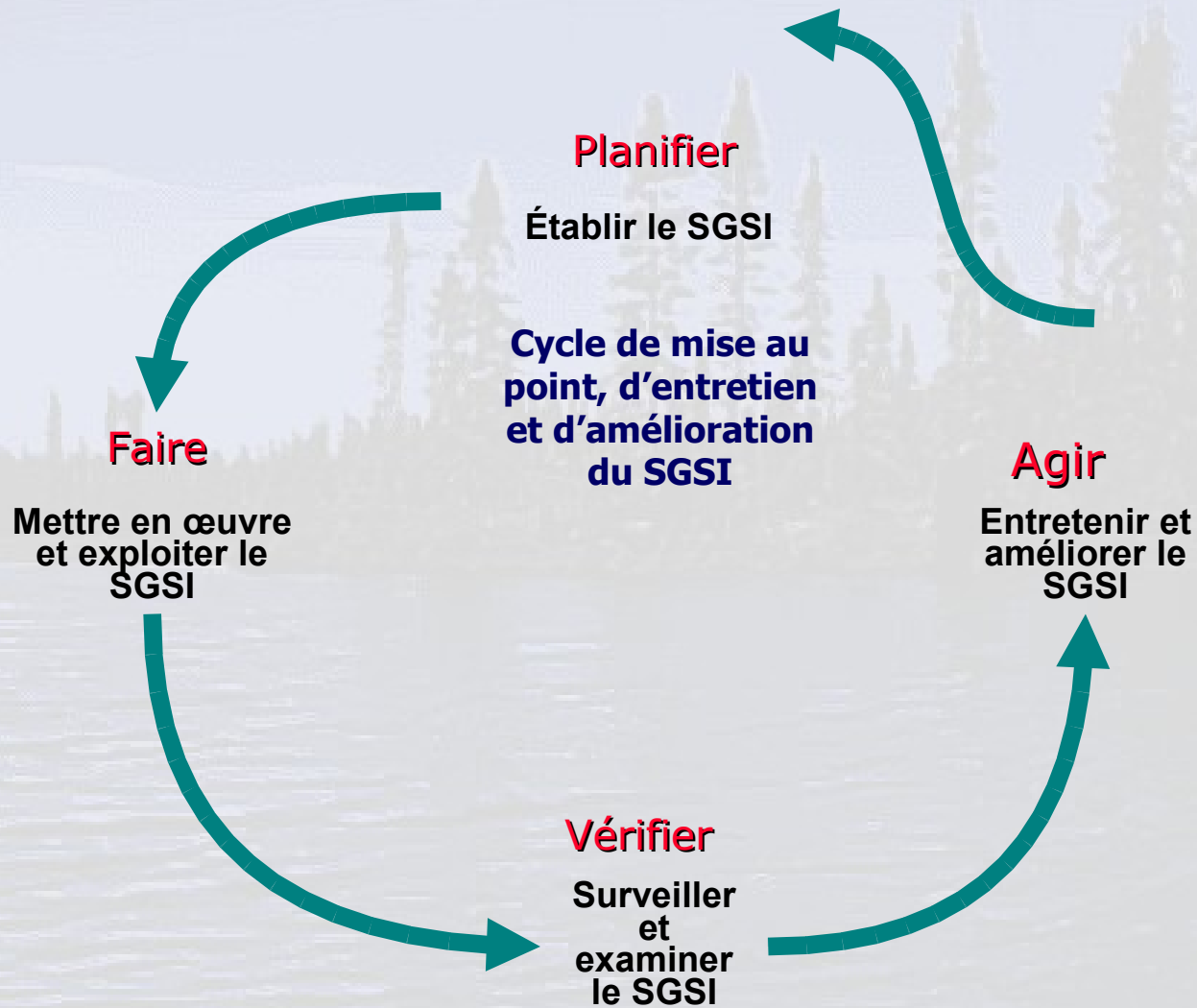
# Mise en œuvre du SGSI



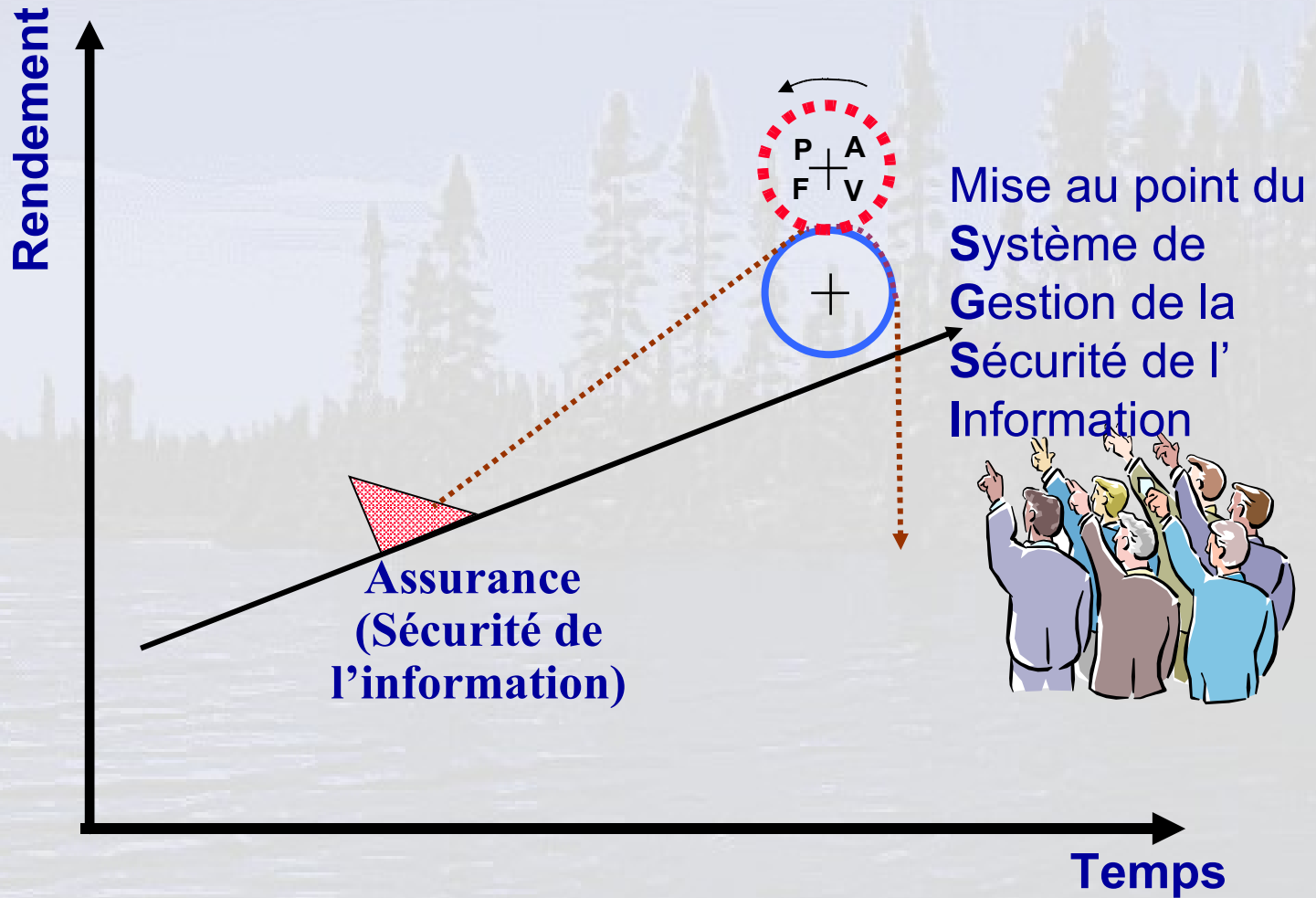
## Entretien et améliorer le SGSI

- Mettre en œuvre les améliorations identifiées
- Prendre des mesures correctives et préventives appropriées
- Communiquer les résultats et les actions entreprises et s'entendre avec toutes les parties intéressées
- Veiller à ce que les améliorations atteignent les résultats visés

# Mise en œuvre du SGSI



# Amélioration continue du SGSI



# Qui a besoin d'un SGSI?

Les organisations qui traitent de l'information :

- les banques;
- les gouvernements;
- les sociétés d'experts-conseils;
- les écoles et les universités;
- les compagnies d'assurance;
- les hôpitaux;

**Tout le monde!**

# Gestion de la sécurité dans les soins de santé à l'aide de ISO/CEI 17799

# Gestion de la sécurité dans les soins de santé à l'aide de ISO/CEI 17799

mise au point par le GT4 TC215 afin de  
fournir

une orientation détaillée aux  
organismes de soins de santé  
qui mettent en œuvre

ISO/CEI 17799 : 2000

The background of the slide is a soft-focus photograph of a calm lake with a dense forest of evergreen trees in the distance under a pale sky. The text is centered over this background.

# ISO/CEI 17799

# Comment établir les exigences de sécurité

## Sources des exigences de sécurité :

1. évaluation des risques;
2. exigences juridiques, législatives, réglementaires et contractuelles;
3. principes, objectifs et exigences fonctionnelles pour le traitement de l'information.

# SÉLECTION DES CONTRÔLES

Il faut sélectionner les contrôles et les mettre en œuvre en tenant compte :

- a) des exigences et des contraintes législatives et réglementaires;
- b) des exigences et des contraintes fonctionnelles et opérationnelles;
- c) du coût de mise en œuvre par rapport aux risques réduits et du maintien de la proportionnalité par rapport aux exigences et aux contraintes de l'organisation;
- d) des pertes potentielles en cas d'atteinte à la sécurité.

# FACTEURS DE SUCCÈS DÉTERMINANTS

- Politique de sécurité de l'information
- Respect de la culture organisationnelle
- Soutien et engagement
- Compréhension des exigences
- Commercialisation efficace
- Orientation
- Financement
- Sensibilisation
- Gestion des incidents
- Évaluation du rendement

## Section 4

# ÉVALUATION ET TRAITEMENT DES RISQUES

- ÉVALUATION DES RISQUES À LA SÉCURITÉ
  - identifier, quantifier et prioriser les risques par rapport à des critères et à des objectifs pertinents à l'organisation;
  - les résultats doivent guider et déterminer les mesures et les priorités de gestion appropriées.
- TRAITEMENT DES RISQUES À LA SÉCURITÉ
  - veiller à ce que les risques soient réduits à un degré acceptable en tenant compte :
    - des objectifs organisationnels;
    - des exigences et des contraintes de la législation;
    - des exigences et des contraintes opérationnelles;
    - du coût par rapport aux risques réduits et du maintien de la proportionnalité par rapport aux exigences de l'organisation;
    - de la nécessité d'équilibrer les investissements par rapport aux torts éventuels des risques.

## Section 5 POLITIQUE DE SÉCURITÉ

- POLITIQUE DE SÉCURITÉ DE L'INFORMATION
  - Contrôle 5.1.1 Document de la politique de sécurité de l'information
  - Contrôle 5.1.2 Examen de la politique de sécurité de l'information



## Section 6

# ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION

- ORGANISATION INTERNE
  - **Contrôle 6.1.1 Engagement de la direction par rapport à la sécurité de l'information**
  - **Contrôle 6.1.2 Coordination de la sécurité de l'information**
  - **Contrôle 6.1.3 Attribution des responsabilités liées à la sécurité de l'information**
  - **Contrôle 6.1.4 Processus d'approbation des installations de traitement de l'information**
  - **Contrôle 6.1.5 Ententes de confidentialité**
  - **Contrôle 6.1.6 Communication avec les autorités**
  - **Contrôle 6.1.7 Communication avec les groupes d'intérêt spéciaux**
  - **Contrôle 6.1.8 Examen indépendant de la sécurité de l'information**
- PARTIES EXTERNES
  - **Contrôle 6.2.1 Identification des risques liés aux parties externes**
  - **Contrôle 6.2.2 Sécurité dans les rapports avec la clientèle**
  - **Contrôle 6.2.3 Sécurité dans les rapports avec les titulaires de contrats d'entiercement**

## Section 7

# GESTION DE L'ACTIF INFORMATIONNEL

- **RESPONSABILITÉ POUR L'ACCÈS**
  - Contrôle 7.1.1 Inventaire de l'actif informationnel
  - Contrôle 7.1.2 Propriété de l'actif
  - Contrôle 7.1.3 Usage acceptable de l'actif
- **CLASSIFICATION DE L'INFORMATION**
  - Contrôle 7.2.1 Lignes directrices de classification
  - Contrôle 7.2.2 Manipulation et étiquetage de l'information

## Section 8 SÉCURITÉ DES RESSOURCES HUMAINES

- PRÉALABLE À L'EMPLOI
  - Contrôle 8.1.1 Rôles et responsabilités
  - Contrôle 8.1.2 Dépistage
  - Contrôle 8.1.3 Conditions d'emploi
- EN COURS D'EMPLOI
  - Contrôle 8.2.1 Responsabilités de gestion
  - Contrôle 8.2.2 Sensibilisation, formation et éducation à la sécurité de l'information
  - Contrôle 8.2.3 Processus disciplinaire
- CESSATION OU CHANGEMENT D'EMPLOI
  - Contrôle 8.3.1 Responsabilités en matière de cessation d'emploi
  - Contrôle 8.3.2 Retour des éléments d'actif informationnel
  - Contrôle 8.3.3 Retrait des droits d'accès

## Section 9

# SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

- ZONES SÉCURITAIRES
  - Contrôle 9.1.1 Périmètre de sécurité physique
  - Contrôle 9.1.2 Contrôles d'entrée physique
  - Contrôle 9.1.3 Sécurisation des bureaux, salles et installations
  - Contrôle 9.1.4 Protection contre les menaces externes et environnementales
  - Contrôle 9.1.5 Travail dans les zones sécuritaires
  - Contrôle 9.1.6 Zones d'accès public, de livraison et de chargement
- SÉCURITÉ DE L'ÉQUIPEMENT
  - Contrôle 9.2.1 Situation et protection de l'équipement
  - Contrôle 9.2.2 Services public de soutien
  - Contrôle 9.2.3 Sécurité du câblage
  - Contrôle 9.2.4 Entretien de l'équipement
  - Contrôle 9.2.5 Sécurité de l'équipement hors des lieux
  - Contrôle 9.2.6 Sécurité de la mise au rebut ou de la réutilisation de l'équipement
  - Contrôle 9.2.7 Retrait de la propriété

## Section 10

# GESTION DES COMMUNICATIONS ET DES OPÉRATIONS

- RESPONSABILITÉS ET PROCÉDURES OPÉRATIONNELLES
- GESTION DE LA LIVRAISON DES SERVICES À DES TIERS
- PLANIFICATION ET ACCEPTATION DES SYSTÈMES
- PROTECTION CONTRE LES CODES MALICIEUX ET MOBILES
- ARCHIVAGE
- GESTION DE LA SÉCURITÉ DES RÉSEAUX
- INTERVENTION AUPRÈS DES MÉDIAS
- ÉCHANGES D'INFORMATION
- SERVICES DE COMMERCE ÉLECTRONIQUE
- SURVEILLANCE

## Section 11

# CONTRÔLE D'ACCÈS

- EXIGENCES FONCTIONNELLES DU CONTRÔLE D'ACCÈS
- GESTION DES ACCÈS UTILISATEURS
- RESPONSABILITÉS DES UTILISATEURS
- CONTRÔLE D'ACCÈS AUX RÉSEAUX
- CONTRÔLE D'ACCÈS AU SYSTÈME D'EXPLOITATION
- CONTRÔLE D'ACCÈS AUX APPLICATIONS ET À L'INFORMATION
- INFORMATIQUE MOBILE ET TÉLÉTRAVAIL

## Section 12

# ACQUISITION, DÉVELOPPEMENT ET ENTRETIEN DES SYSTÈMES D'INFORMATION

- EXIGENCES DE SÉCURITÉ DES SYSTÈMES D'INFORMATION
- TRAITEMENT CORRECT DES APPLICATIONS
- CONTRÔLES CRYPTOGRAPHIQUES
- SÉCURITÉ DES FICHIERS DE SYSTÈME
- SÉCURITÉ DES PROCESSUS DE DÉVELOPPEMENT ET DE SOUTIEN
- GESTION DE LA VULNÉRABILITÉ

## Section 13

# GESTION DES INCIDENTS EN SÉCURITÉ DE L'INFORMATION

- **SIGNALEMENT DES ÉVÉNEMENTS ET DES FAIBLESSES RELATIFS À LA SÉCURITÉ DE L'INFORMATION**
  - Contrôle 13.1.1 Signalement des événements relatifs à la sécurité de l'information
  - Contrôle 13.1.2 Signalement des faiblesses relatives à la sécurité
- **GESTION DES INCIDENTS ET DES AMÉLIORATIONS RELATIFS À LA SÉCURITÉ DE L'INFORMATION**
  - Contrôle 13.2.1 Responsabilités et procédures
  - Contrôle 13.2.2 Leçons des incidents relatifs à la sécurité de l'information
  - Contrôle 13.2.3 Recueil des preuves

## Section 14

# GESTION DE LA CONTINUITÉ DES OPÉRATIONS

- ASPECTS DE LA GESTION DE LA CONTINUITÉ DES OPÉRATIONS RELATIFS À LA SÉCURITÉ DE L'INFORMATION
  - Contrôle 14.1.1 Inclusion de la sécurité de l'information dans le processus de gestion de la continuité des opérations
  - Contrôle 14.1.2 Continuité des opérations et évaluation des risques
  - Contrôle 14.1.3 Élaboration et mise en œuvre de plans de continuité tenant compte de la sécurité de l'information
  - Contrôle 14.1.4 Cadre de planification de la continuité des opérations
  - Contrôle 14.1.5 Vérification, entretien et réévaluation des plans de continuité des opérations

## Section 15 RESPECT

- RESPECT DES EXIGENCES LÉGISLATIVES
  - Contrôle 15.1.1 Identification de la législation pertinente
  - Contrôle 15.1.2 Droits de propriété intellectuelle (DPI)
  - Contrôle 15.1.3 Sauvegarde des dossiers organisationnels
  - Contrôle 15.1.4 Protection des données et confidentialité des renseignements personnels
  - Contrôle 15.1.5 Prévention du mésusage des installations de traitement de l'information
  - Contrôle 15.1.6 Régulation des contrôles cryptographiques
- RESPECT DES POLITIQUES ET DES NORMES DE SÉCURITÉ
  - Contrôle 15.2.1 Respect des politiques et des normes de sécurité
  - Contrôle 15.2.2 Vérification du respect technique
- CONSIDÉRATIONS RELATIVES À LA VÉRIFICATION DES SYSTÈMES D'INFORMATION
  - Contrôle 15.3. Contrôles de vérification des systèmes d'information
  - Contrôle 15.3.2 Protection des outils de vérification des systèmes d'information