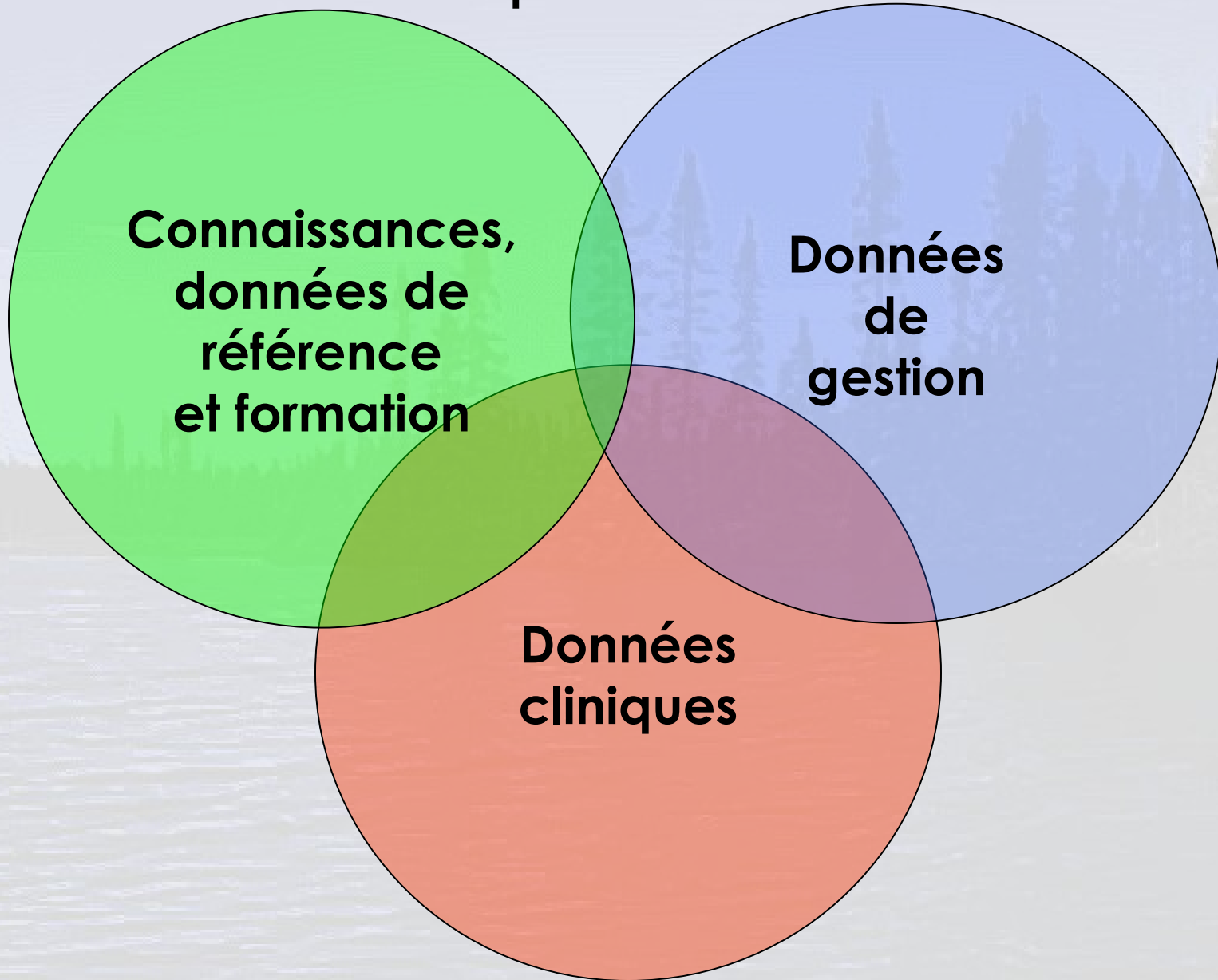


Gestion du risque avec *ISO/EIC 17799*

Code de bonnes pratiques pour
une meilleure gestion en sécurité
de l'information

Marc-André Léger, MScA (MIS)
Université de Sherbrooke

Informatique de la santé



Rôle de l'informatique dans la santé

- Informer la population;
- Éducation des patients;
- Gestion financière et statistiques;
- Gestion des ressources humaines;
- Support à la prise de décision aux professionnels de la santé;
- Formation continue des professionnels de la santé.

Inforoute Santé du Canada

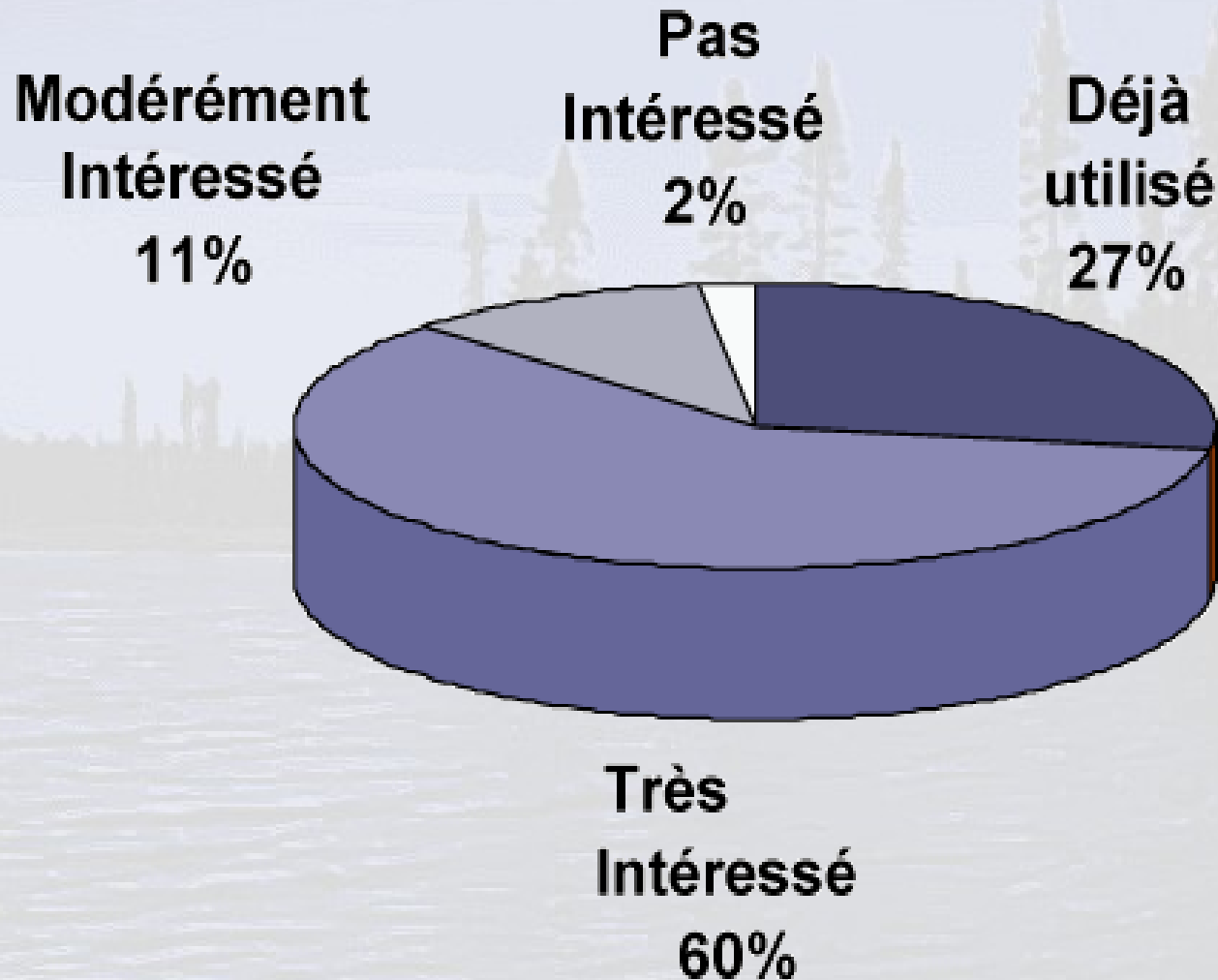
‘On reconnaît généralement que les dossiers de santé électroniques (DSE) sont essentiels à la modernisation du système de santé canadien ainsi que pour soutenir les objectifs du renouvellement des soins de santé : soit améliorer leur qualité, leur accessibilité et leur durabilité.’

Inforoute Santé du Canada, Plan d'affaires 2004
<http://www.infoway-inforoute.ca/>

L'utilisation de normes et de méthodes

*Mes recherches en matière de sécurité de l'information démontrent que l'utilisation de normes et de méthodes constituent l'une des **meilleures façons de mettre en place des processus** susceptibles de produire avec constance des résultats de qualité.*

L'intérêt pour les normes de sécurité est grandissant



Source : Giga Information Group

Les normes en santé

- ISO : International
- TC 215 : Informatique de la santé
- CEN : Europe
- DICOM – Imagerie
- ICD-9 (ICD-10)
- EDIFACT - Nations Unies
- HL7 – Échanges de données cliniques
- IEEE – Appareils médicaux

Pourquoi utiliser une norme en sécurité de l'information?

- Ne rien oublier
- Établir un climat de confiance
- Sécuriser les partenariats
- Favoriser les échanges électronique
- Mieux gérer le risque
- Réductions de coûts
- Économies d'échelle
- Diminution des primes d'assurances
- Appels d'offres le demande (Europe)
- Image de marque vis à vis de la sécurité
- Conformité (SOX, HIPPA)

Enjeux de la sécurité de l'information dans la santé

- L'identification de lignes directrices;
- La reconnaissance l'importance de la sécurité de l'information par les professionnels de la santé;
- Démonstrabilité du niveau de sécurité de l'information;
- La mise en place de standards .

Notre suggestion

ISO 17799 est une bonne solution pour implanter la sécurité de l'information dans le secteur de la santé au Québec:

- Couvre les exigences du cadre global de gestion des actifs informationnels du MSSS;
- État de l'art en sécurité;
- Outils disponibles;
- Expertise disponible;
- Utilisé ailleurs dans la santé;
- Économies d'échelles possible.

ISO 17799 dans la Santé

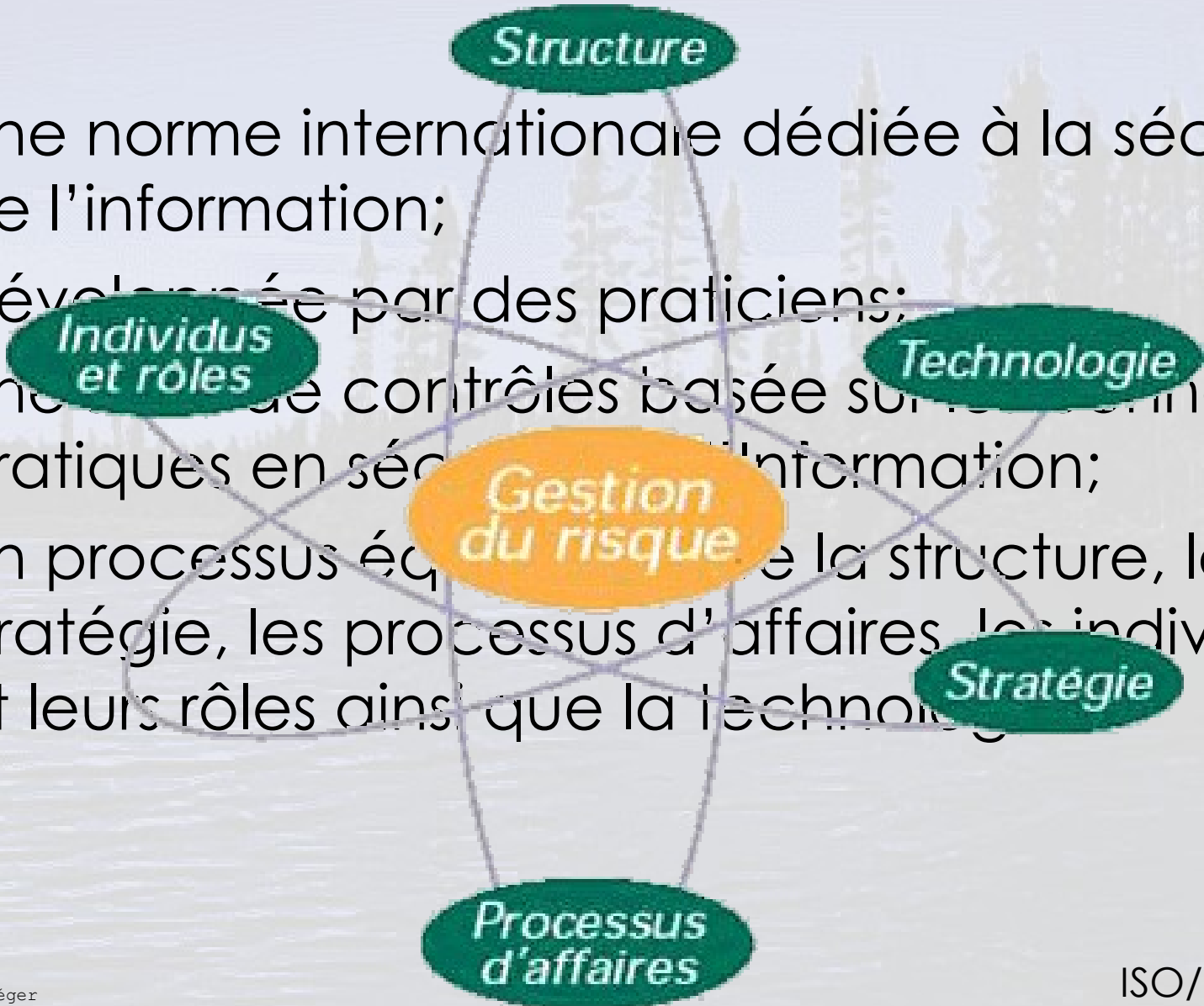
- Royaume Unis (NHS)
- Nouvelle Zélande
- Australie
- Suède
- Alberta
- USA (pour la conformité HIPPA)

ISO/EIC 17799:2000

La norme *ISO/EIC 17799:2000* est la norme **la plus utilisée** actuellement pour l'établissement de lignes directrices en matière de sécurité de l'information **à travers le monde.**

ISO/EIC 17799:2000 est:

- Une norme internationale dédiée à la sécurité de l'information;
- Développée par des praticiens;
- Une série de contrôles basée sur les meilleures pratiques en sécurité de l'information;
- Un processus équilibré de la structure, la stratégie, les processus d'affaires, les individus et leurs rôles ainsi que la technologie.



ISO/EIC 17799:2000 n'est pas:

- Une norme technique orientée produit ou logiciel
- Une norme de gestion de risques
- Une norme de classification des actifs
- Une norme d'évaluation technologique
- Un système de gestion de la sécurité de l'information
- Une norme qui offre des schémas de certification

Qu'est-ce ça prend pour implanter ISO/EIC 17779 ?

- Politique de sécurité
- Méthode d'évaluation du risque
- ISMS
- Sélection de contrôles
- Architecture de sécurité

Méthode d'analyse de risques

ISO/EIC 17799:2000 ne précise aucune obligation quant à la méthode d'analyse de risques. Chaque organisation ayant ses besoins et spécificités propres.

Les méthodes d'analyse de risque

Il existe différentes méthodes reconnues :

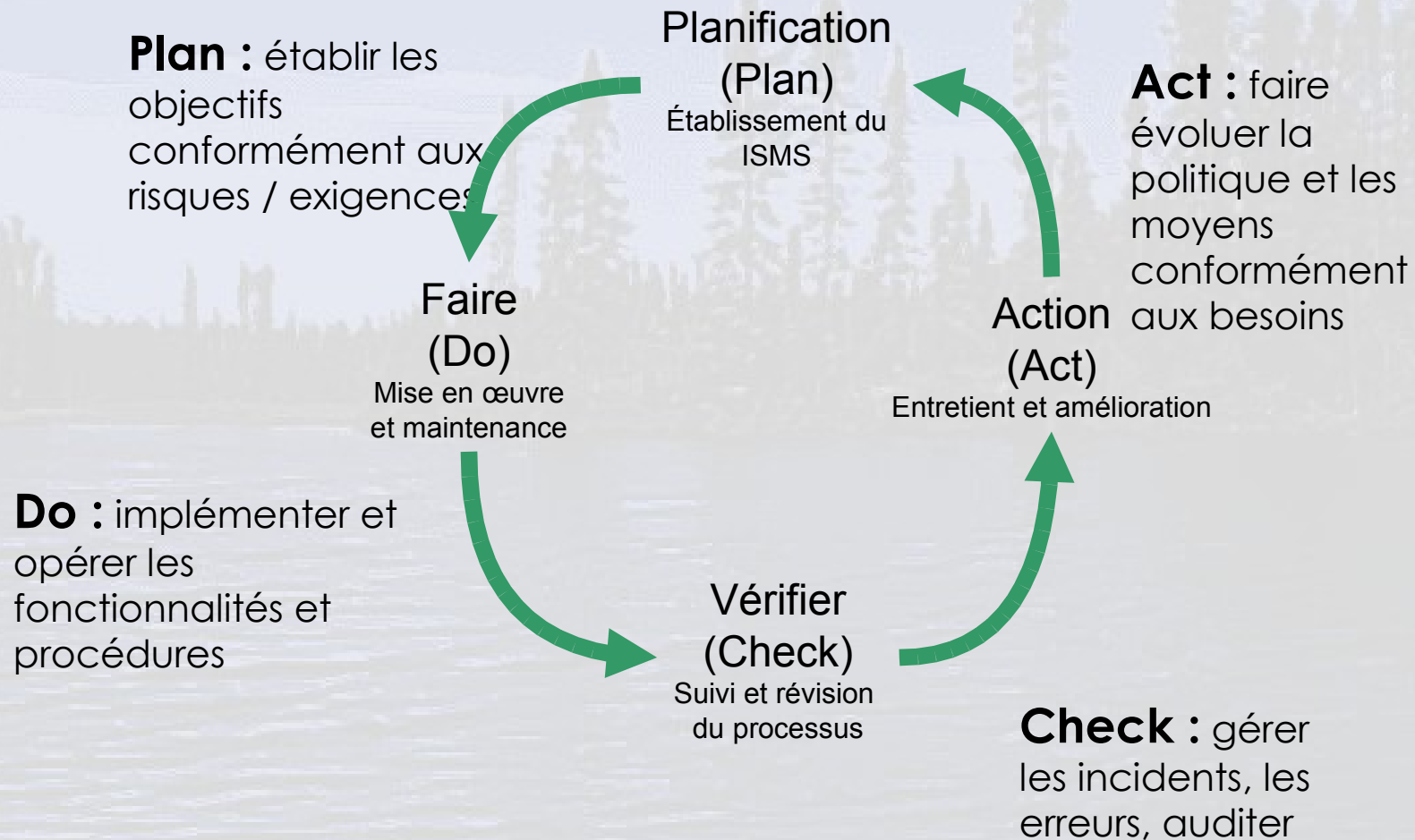
- Au Canada: MG-9 et TSIT
- Etats-Unis: Octave du CERT
- France: MEHARI-CLUSIF, EBIOS-DCSSI et MARION
- UK: CRAMM

ISMS

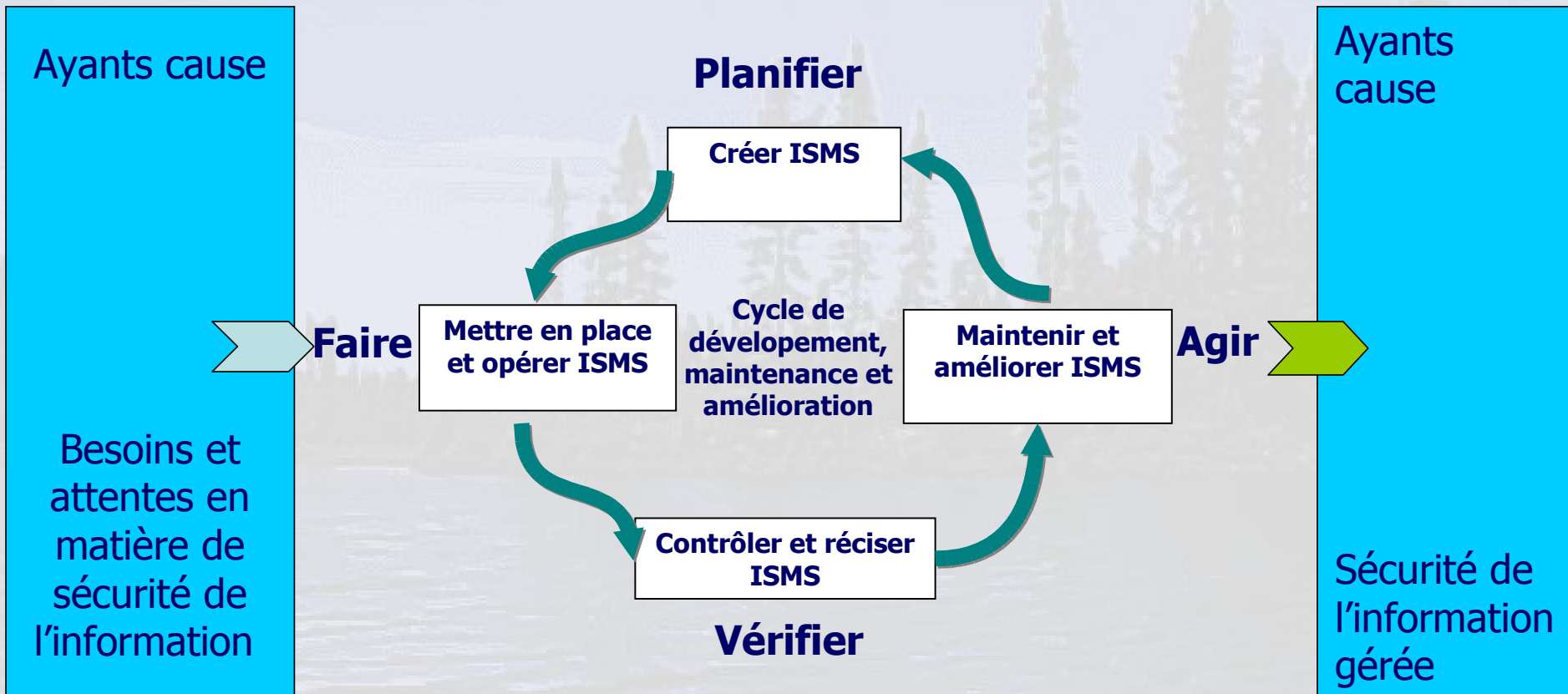
Systeme de gestion de la
sécurité de l'information

Mise en oeuvre d'un ISMS

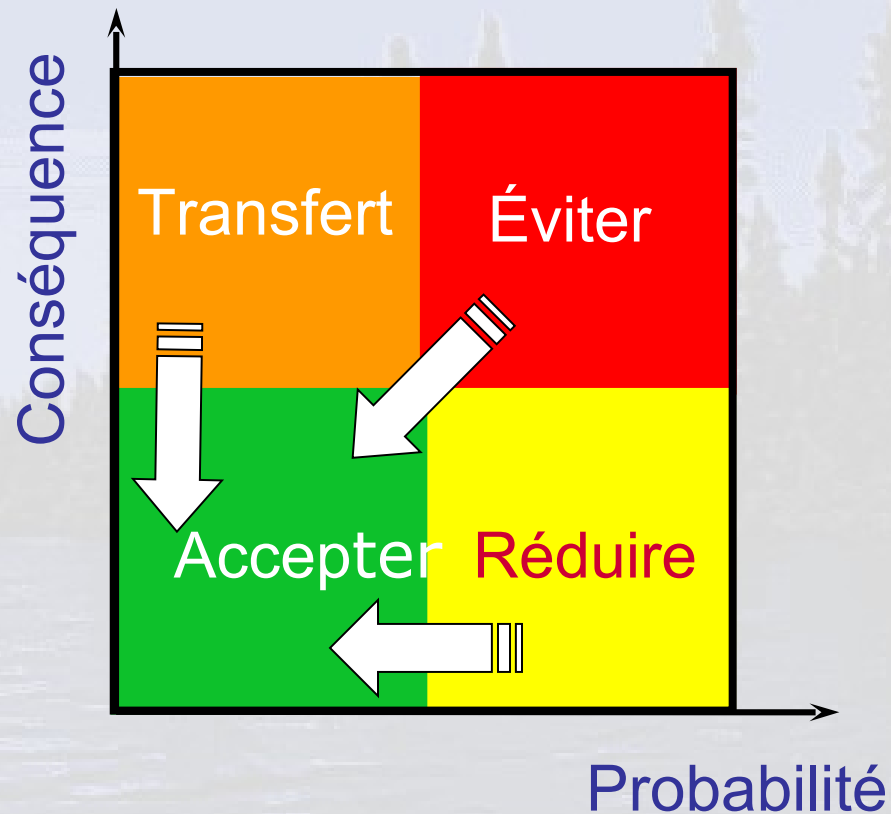
Modèle PDCA



Information Security Management System – ISMS



Évaluation et gestion du risque avec ISMS

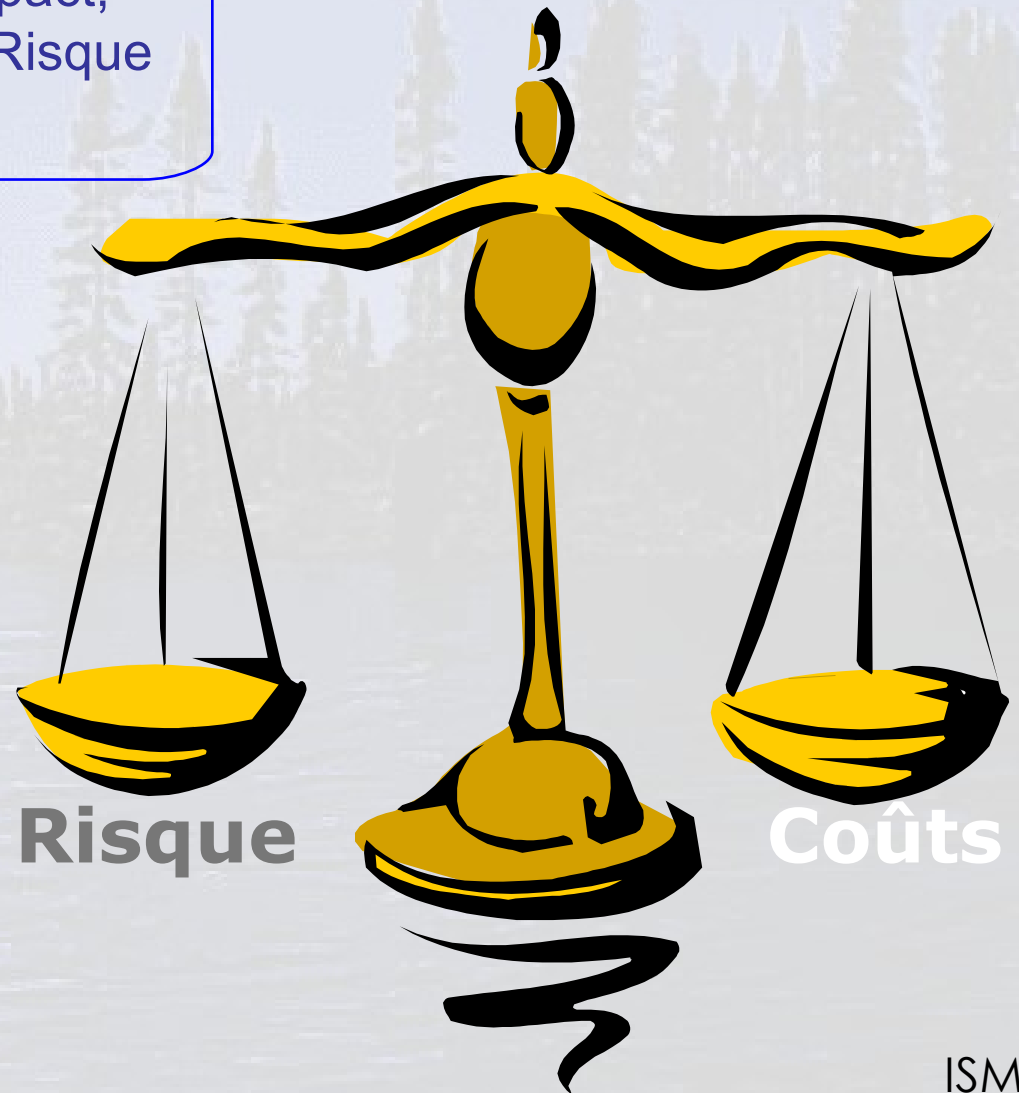


Identification des besoins

Besoins
d'affaires

Menace, Impact,
Probabilité = Risque

Besoin de
protection



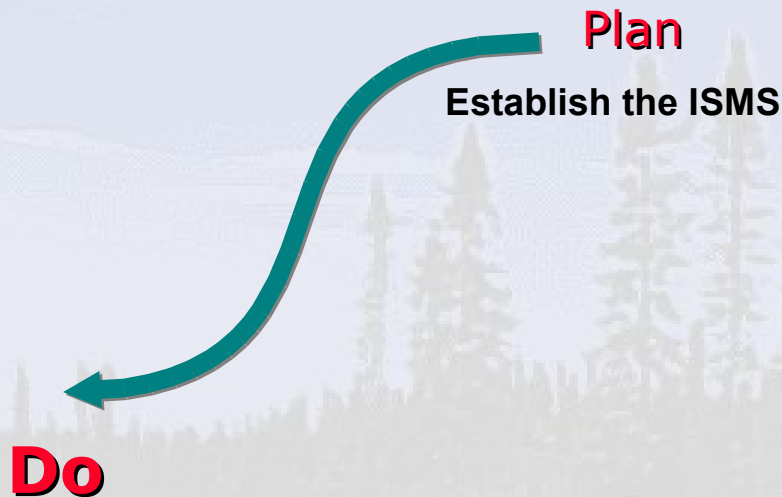
Mise en oeuvre du ISMS

Plan

Establish the ISMS

- a) Define scope of the ISMS
- b) Define an ISMS policy
- c) Define a systematic approach to risk assessment
- d) Identify risks
- e) Assess the risks
 - f) Identify and evaluate options for the treatment of risks
 - g) Select control objectives and controls for the treatment of risks
 - h) Prepare a Statement of Applicability

Mise en oeuvre du ISMS



Implement and operate the ISMS

- a) Formulate a risk treatment plan
- b) Implement the risk treatment plan
- c) Implement controls
- d) Implement training and awareness programmes
- e) Manage operations
- f) Manage resources
- g) Implement procedures and other controls for incident handling

Mise en oeuvre du ISMS

Plan

Establish the ISMS

Do

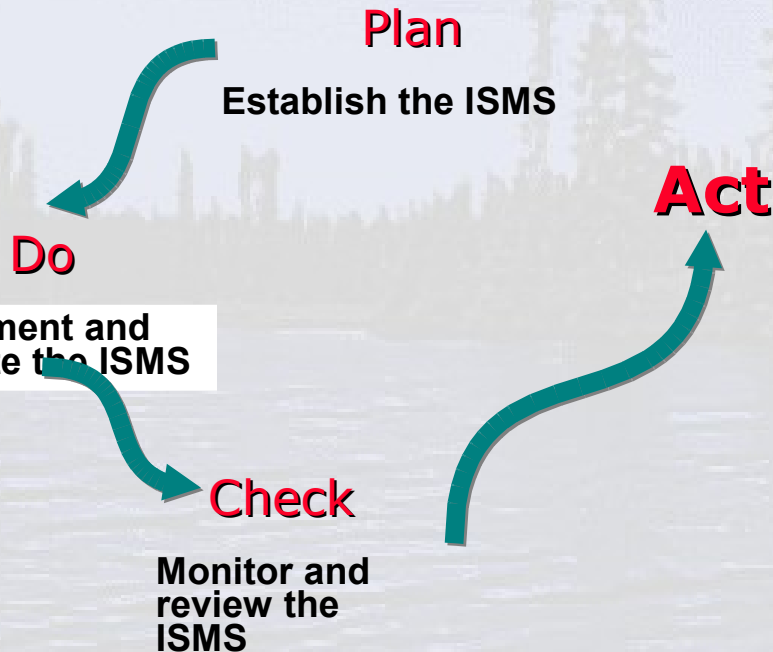
Implement and operate the ISMS

Check

Monitor and review the ISMS

- a) Execute monitoring procedures and other controls
- b) Undertake regular reviews of the effectiveness of the ISMS
- c) Review the level of residual risk and acceptable risk
- d) Conduct internal ISMS audits
- e) Undertake management review of the ISMS
- f) Record actions and events that could have an impact on the effectiveness or performance of the ISMS

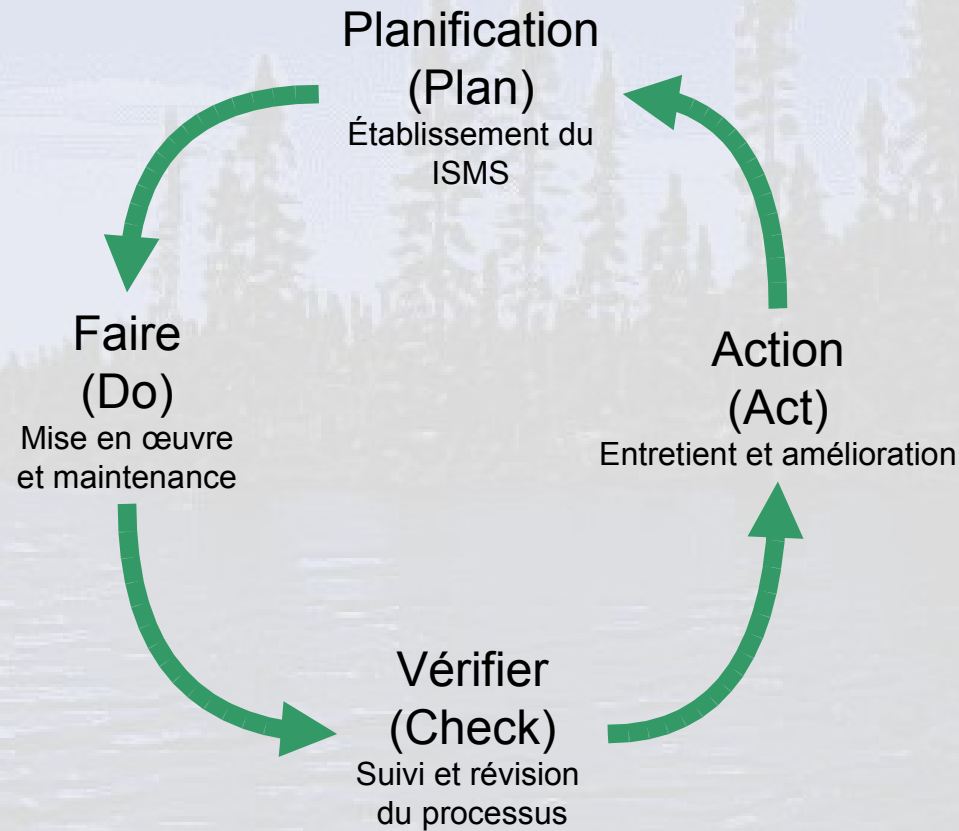
Mise en oeuvre du ISMS



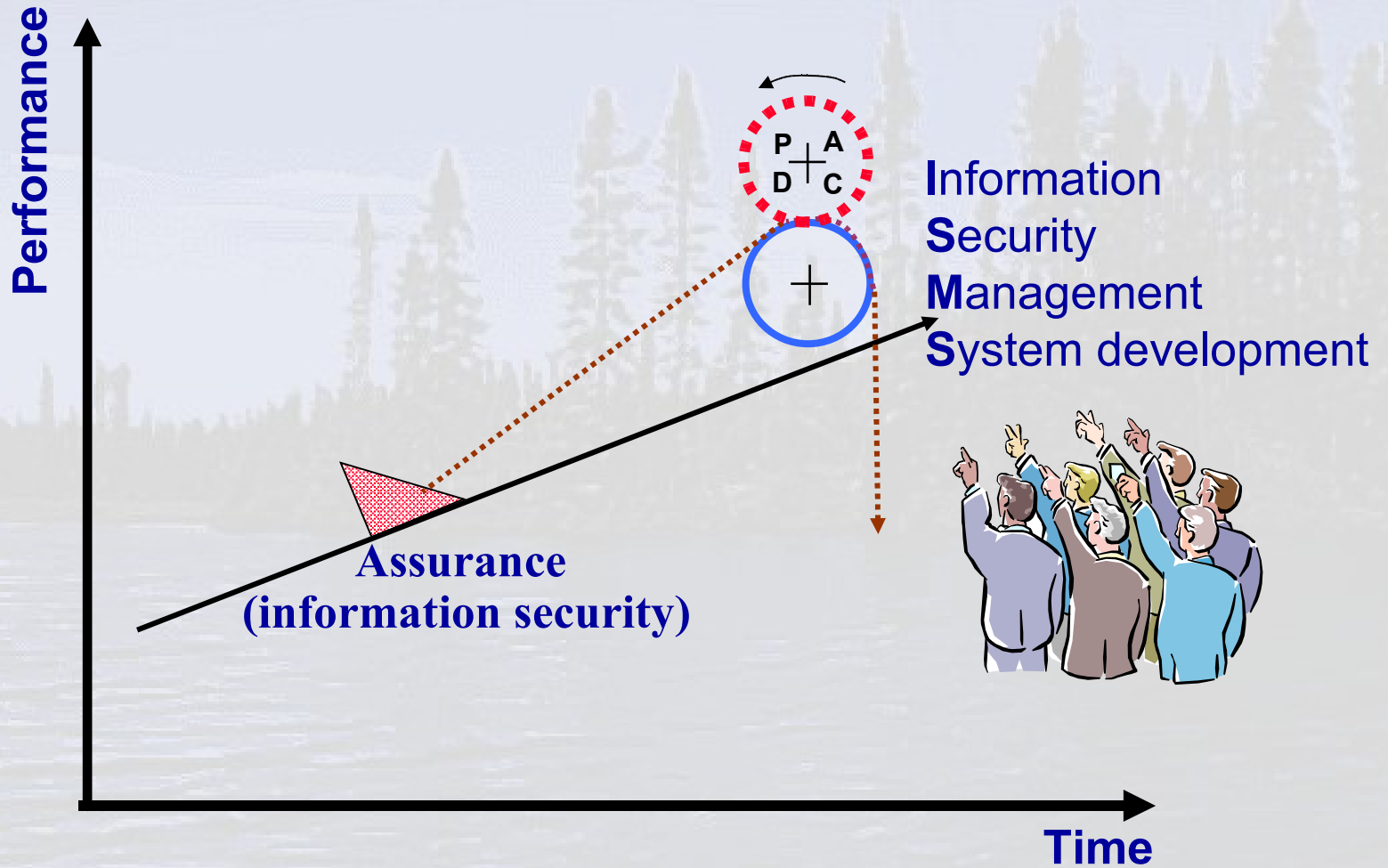
Maintain and improve the ISMS

- Implement the identified improvements
- Take appropriate corrective and preventive actions
- Communicate the results and actions and agree with all interested parties
- Ensure that the improvements achieve their intended objectives

Mise en oeuvre du ISMS



Amélioration continue du ISMS



Gérer la sécurité dans la santé avec ISO/IEC 17799



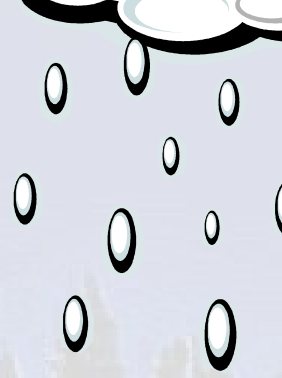
Comment établir les besoins

- Analyser l'organisation
- Évaluer le risque
 - légal,
 - réglementaire et
 - contractuel
- Déterminer les aspects éthiques
- Identifier les principes, objectifs et besoins d'affaires pour la gestion de l'information

Sélection des contrôles

Choisis en considérant:

- Les besoins et les obligations légales;
- Les besoins d'affaires;
- Le coût de mise en oeuvre considérant les risques en relation aux capacités de l'organisation; et
- Les pertes potentielles.



Facteurs critiques de succès

- Politique de sécurité de l'information
- Respect de la culture de l'organisation
- Support et engagement de la direction
- Compréhension des besoins
- Bon marketing
- Guides
- Financement adéquat
- Sensibilisation
- Gestion des incidents
- Évaluation de la performance

Section 4

RISK ASSESSMENT AND TREATMENT

- ASSESSING SECURITY RISKS
 - identify, quantify and prioritize risks against criteria and objectives relevant to the organization
 - The results should guide and determine the appropriate management action and priorities.
- TREATING SECURITY RISKS
 - ensure that risks are reduced to an acceptable level taking into account:
 - organizational objectives;
 - requirements and constraints of legislation;
 - operational requirements and constraints;
 - cost in relation to the risks being reduced, and remaining proportional to the organization's requirements;
 - the need to balance the investment against the harm likely to result.

Section 5

SECURITY POLICY

- INFORMATION SECURITY POLICY
 - Control 5.1.1 Information security policy document
 - Control 5.1.2 Review of the information security policy



Section 6

ORGANIZING INFORMATION SECURITY

- INTERNAL ORGANIZATION
 - Control 6.1.1 Management commitment to information security
 - Control 6.1.2 Information security co-ordination
 - Control 6.1.3 Allocation of information security responsibilities
 - Control 6.1.4 Approval process for information processing facilities
 - Control 6.1.5 Confidentiality agreements
 - Control 6.1.6 Contact with authorities
 - Control 6.1.7 Contact with special interest groups
 - Control 6.1.8 Independent review of information security
- EXTERNAL PARTIES
 - Control 6.2.1 Identification of risks related to external parties
 - Control 6.2.2 Addressing security when dealing with customers
 - Control 6.2.3 Addressing security in third party agreements

Section 7

ASSET MANAGEMENT

- RESPONSIBILITY FOR ASSETS
 - Control 7.1.1 Inventory of assets
 - Control 7.1.2 Ownership of assets
 - Control 7.1.3 Acceptable use of assets
- INFORMATION CLASSIFICATION
 - Control 7.2.1 Classification guidelines
 - Control 7.2.2 Information labeling and handling

Section 8

HUMAN RESOURCES SECURITY

- PRIOR TO EMPLOYMENT
 - Control 8.1.1 Roles and responsibilities
 - Control 8.1.2 Screening
 - Control 8.1.3 Terms and conditions of employment
- DURING EMPLOYMENT
 - Control 8.2.1 Management responsibilities
 - Control 8.2.2 Information security awareness, education and training
 - Control 8.2.3 Disciplinary process
- TERMINATION OR CHANGE OF EMPLOYMENT
 - Control 8.3.1 Termination responsibilities
 - Control 8.3.2 Return of assets
 - Control 8.3.3 Removal of access rights

Section 9

PHYSICAL AND ENVIRONMENTAL SECURITY

- SECURE AREAS
 - Control 9.1.1 Physical security perimeter
 - Control 9.1.2 Physical entry controls
 - Control 9.1.3 Securing offices, rooms and facilities
 - Control 9.1.4 Protecting against external and environmental threats
 - Control 9.1.5 Working in secure areas
 - Control 9.1.6 Public access, delivery and loading areas
- EQUIPMENT SECURITY
 - Control 9.2.1 Equipment siting and protection
 - Control 9.2.2 Supporting utilities
 - Control 9.2.3 Cabling security
 - Control 9.2.4 Equipment maintenance
 - Control 9.2.5 Security of equipment off-premises
 - Control 9.2.6 Secure disposal or re-use of equipment
 - Control 9.2.7 Removal of property

Section 10

COMMUNICATIONS AND OPERATIONS MANAGEMENT

- OPERATIONAL PROCEDURES AND RESPONSIBILITIES
- THIRD PARTY SERVICE DELIVERY MANAGEMENT
- SYSTEM PLANNING AND ACCEPTANCE
- PROTECTION AGAINST MALICIOUS AND MOBILE CODE
- BACK-UP
- NETWORK SECURITY MANAGEMENT
- MEDIA HANDLING
- EXCHANGES OF INFORMATION
- ELECTRONIC COMMERCE SERVICES
- MONITORING

Section 11

ACCESS CONTROL

- BUSINESS REQUIREMENT FOR ACCESS CONTROL
- USER ACCESS MANAGEMENT
- USER RESPONSIBILITIES
- NETWORK ACCESS CONTROL
- OPERATING SYSTEM ACCESS CONTROL
- APPLICATION AND INFORMATION ACCESS CONTROL
- MOBILE COMPUTING AND TELEWORKING

Section 12

INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

- SECURITY REQUIREMENTS OF INFORMATION SYSTEMS
- CORRECT PROCESSING IN APPLICATIONS
- CRYPTOGRAPHIC CONTROLS
- SECURITY OF SYSTEM FILES
- SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES
- VULNERABILITY MANAGEMENT

Section 13

INFORMATION SECURITY INCIDENT MANAGEMENT

- REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES
 - Control 13.1.1 Reporting information security events
 - Control 13.1.2 Reporting security weaknesses
- MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS
 - Control 13.2.1 Responsibilities and procedures
 - Control 13.2.2 Learning from information security incidents
 - Control 13.2.3 Collection of evidence.

Section 14

BUSINESS CONTINUITY MANAGEMENT

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

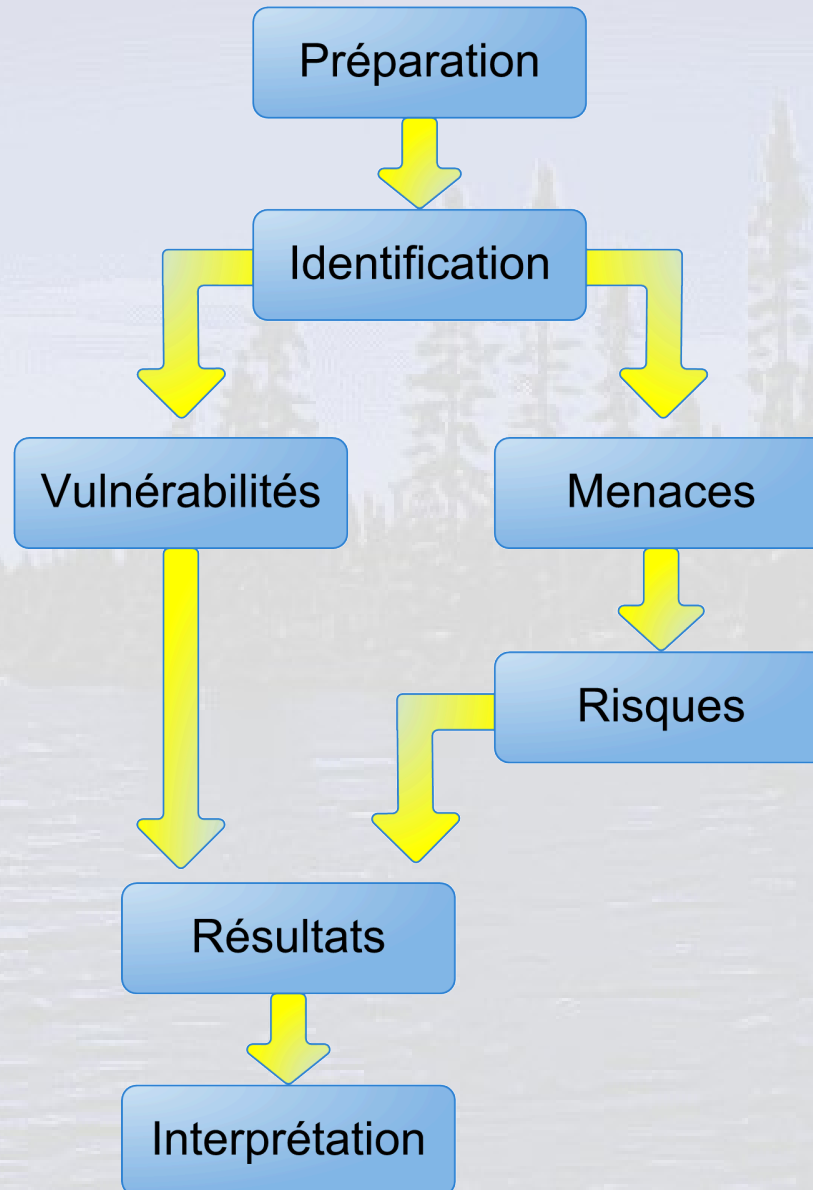
- Control 14.1.1 Including information security in the business continuity management process
- Control 14.1.2 Business continuity and risk assessment
- Control 14.1.3 Developing and implementing continuity plans including information security
- Control 14.1.4 Business continuity planning framework
- Control 14.1.5 Testing, maintaining and re-assessing business continuity plans

Section 15

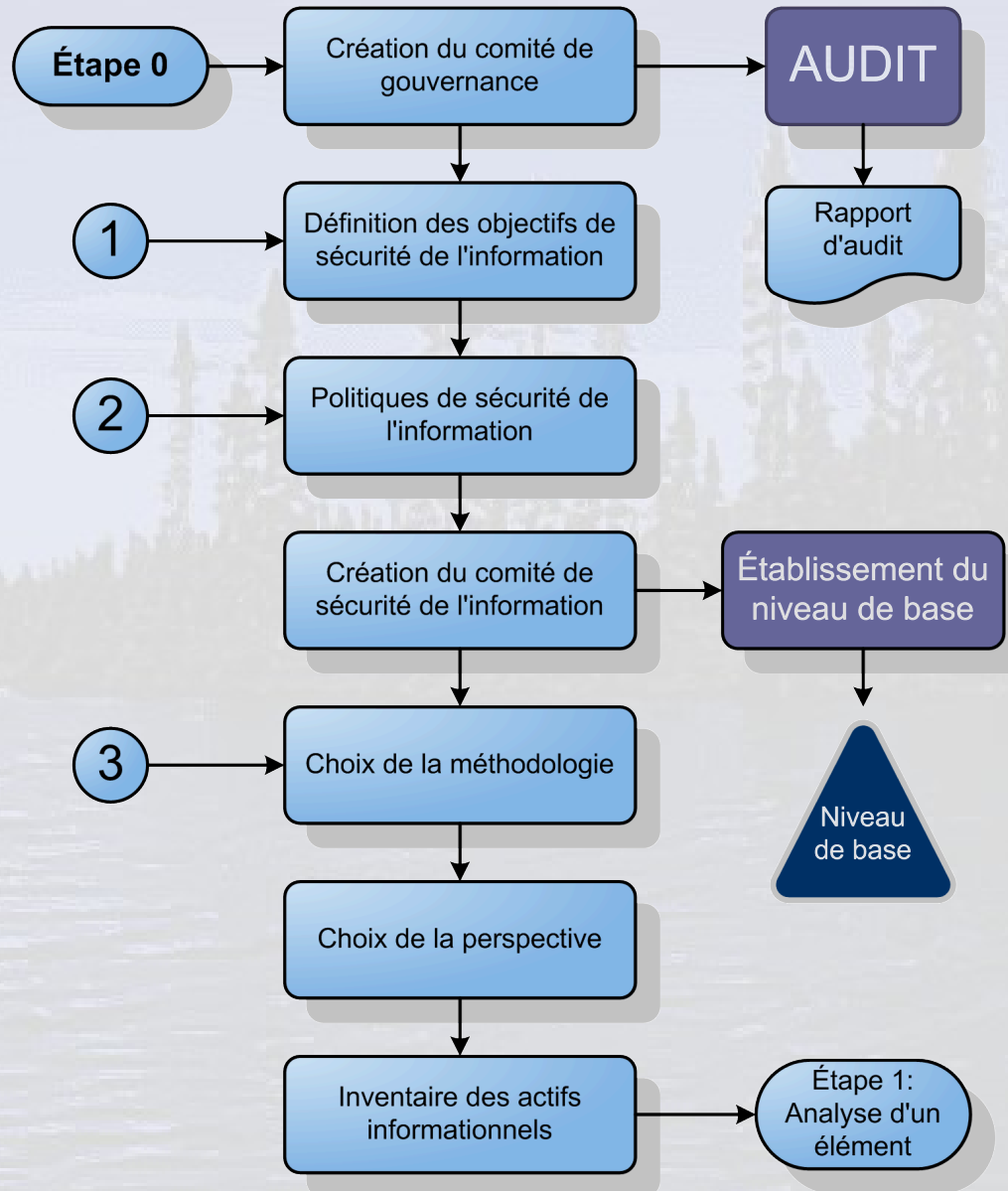
COMPLIANCE

- COMPLIANCE WITH LEGAL REQUIREMENTS
 - Control 15.1.1 Identification of applicable legislation
 - Control 15.1.2 Intellectual property rights (IPR)
 - Control 15.1.3 Safeguarding of organizational records
 - Control 15.1.4 Data protection and privacy of personal information
 - Control 15.1.5 Prevention of misuse of information processing facilities
 - Control 15.1.6 Regulation of cryptographic controls
- COMPLIANCE WITH SECURITY POLICIES AND STANDARDS
 - Control 15.2.1 Compliance with security policy and standards
 - Control 15.2.2 Technical compliance checking
- INFORMATION SYSTEMS AUDIT CONSIDERATIONS
 - Control 15.3.1 Information systems audit controls
 - Control 15.3.2 Protection of information systems audit tools

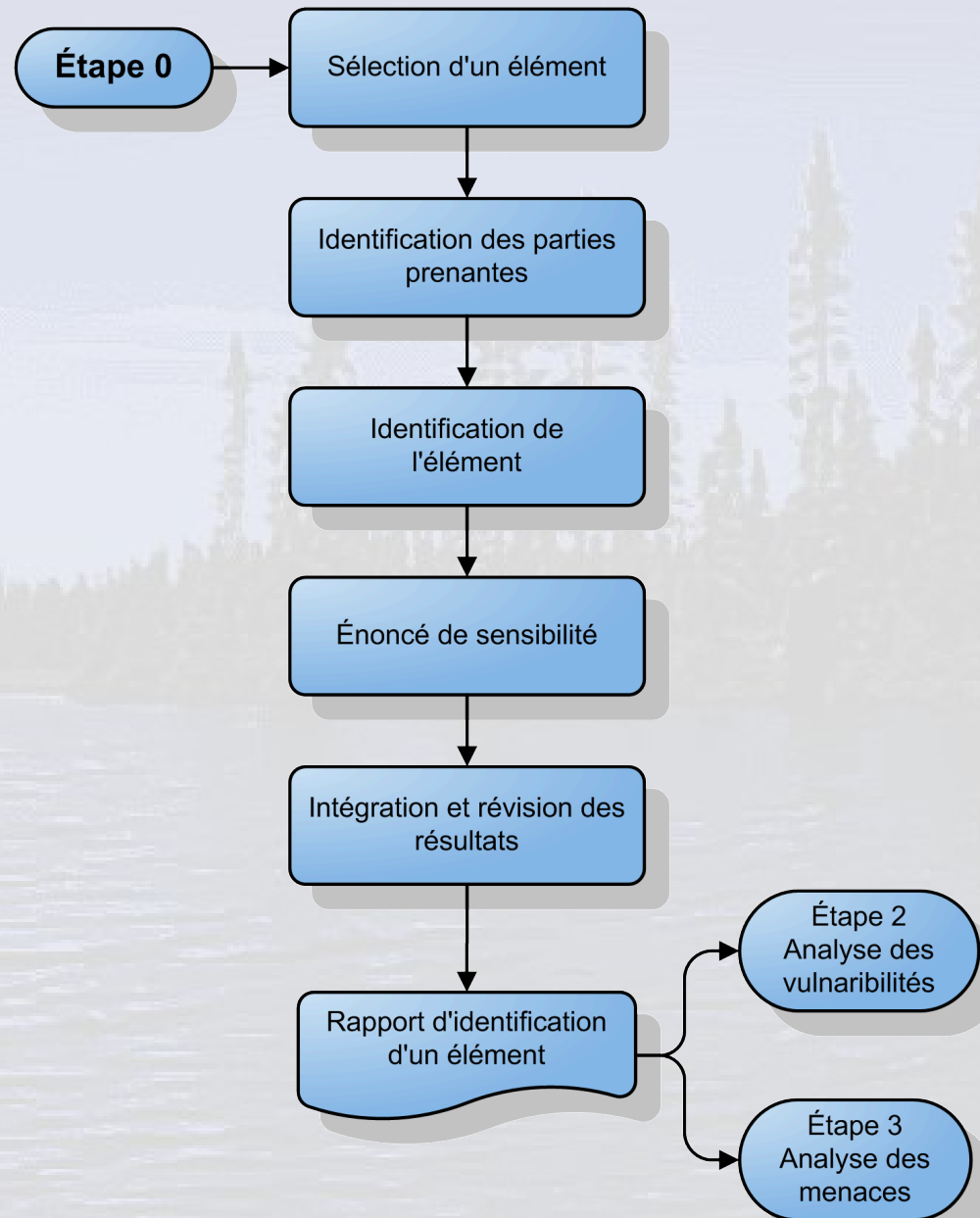
Méthodologie IVRI™ de gestion du risque



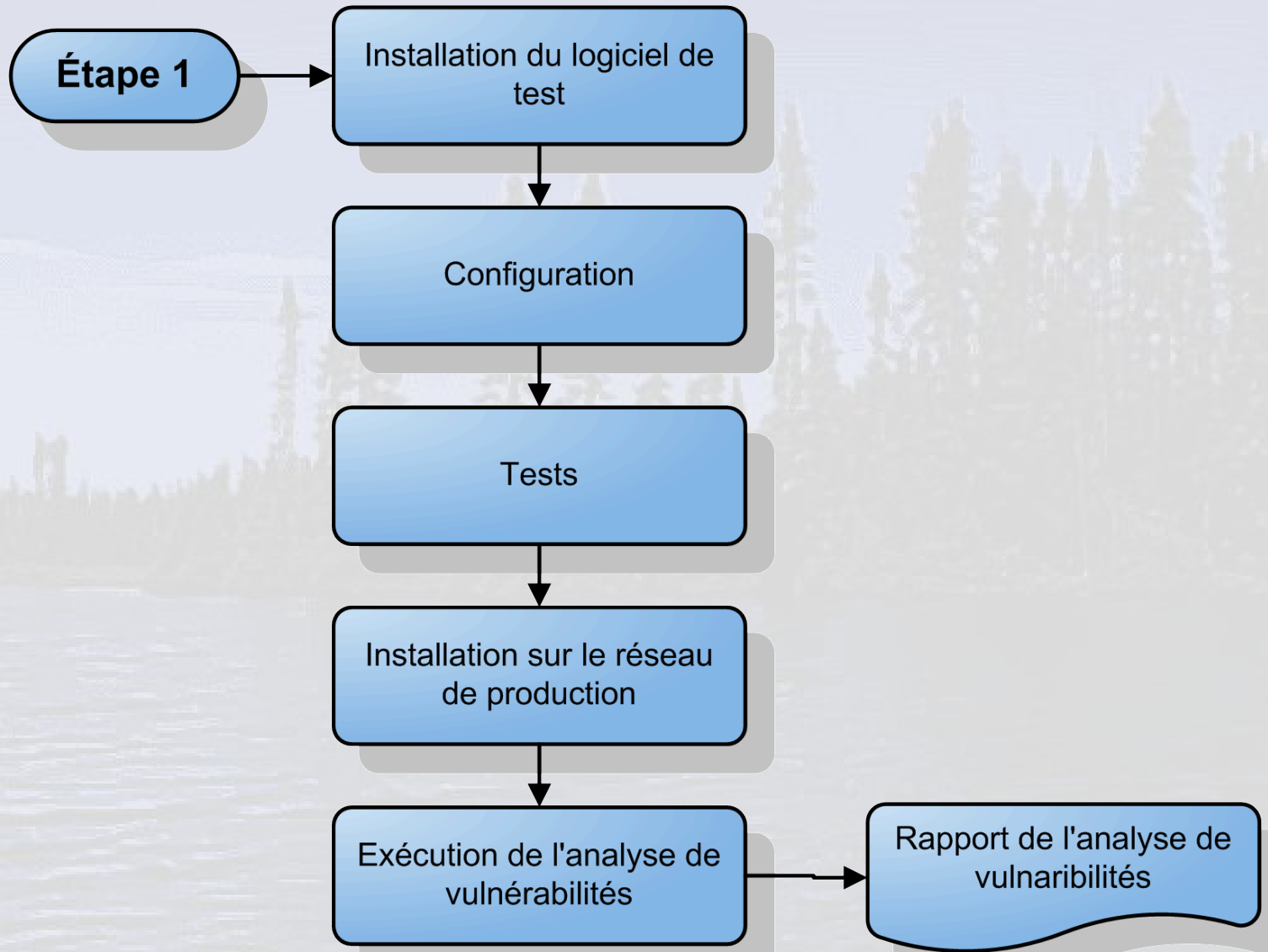
Préparation



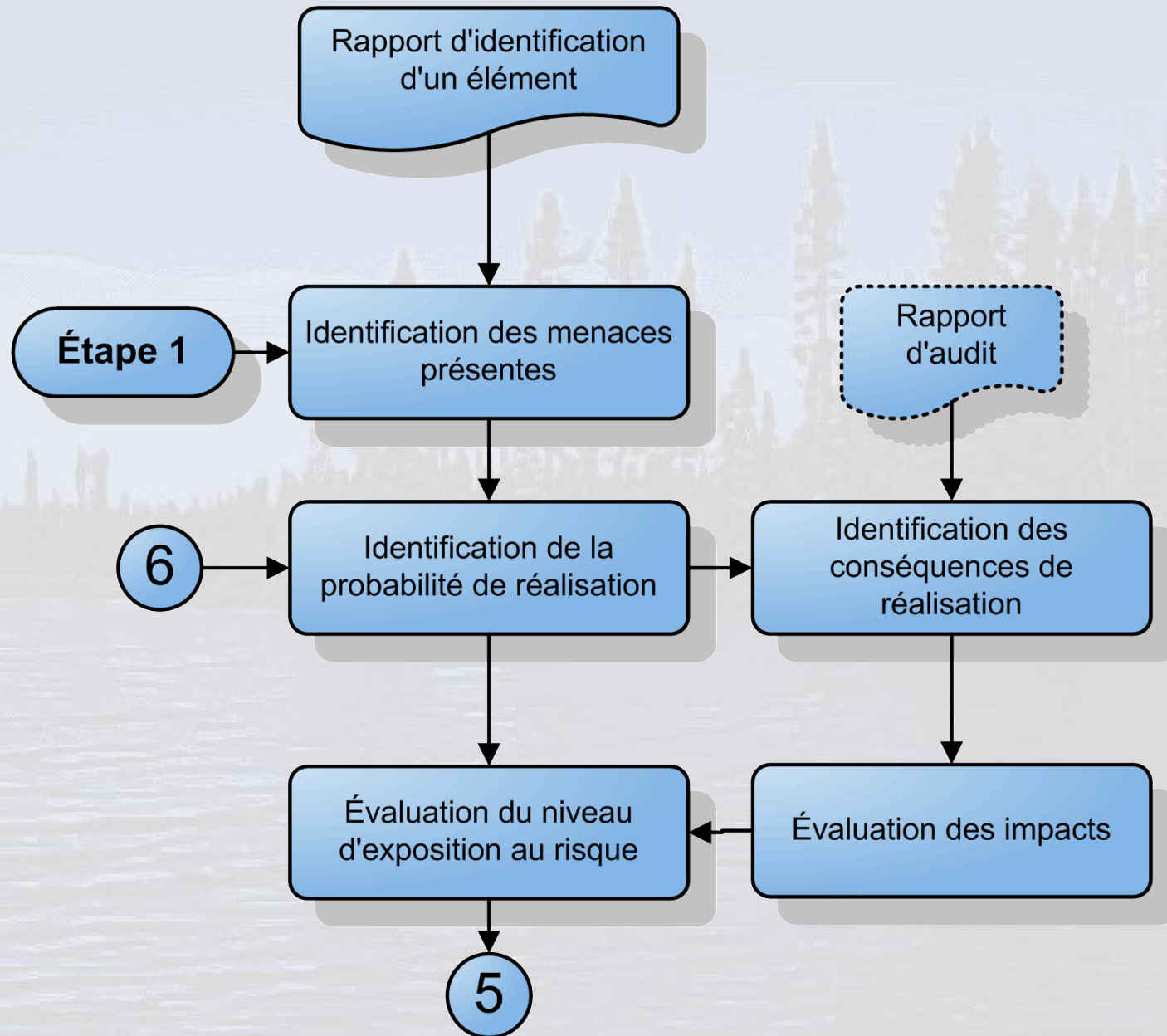
Identification d'un élément



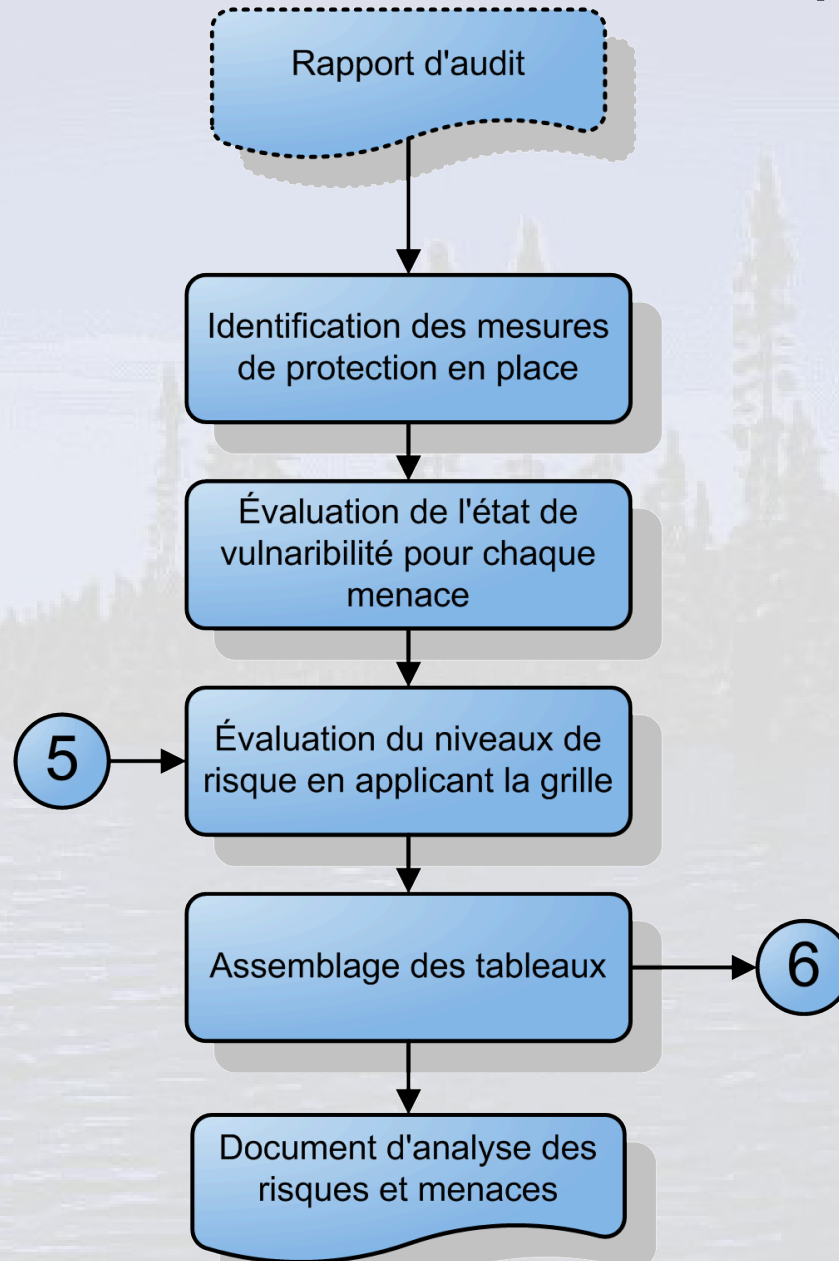
Analyse des vulnérabilités



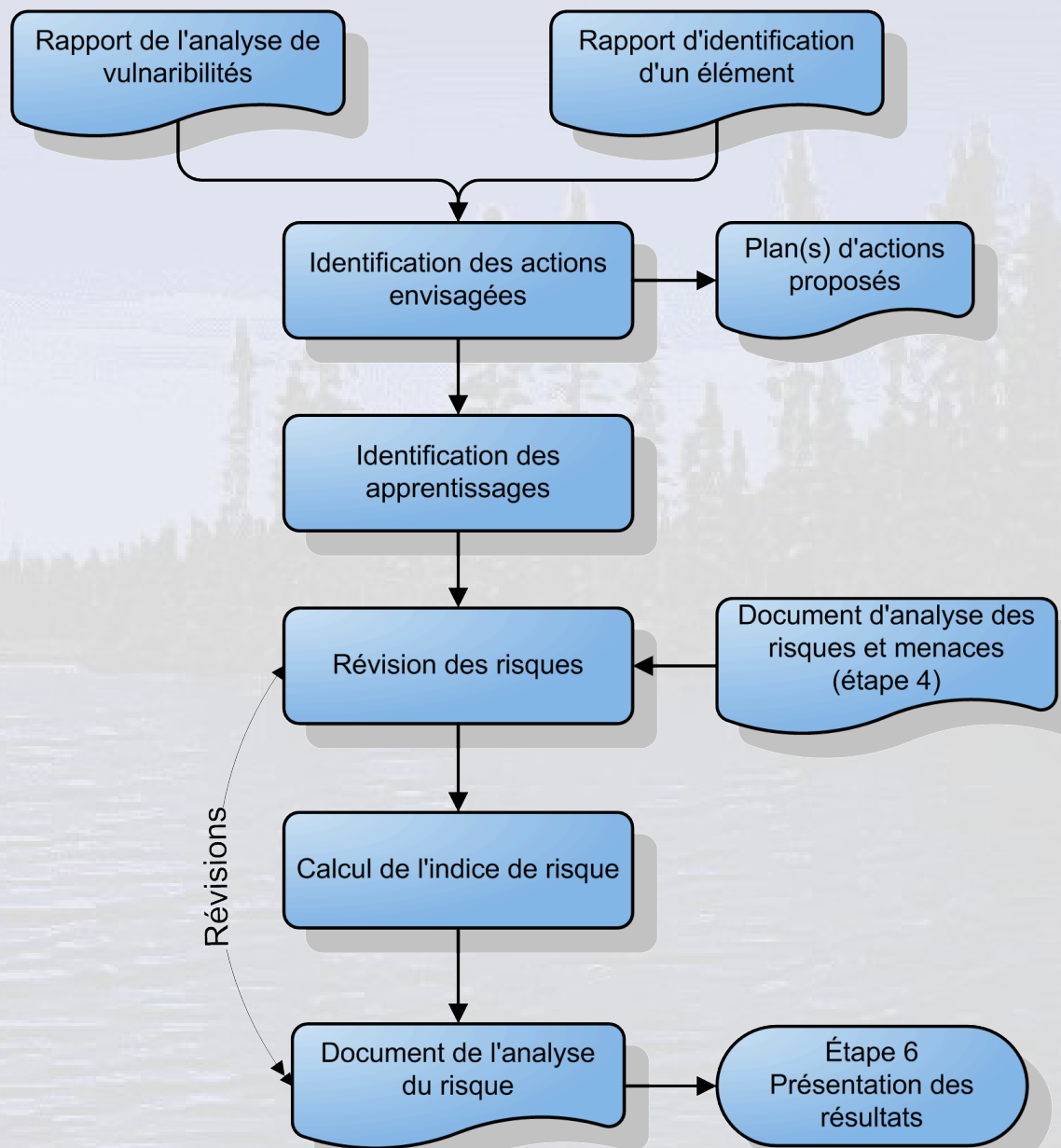
Évaluation de la menace



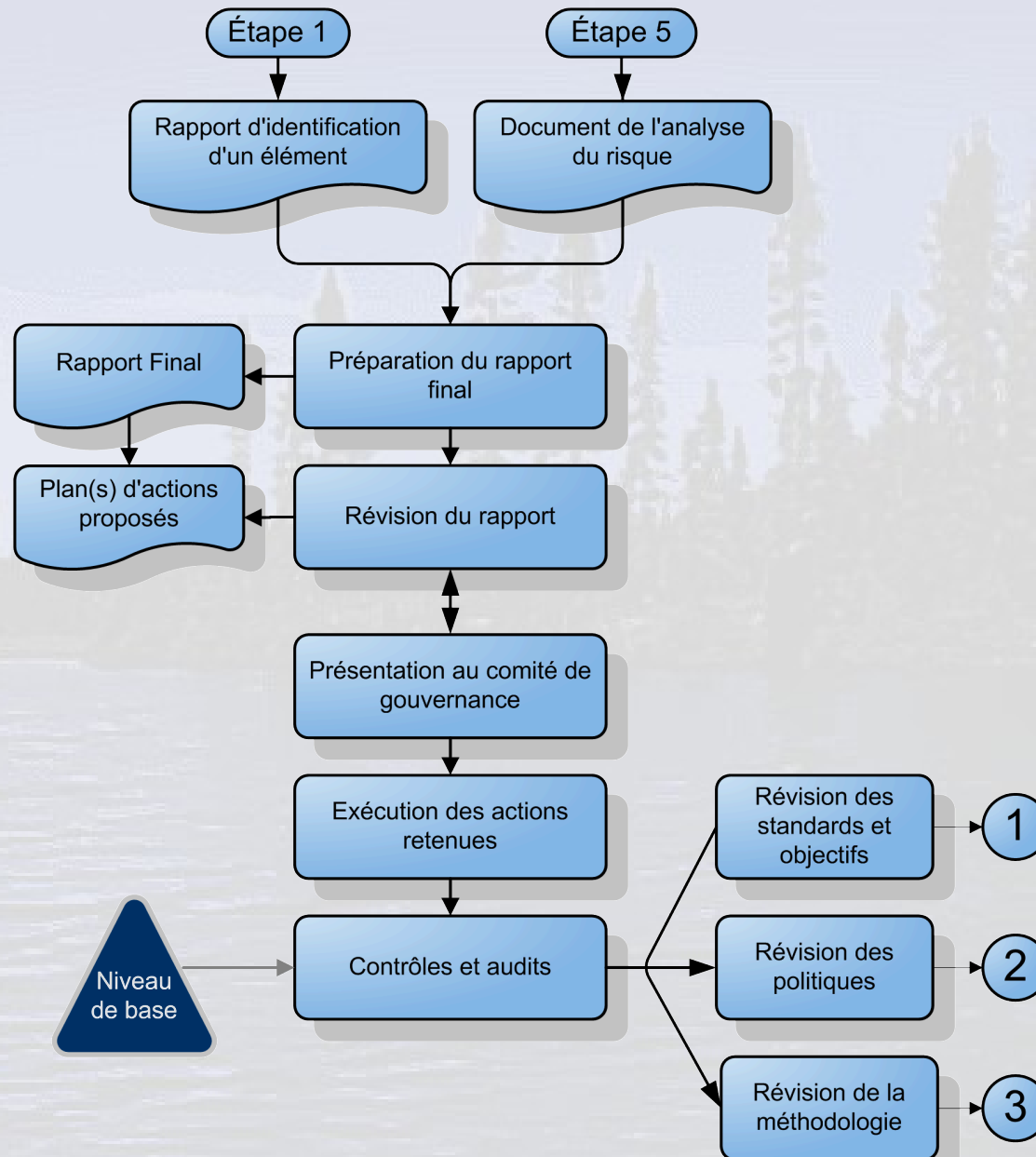
Évaluation des risques

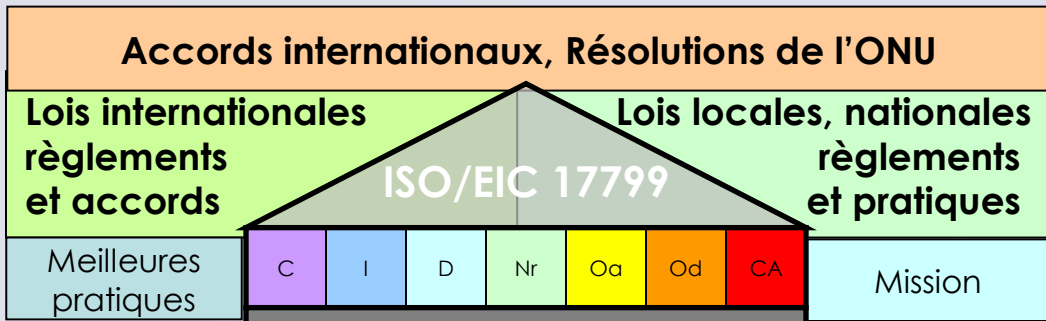


Interprétation des résultats

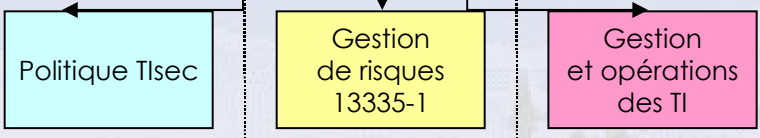


Présentation des résultats



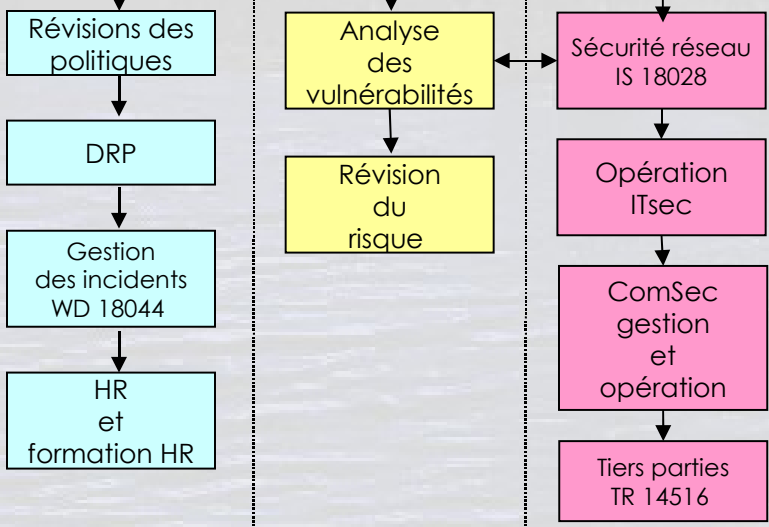


Sélection des Contrôles



Gestion de risques

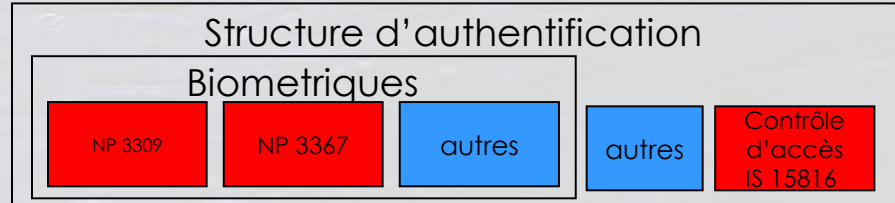
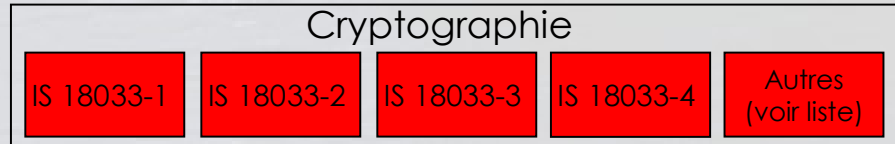
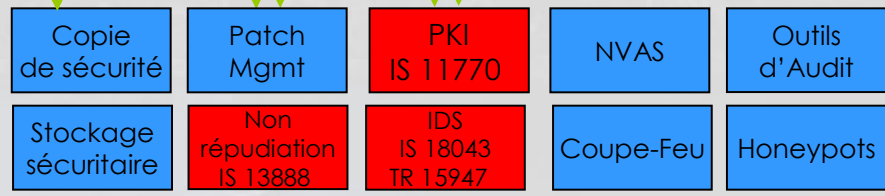
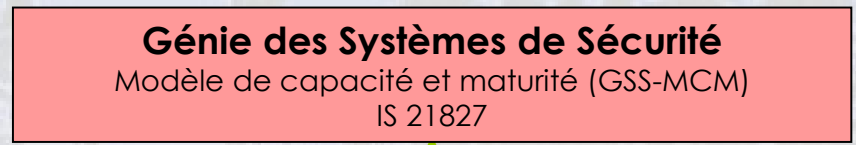
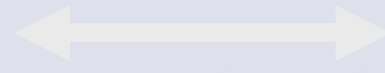
Méthodologie de gestion de risques



Normes organisationnelles

Normes en gestion de risques

Normes opérationnelles



Normes applicatives

Questions

marcandre@leger.ca