

Analyse de risque

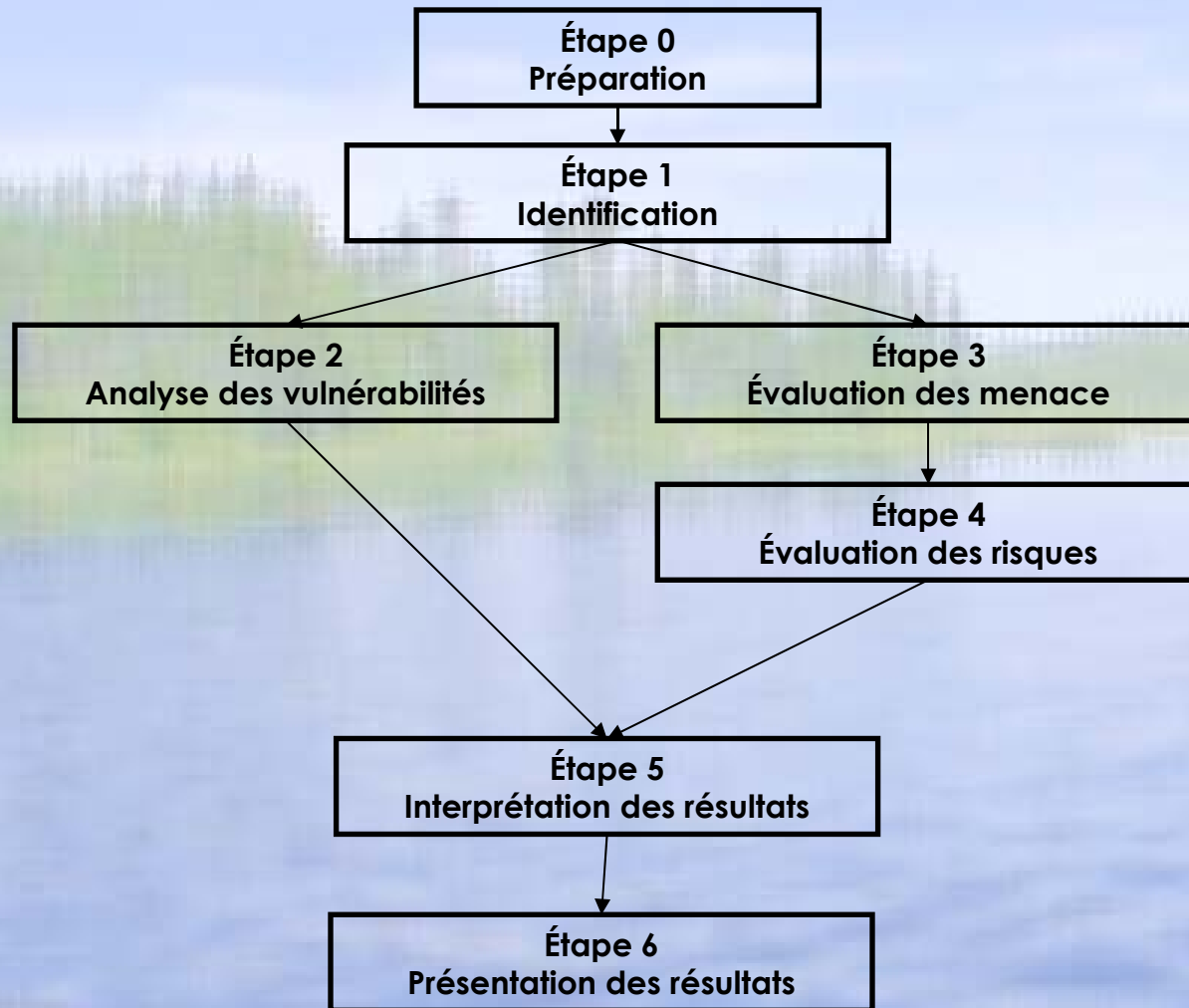


méthodologie **IVRI**tm

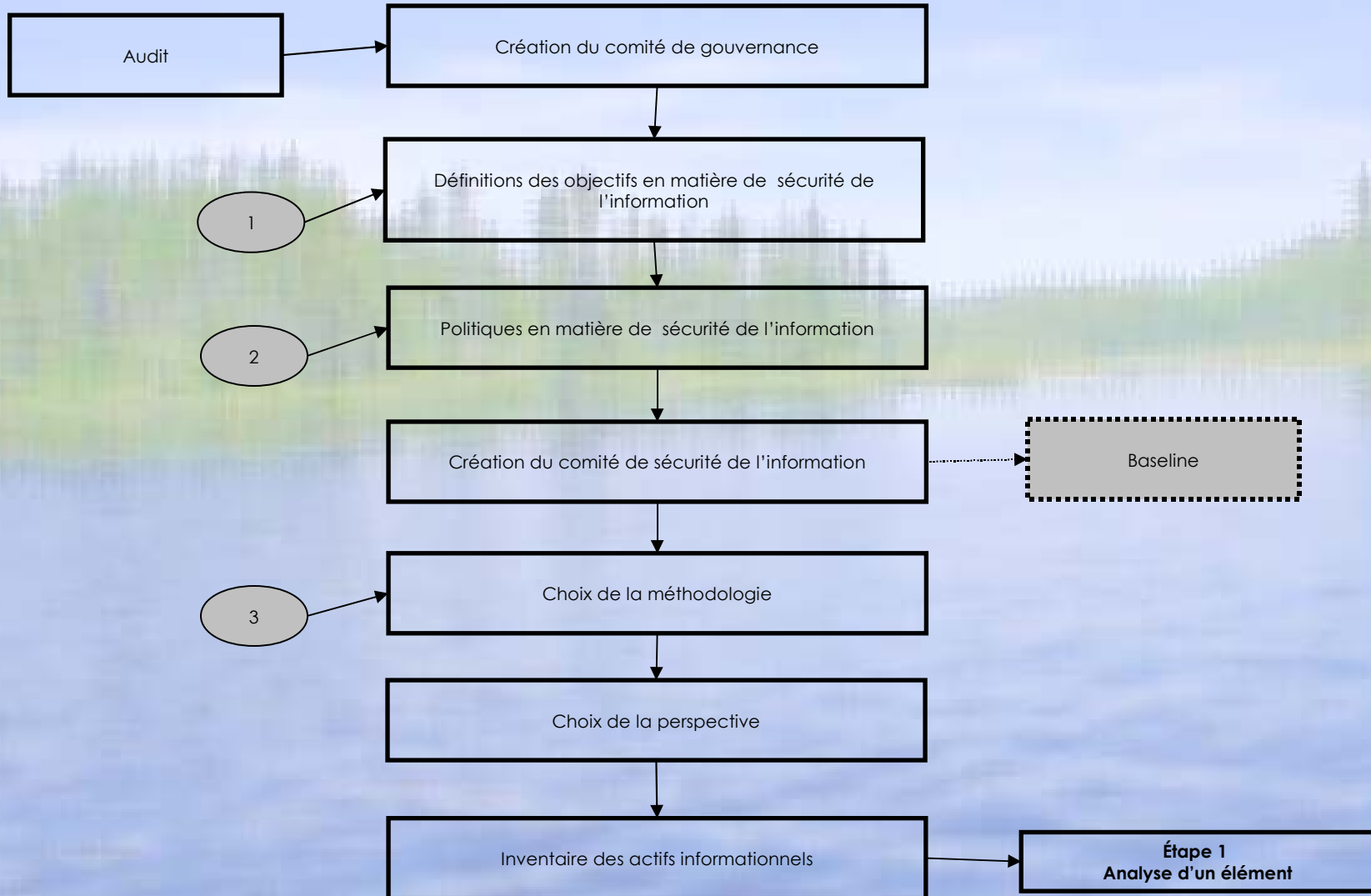
Méthodologie IVRI^{md} de gestion du risque en matière de sécurité de l'information

Par Marc-André Léger, MScA (MIS)

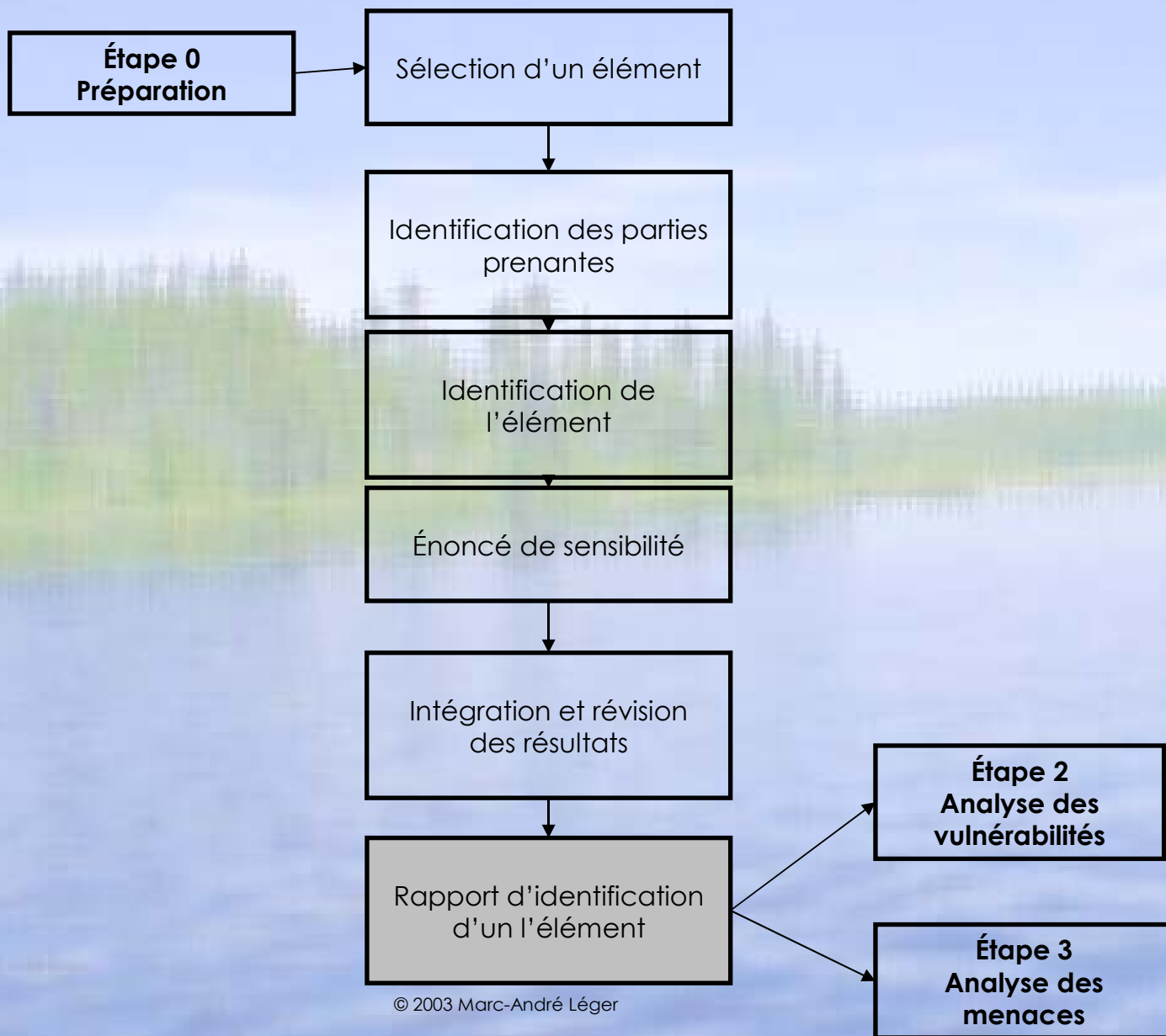
Méthodologie IVRI de gestion du risque



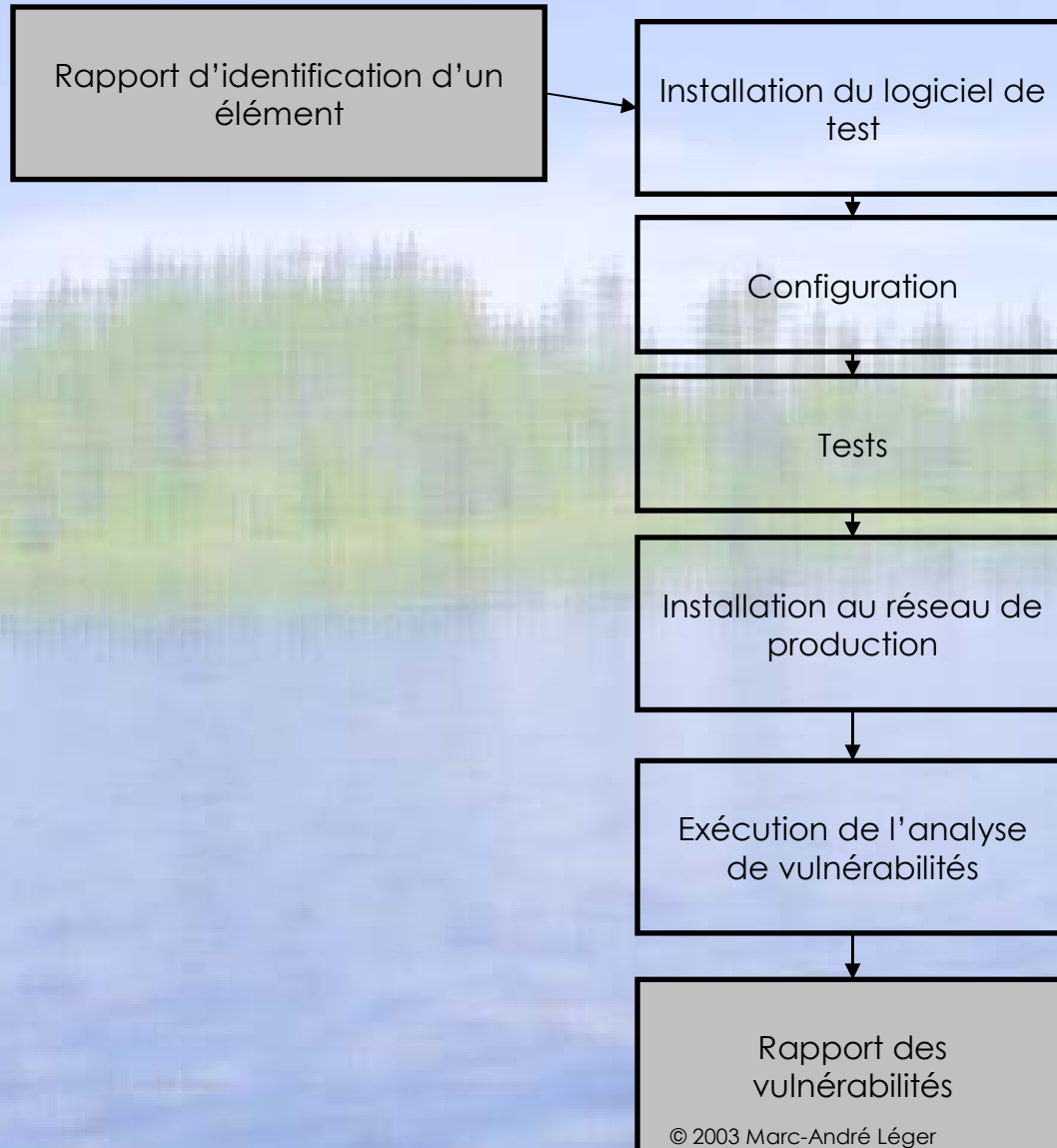
Préparation



Identification d'un élément



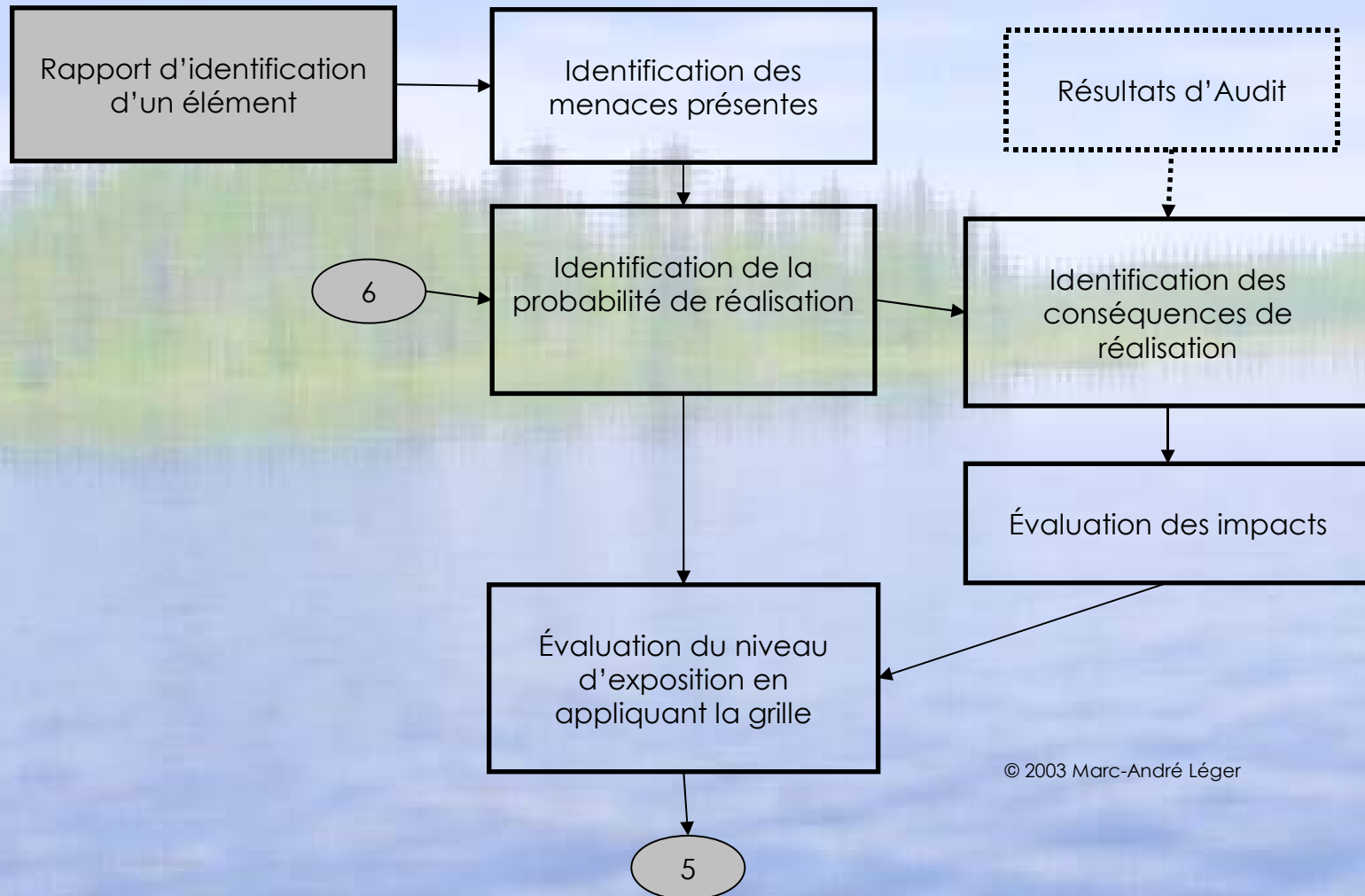
Analyse des vulnérabilités



Analyse du rapport de Nessus

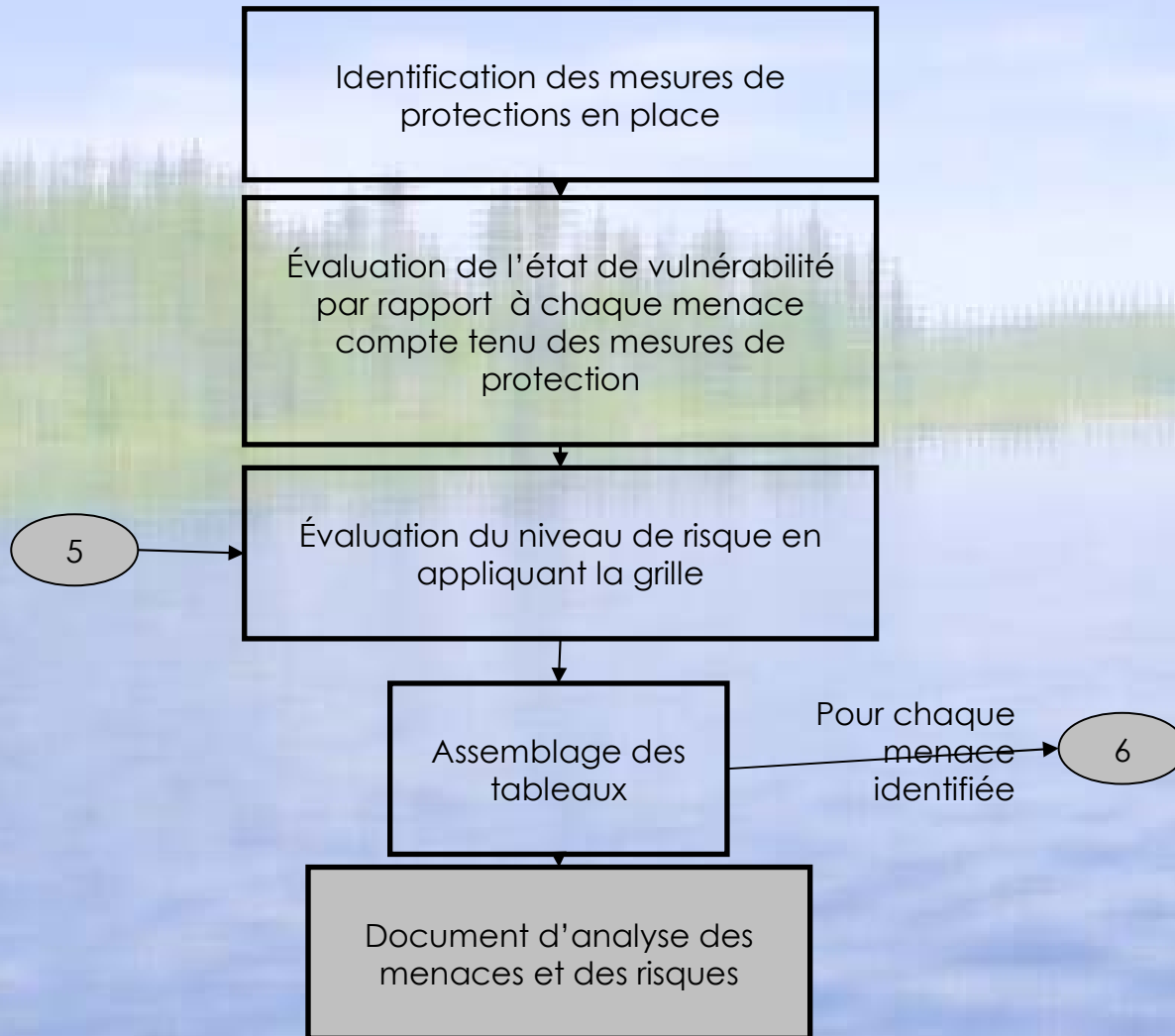
Vulnérabilité technologique	Commentaire(s) fdes praticiens	Action envisage
telnet (23/tcp)	Ce service est filtré de l'Internet au niveau du TCN; Il est accessible	Il est proposé de modifier les fichiers de configuration pour limiter les adresses IP ayant un accès ; Il est proposé de considérer la mise en place de OpenSSH
ftp (21/tcp)	L'accès FTP est nécessaire pour les mises à jour de pages sur le serveur Apache	Il est proposé de configurer des filtres (TCP Wrapper) afin de limiter les accès ; Il est proposé de considérer de remplacer FTP par un service OpenSSH
www (80/tcp)	Le problème associé au module mod_jk n'est pas une surprise; le module mod_jk fait le lien entre Apache et Jakarta ; des changements au module PHP serait difficile à faire ; le développement en PHP est fait par une firme de consultants externe (S2I) ; l'affichage de la version de Apache est volontaire afin de publiciser son usage par le TCR dans un but essentiellement pédagogique.	Il est proposé de considérer de mettre à jour le module mod_jk ;
sunrpc (111/tcp)	Ce service n'a pas d'utilité pour ce système; Il a été installé par défaut ;	Il est proposé d'enlever ce service sur le serveur ;
4600/tcp à 4625/tcp	Ce service est inconnu; Il s'agit possiblement des ports utilisés pour les branchements aux bases de données;	Il est propose de faire des recherches pour tenter d'identifier avec plus de certitude ce dont il s'agit ; L'utilisation de TCP Wrapper pourrait sécuriser ce port contre des attaques de type Man-in-the-middle
ajp13 (8009/tcp)	Ce service est utilisé par le module Tomcat	Ce service est nécessaire dans la configuration actuelle.
zeus-admin (9090/tcp)	Il s'agit du service d'indexation web	Ce service est nécessaire

Évaluation de la menace



© 2003 Marc-André Léger

Évaluation des risques



Évaluation qualitative

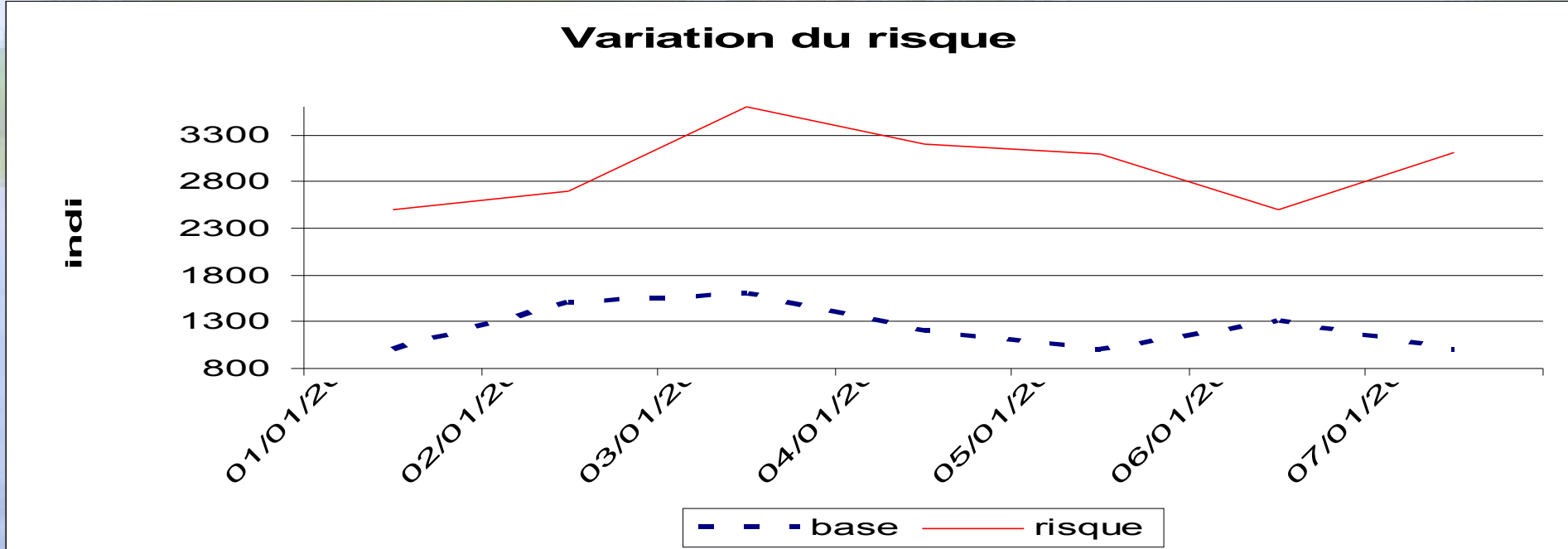
Menace			
Type de menace	Probabilité de réalisation	Impact	Niveau d'exposition
	Sans objet	Nul	Nul
	Faible	Moins grave	Faible
	Moyenne	Grave	Moyen
	Élevé	Très grave	Élevé
	Inconnu		Incomme
Risque			
Mesures de protection		État de vulnérabilité	Niveau de risque
		Sécurité excessive	Nul
		Équilibré	Faible
		vulnérabilité	Moyen
			Inconnu

Menace	Probabilité de réalisation	Impact	État de vulnérabilité
Bris accidentel	moyenne	grave	vulnérabilité
Panne accidentelle	moyenne	grave	vulnérabilité
Accident périphérique significatif	faible	grave	équilibre
Accident industriel	faible	très grave	équilibre
Incendie	moyenne	grave	vulnérabilité
Inondation	faible	grave	vulnérabilité
Tremblement de terre – séisme	faible	moins grave	équilibre
Tornade – Ouragan	faible	moins grave	équilibre
Panne de courant	élevée	moins grave	équilibre
Pointes de courant	élevée	moins grave	équilibre
Champs électromagnétiques	moyenne	moins grave	équilibre
Désastre environnemental	faible	moins grave	équilibre
Dommages collatéraux (Guerre)	faible	moins grave	équilibre
Vandalisme			
Vol	faible	grave	équilibre
Incendie	faible	grave	équilibre
Sabotage	faible	grave	équilibre
Guerre	faible	grave	équilibre
Activisme ou cyberactivisme	faible	grave	équilibre
Terrorisme ou cyberterrorisme	faible	grave	équilibre
Erreur			
Erreur de manipulation	moyenne	moins grave	équilibre
Erreur dans l'entrée des données	élevée	grave	équilibre
Erreur de programmation	moyenne	grave	équilibre
Erreur de configuration	moyenne	grave	équilibre
Erreur de gestion de la capacité	moyenne	moins grave	équilibre
Vulnérabilité universelle	élevée	grave	équilibre
La fraude économique			
Virement frauduleux	faible	moins grave	équilibre
Détournement de biens	faible	moins grave	équilibre
Espionnage industriel	faible	moins grave	vulnérabilité
Vol d'identité		grave	équilibre
Erreur volontaire dans l'entrée des données			

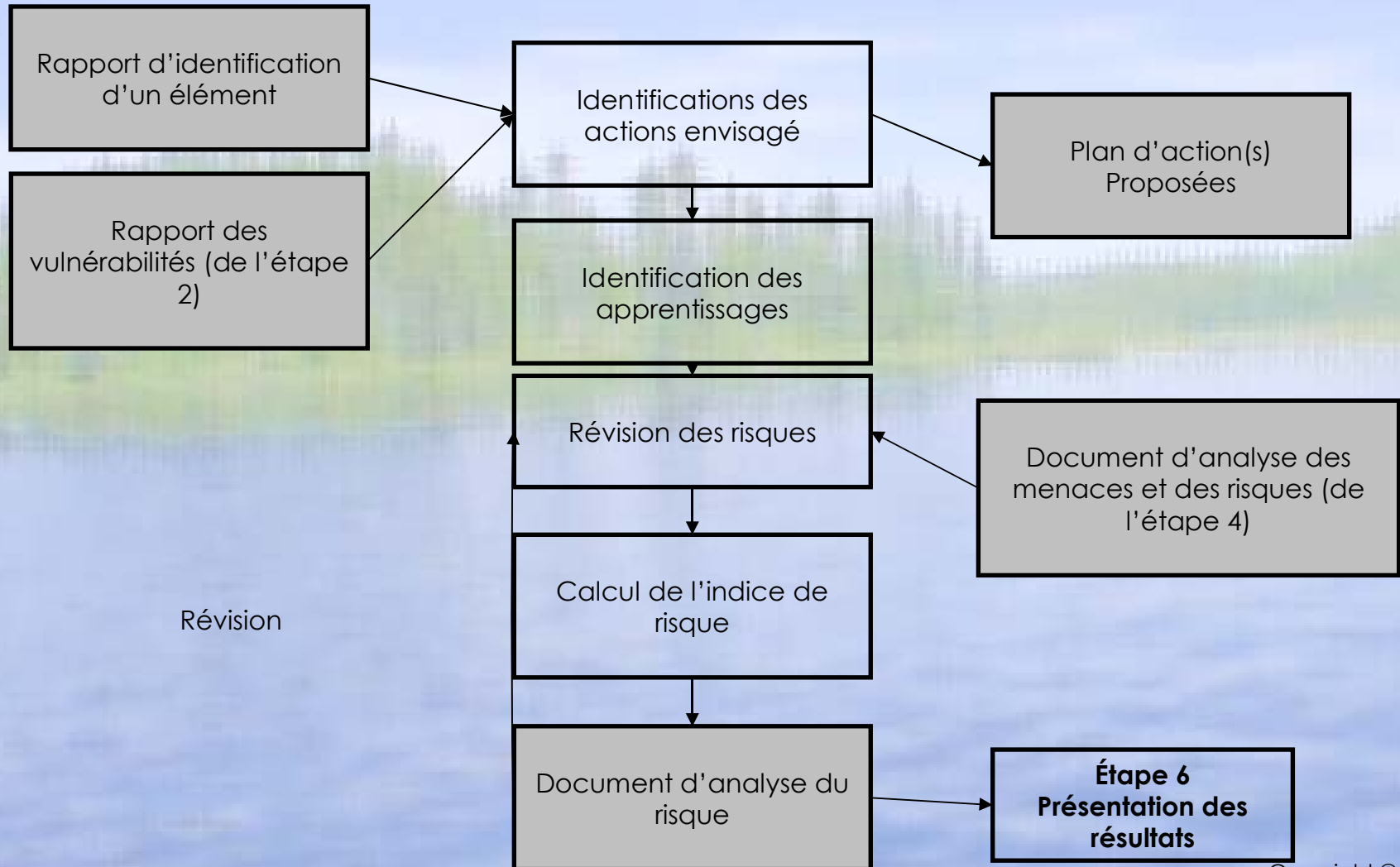
Tableau de bord

méthodologie
IVRI

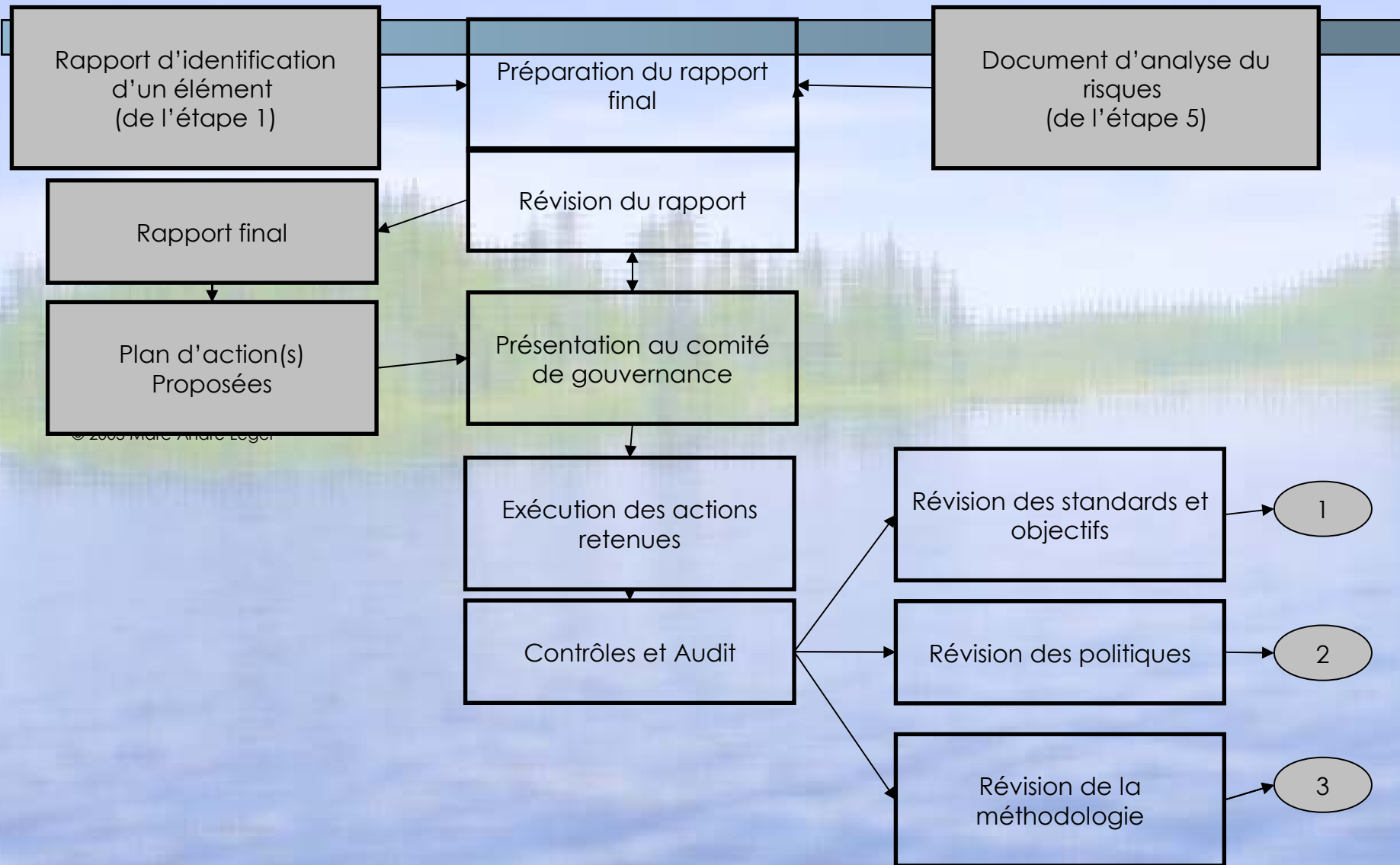
Indice de base : 1,005
Indice de risque : 3,115
Conformité IVRI-17799 : 89%

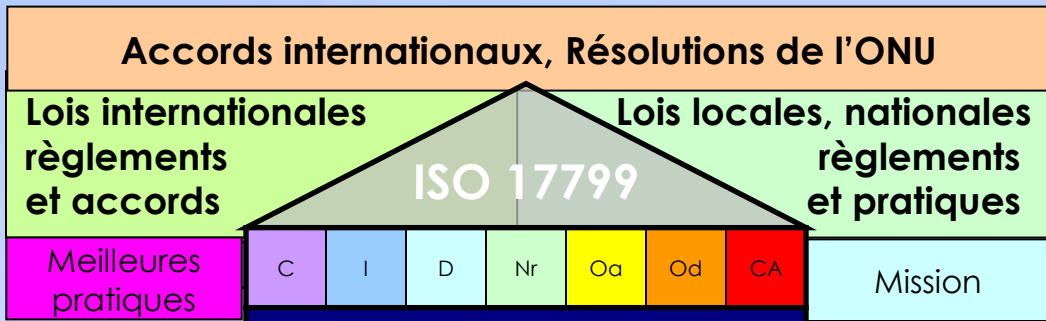


Interprétation des résultats

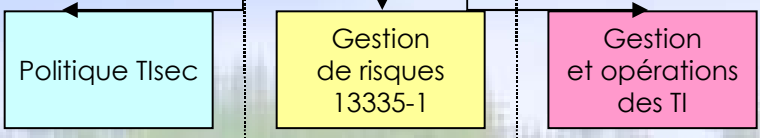


Présentation des résultats



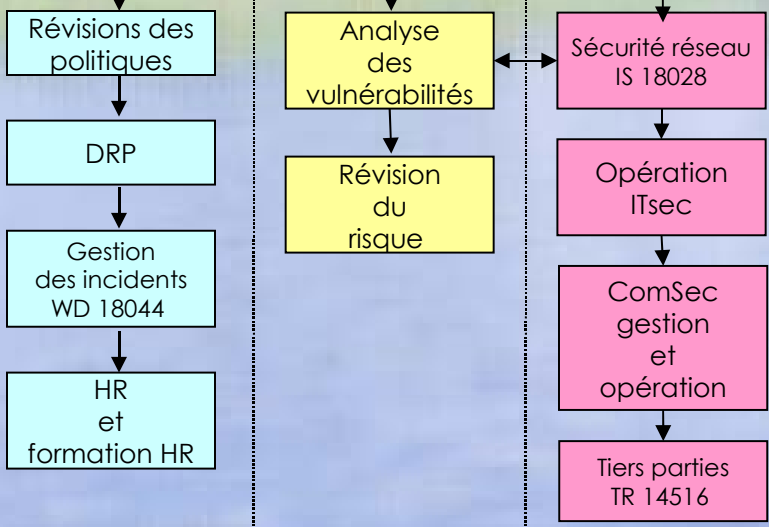


Sélection des Contrôles



Gestion de risques

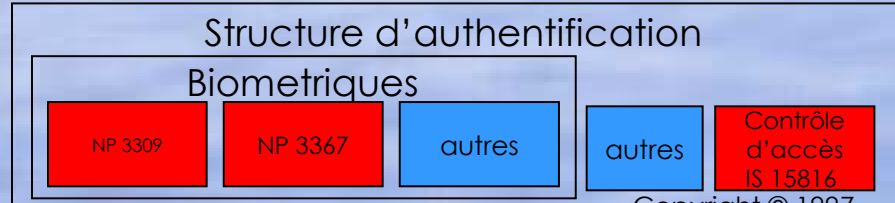
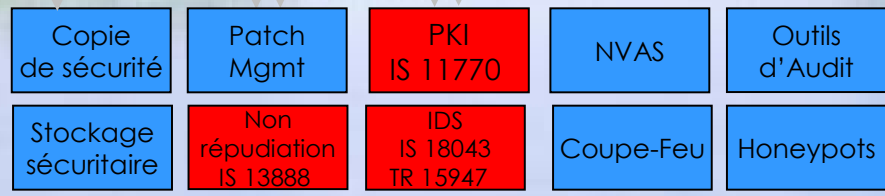
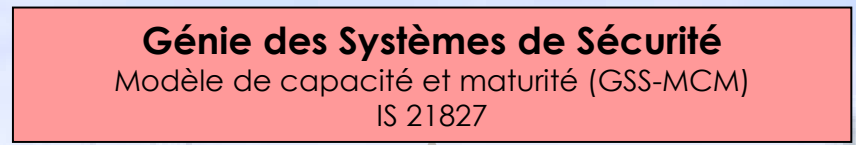
Méthodologie de gestion de risques



Normes organisationnelles

Normes en gestion de risques

Normes opérationnelles



Normes applicatives