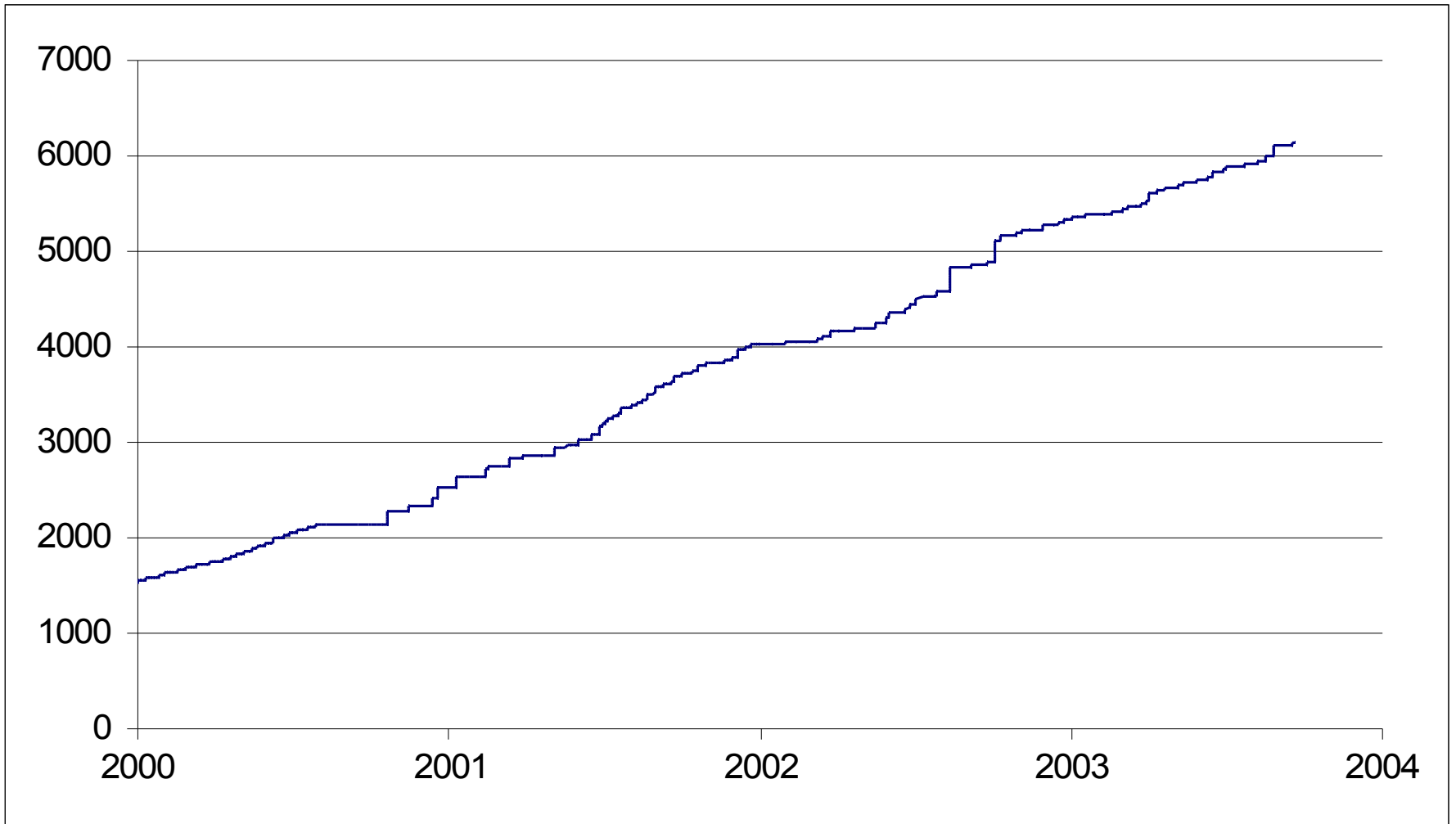


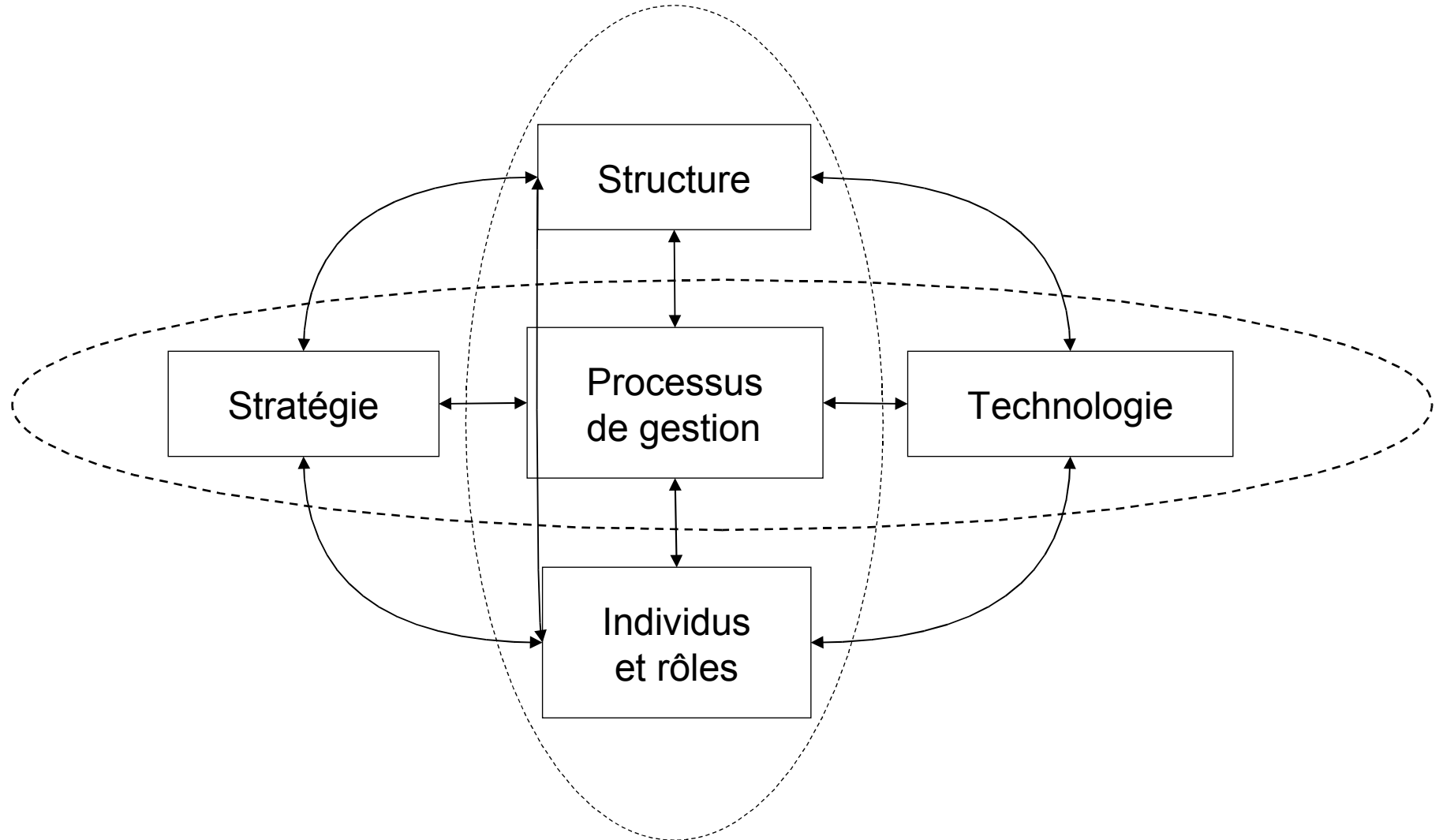


Identification
Vulnérabilités
Risques
Interprétation

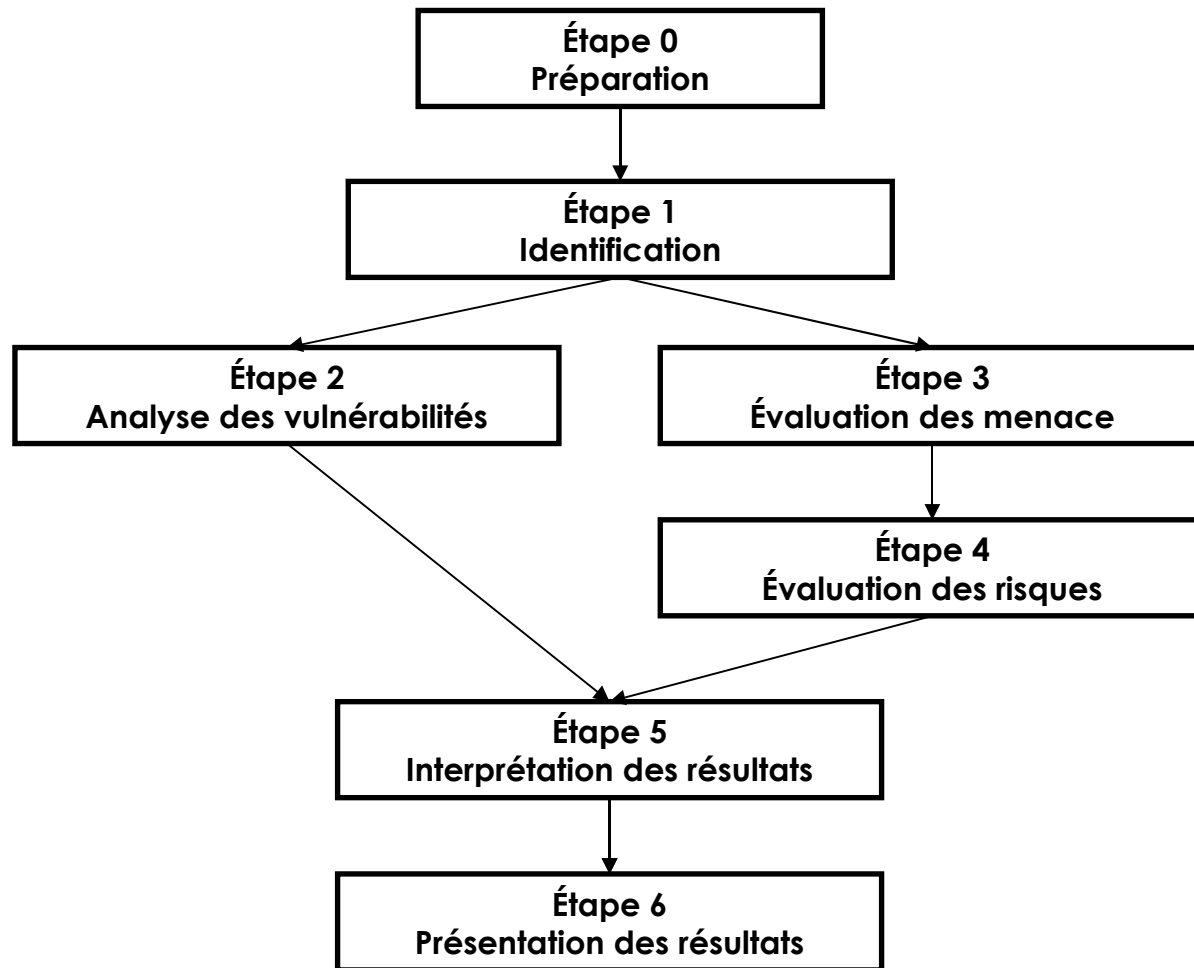
les vulnérabilités



Vision de l'organisation comme système organique pluricellulaire



Gestion du risque en matière de sécurité de l'information



Audit

NORMES GENERALES POUR L'AUDIT DES SYSTEMES D'INFORMATION

- **Responsabilité et autorité**
- **Indépendance professionnelle**
- **Rapport organisationnel**
- **Code d'éthique**
- **Conscience professionnelle**
- **Compétence et connaissances**
- **Planification d'un audit**
- **Supervision**
- **Éléments probants**
- **Rapport**
- **Activités de suivi**

Inventaire des actifs informationnels

- Serveurs;
- Postes de travail;
- Périphériques
- Équipement de télécommunications;
- Logiciels;
- Données.

Énoncé de sensibilité

but : évaluer l'actif et son rôle en vertu des besoins et obligations en relation aux principaux objectifs de la sécurité.

- la confidentialité des données;
- l'intégrité des données;
- la disponibilité des données;
- la non répudiation des transactions;
- l'authentification des utilisateurs;
- l'authentification de l'origine des données;
- le contrôle des accès.

Typologie des menaces

- Les menaces ont été classées en deux catégories principales :
- les menaces pouvant causer des dommages matériels; et
- les menaces causant des dommages immatériels.

Évaluation des menaces et des risques

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

Analyse du risque

Phénomènes accidentels	
Menace	Niveau de risque évalué
Bris accidentels	Certain
Panne accidentelle	Certain
Accident périphérique	Moyen
Incendie	Moyen
Inondation	Moyen
Panne de courant	Certain
Pointes de courant	Faible
Champs électromagnétiques	Faible

Vandalisme	
Menace	Niveau de risque évalué
Vol	Faible
Incendie	Faible
Sabotage	Faible
Guerre	Faible
Activisme	Faible
Terrorisme	Faible

Erreur	
Erreur de manipulation	Moyen
Erreur dans l'entrée des données	Faible
Erreur de programmation	Moyen
Erreur de configuration	Moyen
Erreur de gestion de la capacité	Faible
Vulnérabilité technologique	Moyen
Fraude	
Erreur volontaire dans l'entrée des données	Faible
Erreur volontaire de programmation	Faible
Cyber-crimes	
Menace	Niveau de risque évalué
Écoute (Keylogging)	Faible
Écoute réseau (Sniffer)	Faible
Virus Vers Cheval de Troie	Moyen
Attaques ciblées immédiates	Moyen
Attaques ciblée retardée	Moyen
Attaques ciblées distribuées	Moyen
Prise de contrôle	Faible
Cyber-squattage	Faible
Cyber-activisme	Faible
Cyber-terrorisme	Moyen

Qu'est-ce qu'un Network Vulnerability Assessment Software

- Logiciel client-serveur
- Balayage TCP-IP
- Base de signatures de vulnérabilités
- Générateur de rapports
- Interface utilisateur

Nessus

- Nessus est un détecteur de vulnérabilité
- développé par Renaud Deraison
- disponible sous une licence de type Open source.
- permet d'effectuer un balayage réseau pour identifier des vulnérabilités en relation à une base de signatures, un peu comme un progiciel anti-virus.
- identification de vulnérabilités directement attribuable à la présence d'une signature.

Service (port)	résultat
inconnu (4612/tcp)	Security notes found
inconnu (4611/tcp)	Security notes found
inconnu (4610/tcp)	Security notes found
inconnu (4609/tcp)	Security notes found
inconnu (4608/tcp)	Security notes found
inconnu (4607/tcp)	Security notes found
inconnu (4606/tcp)	Security notes found
inconnu (4605/tcp)	Security notes found
inconnu (4625/tcp)	Security notes found
inconnu (4624/tcp)	Security notes found
inconnu (4623/tcp)	Security notes found
ajp13 (8009/tcp)	No Information
zeus-admin (9090/tcp)	Security notes found
general/icmp	Security warning(s) found
general/tcp	Security notes found
sunrpc (111/udp)	Security notes found
ntp (123/udp)	Security warning(s) found
general/udp	Security notes found

Analyse du rapport de Nessus

Vulnérabilité technologique	Commentaire(s) des praticiens	Action envisagée
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 proposé 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

Tableau 22 : analyse du rapport de Nessus

Merci