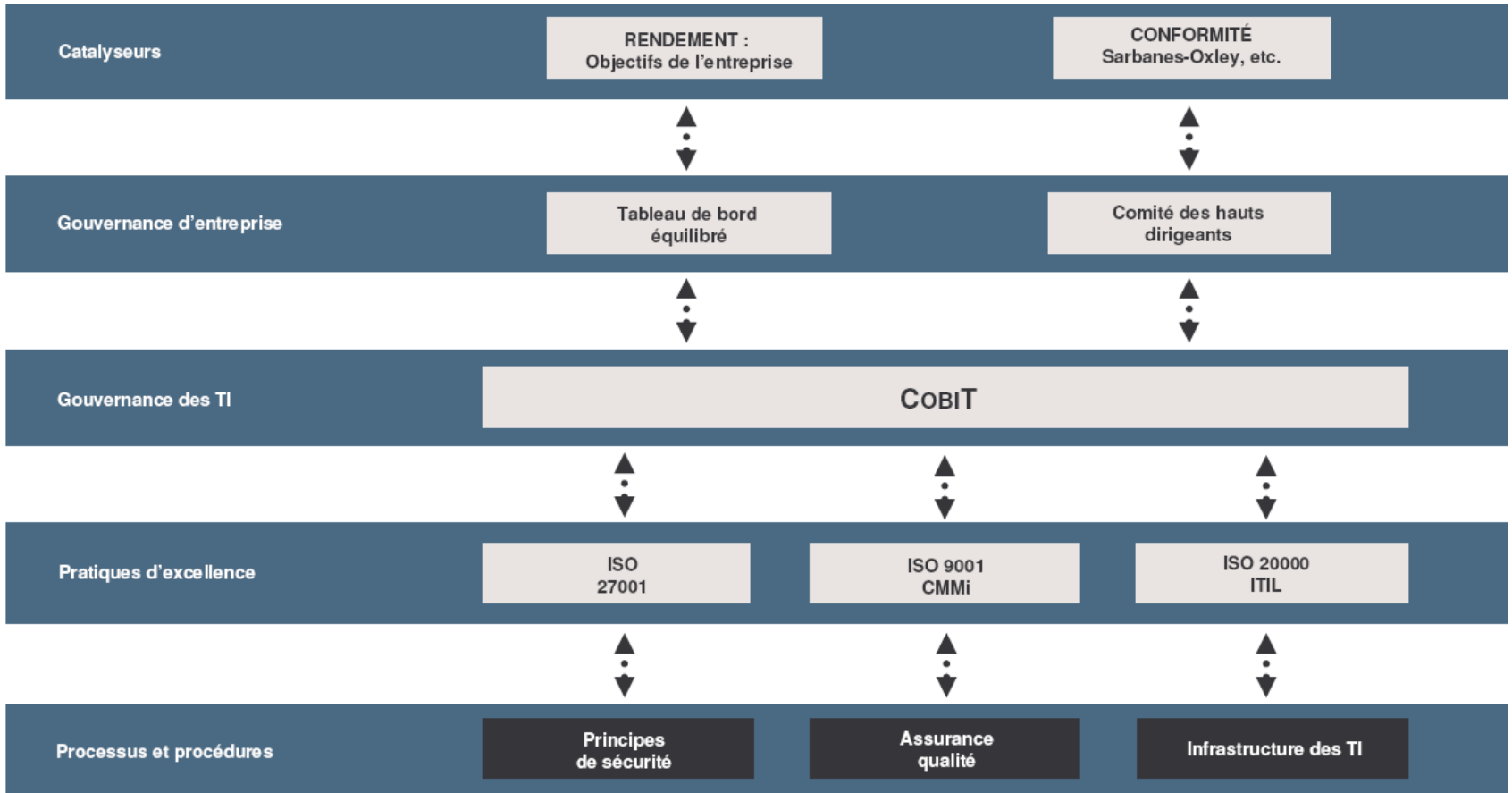




Gestion et automatisation de la conformité

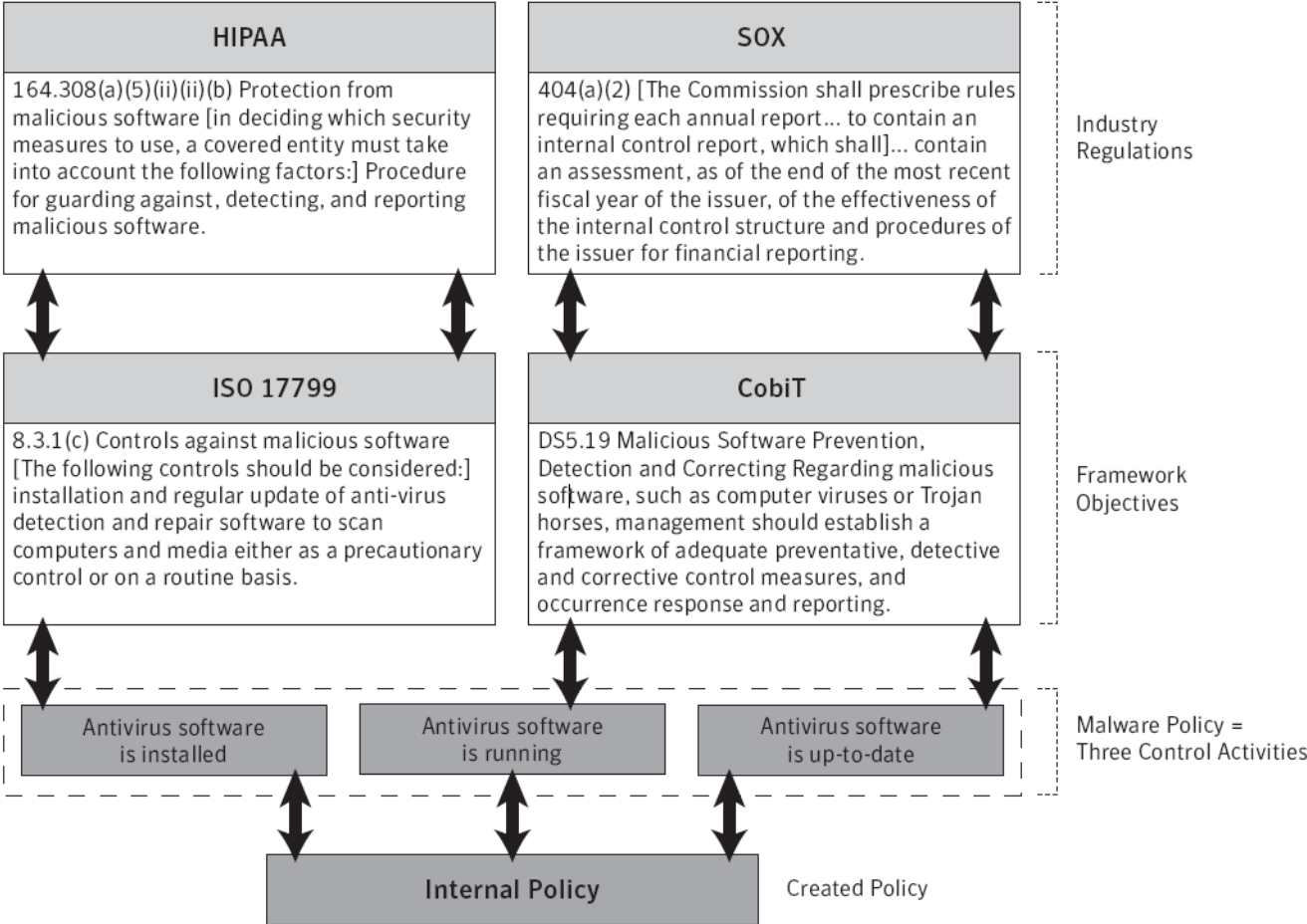
Par: Nicolas Bergevin

Structure haut niveau



©2007 IT Governance Institute

Exemple d'interrelations normatives



La conformité – Le contexte

Le besoin en conformité et gouvernance joue un rôle majeur dans les organisations modernes, que ce soit dans des initiatives d'assurance qualité telles que les standards ISO, une loi d'audit financier telle que Sarbanes-Oxley (SOX), ou bien l'implantation de meilleures pratiques de systèmes TI telles que ITIL® ou ISO, les compagnies dans le monde voient le besoin de gérer la conformité comme faisant partie intégrante de leurs activités **d'exploitation quotidiennes.**

La conformité – pourquoi?

Performance spectrum	Percentage of organizations	Number of IT compliance deficiencies to pass audit	Number of security events resulting in business disruptions	Number of unreported losses or thefts of sensitive data
Lagging firms	20%	26	17	22
Normative firms	67%	6	6	5
Leading firms	13%	2	2	2
Sample		1,779	1,269	694

Table 1. Compliance deficiencies, business disruptions, data losses, and thefts

Source: IT Policy Compliance Group, 2007

La conformité - Comment

- Adopter les meilleures pratiques:
 - Avoir de politiques complètes et déployées;
 - Avoir un modèle d'évaluation des risques;
 - Avoir des structures administrative efficaces (approbation);
 - Mettre en place les outils de gestion des politiques.
- Définir son environnement législatif/normatif:
 - L'organisation doit être en mesure de s'adapter à un environnement législatif/normatif toujours en constante mutation;
 - Mettre en place des outils d'automatisation qui supporte et intègrent l'ensemble des obligations (législatives/normatives) de l'organisation.

La conformité – Comment (suite)

- Mettre en place des contrôles pertinents en fonctions des risques identifiés:
 - Mettre en place un processus systématique et standardisé de sélection des contrôles technologiques et procéduraux;
 - Effectuer un suivi serré sur les dérogations;
 - Gestion des évidences;
- Obtenir une vue d'ensemble sur la situation:
 - Définition de métriques et de tableaux de bord;
- Effectuer une résolution efficace en cas d'incident

Gestion de la conformité

Définir

Déterminer le risque et développer des politiques

Politiques et contrôles



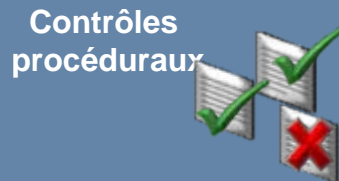
Évaluation de risques



Évaluer

Évaluer l'infrastructure et les processus

Évaluation des contrôles vs les configurations et le politiques



Surveiller

Surveiller et démontrer diligence

Tableaux de bord temps réel/temps donné



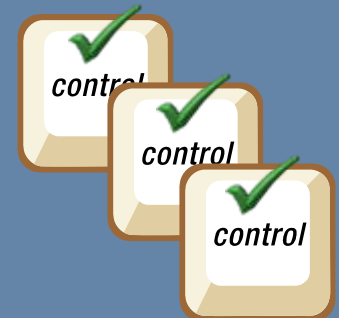
Gestion des audits, des vulnérabilités, de la configuration et des risques



Remédier

Évaluer les risques et résoudre les problèmes

Résolution basée sur le niveau de risque et réponse aux incidents



Les défis du maintien de la conformité

- Le volume de données à gérer et à analyser
- Établir les priorités;
- Maintenir l'expertise interne sur les différents besoins;
- Priorisé les activités de résolution
- Évaluer l'efficacité des ressources et des contrôles;
- Limiter le temps perdu dans les analyses manuelles;
- Éviter l'application inégale des politiques et des procédures.

L'automatisation de la conformité; pourquoi?

- Obtenir une meilleure visibilité sur les risques;
- Contrôler les coûts liés à la gestion et au maintien de la conformité;
- Mesurer l'efficacité des ressources et des contrôles de sécurité;
- Éviter la gestion de multiples outils et processus manuels;
- Assurer l'adhérence entre les multiples normes et standards.

Les bénéfices recherchés

Automatiser

Réduction des activités répétitives

- Définition, publication et gestion de politiques;
- Agrégation des évidences techniques et procédurales;
- Diffusion de l'information sur demande ou cédulée.

Intégrer

Mise à profit des ressources et processus en place

- Traitement et analyse de l'information en mode distribué;
- Association des politique TI et d'un cadre de contrôle;
- Rapprochement avec les systèmes de gestion d'actifs TI.

Prioriser

Transformer les évaluation en impact d'affaires

- Permettre la génération de rapports personnalisés;
- Gestion et décisions basées sur le niveau de risque;
- Résolution efficace et efficiente.

Questions