

Les visages
de la sécurité
Au-delà des apparences



Conférences
Expositions

RSi 2011

Rendez-vous de la **sécurité**
de **l'information**

RSi 2011

Rendez-vous de la **sécurité**
de **l'information**

Approches pratiques à la gouvernance de la sécurité des TI

Benoit Renaud, CISSP, PMP, P.Eng., ITIL v3



les visages
de la **sécurité**
Au-delà des apparences



Plan de la présentation

- Revue des problématiques actuelles de la sécurité des technologies de l'information (TI)
 - Défis de gestion de changement
 - Défis de conformité
 - Défis de gestion de risque
- Revue des cadres de gestion
- Pistes de solutions
 - Modèles de maturité
 - Feuille de route
 - Approche équilibrée (stratégique et tactique)
 - Gestion de risques
 - Importance de la communication



RSi

2011

Rendez-vous de la **sécurité**
de l'**information**

Statistiques inquiétantes ...

- **85%** des attaques n'étaient pas considérées comme hautement difficiles à réaliser
- **79%** des victimes n'avaient pas atteint la conformité
- **61%** des compromis ont été découverts par des tiers
- **96%** des violations auraient pu être prévenues par de simples contrôles

*2010 Data Breach Investigations Report



Les visages
de la sécurité
Au-delà des apparences



Défis de la gestion du changement

- Les organisations ont:
 - Une dépendance accrue envers les systèmes TI
 - Une dépendance accrue envers leurs fournisseurs et leurs systèmes TI (informatique dans les nuages)
 - Besoin de tirer avantage de leurs investissements en TI
- Vitesse des changements
- Peu d'organisations ont des stratégies qui facilitent le positionnement des TI dans l'atteinte des objectifs d'affaires



Défis de la conformité

- Nouvelles normes
- Audiences diverses et multiples
 - Comptables, TI, qualité, vérification interne, sécurité
- Cloisonnement dans l'organisation
- Dédoublément et spécificités
 - Multiples normes, réglementations, cadres, etc.
- Couverture toujours plus large
 - Vertical (nombre de contrôles)
 - Horizontal (applicabilités aux fonctions affaires)
- Effets cumulatifs des contrôles
- Manque de moyens



Défis de la gestion des risques

- Sécurité des TI et gestion de risques sont étroitement liés
- Positionnement dans l'organisation: Où ancrer la gestion de risques dans l'organisation?
 - Plus mature en TI / groupes opérationnels
 - Il n'y a pas de risques TI, que des risques d'affaires
- Importance de connaître l'ensemble des risques
 - Financiers, TI, Conformité,
- Communiquer les risques à tous les niveaux



Ces défis ont pour effets ...

- Dé-enlignement entre les efforts de sécurité et les besoins d'affaires
- Manque de soutien aux initiatives de sécurité
- Rôles ne sont pas clairs
- Responsabilités ne sont pas assignées
- Manquement au niveau de la communication
 - Rapports, risques, avancement, etc.

➡ Mauvaises surprises et conflits

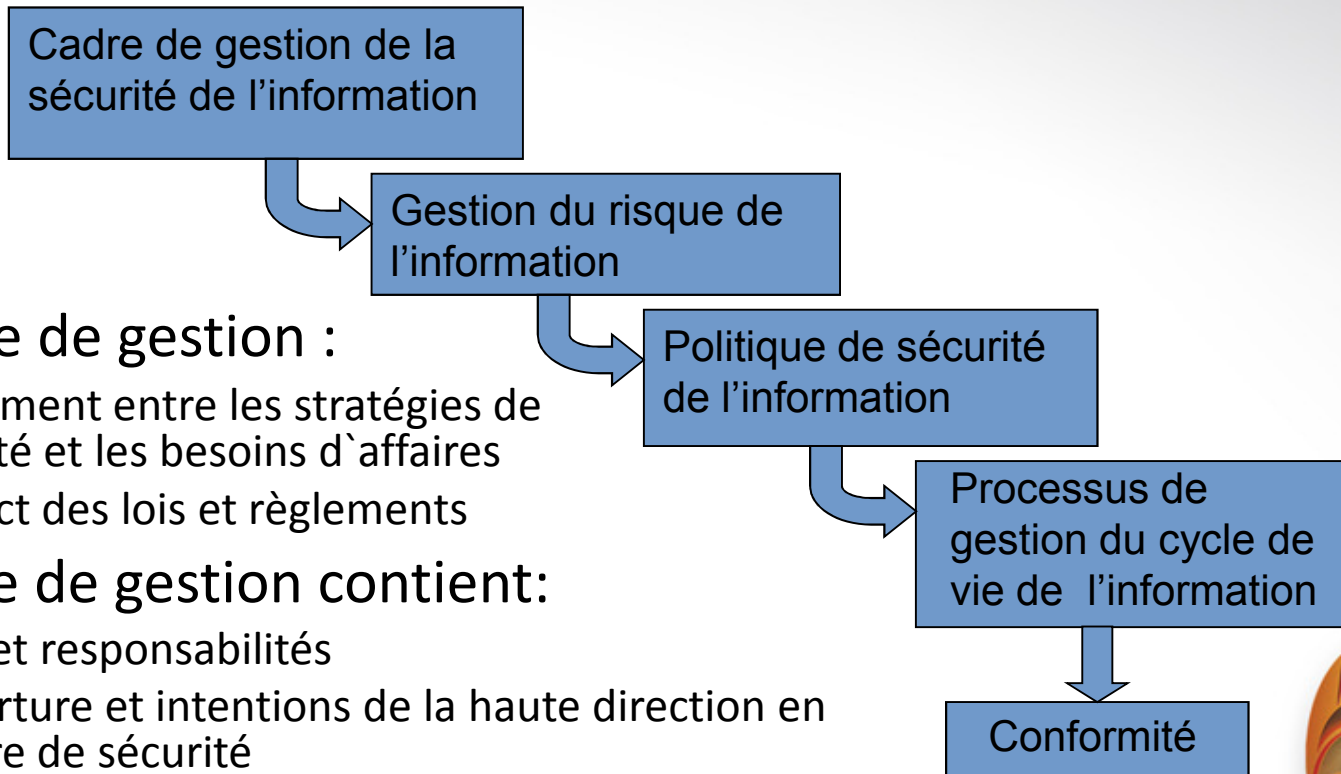
Définition de gouvernance

Le service informatique (et de sécurité) d'une entreprise n'est plus seulement fournisseur de services, mais en devient un acteur déterminant.

Le service informatique (et de sécurité) accompagne l'entreprise dans la formulation de sa stratégie d'affaires



Gouvernance Vue à 10,000 pieds



Le cadre de gestion :

- Alignement entre les stratégies de sécurité et les besoins d'affaires
- Respect des lois et règlements

Le cadre de gestion contient:

- Rôles et responsabilités
- Couverture et intentions de la haute direction en matière de sécurité
- Exigences en matières de communications et de production de rapports



Importance de la conformité aux yeux du Chef de la direction

Business expectations for IT call for greater productivity and continued cost-efficiencies

Business expectations

Ranking of business priorities CIOs selected as one of their top 5 priorities in 2010, and projected for 2013

Ranking	2010		2009	2008	2007	2013
Improving business processes	1	↔	1	1	1	2
Reducing enterprise costs	2	↔	2	5	2	8
Increasing the use of information/analytics	3	↑	5	8	7	5
Improving enterprise workforce effectiveness	4	↓	3	6	4	7
Attracting and retaining new customers	5	↓	4	2	3	3
Managing change initiatives	6	↑	8	3	10	1
Creating new products or services (innovation)	7	↓	6	12	*	12
Targeting customers and markets more effectively	8	↓	7	9	*	9
Consolidating business operations	9	↑	11	13	*	16
Expanding current customer relationships	10	↓	9	7	*	10
Supporting regulation, reporting and compliance	11	↑	12	14	13	15
Creating new sources of competitive advantage	12	↑	13	11	8	4
Expanding into new markets and geographies	13	↓	10	4	*	6



Source: Gartner 2010

Survol des cadres de gestion

- **ISO/IEC 27001 and 27002** : 2005 - International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)
- **COBIT** (Control Objectives for Information and related Technology) v4.2 (v5 en ébauche) – Information System Audit & Control Association (ISACA)
 - Risk IT, Val IT, ITAF (IT Assurance Framework)
- **ITIL ITSM** (Information Technology Infrastructure Library - IT Service Management Framework) v3 – Office of Government Commerce (OGC)
- **CMMI** (Capability Maturity Model Integration) v1.2 - Software Engineering Institute (SEI)
- **PMBok, Prince 2** – Gestion de programme, projets
- **COSO** - Committee of Sponsoring Organizations of the Treadway Commission
- **ISO 31000** – Gestion des risques
- **Normes de l'industrie: SoX, PCI DSS, FISMA, PIPEDA, HIPAA**
- **Qualité - ISO 9000, SixSigma, TQM**



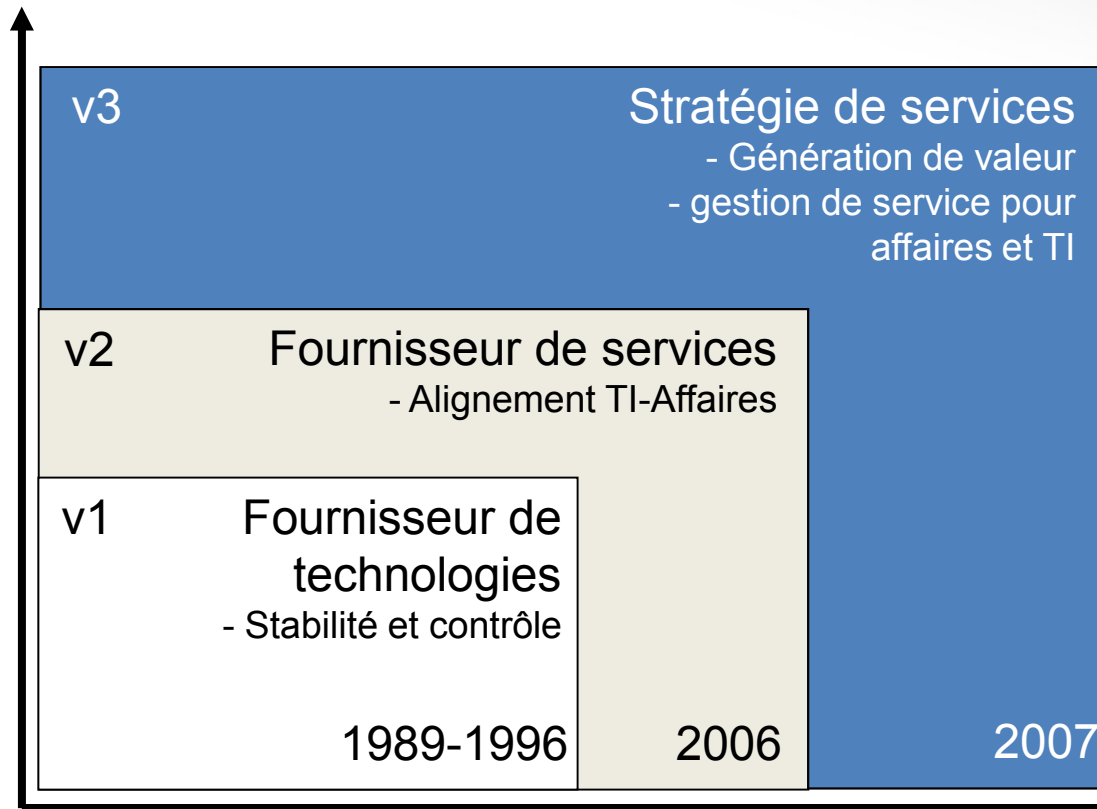
ISO 27001 / 27002

- **ISO 27001:2005** - Exigences d'un système de pilotage de la sécurité des informations
 - Basé sur le dernier standard BS 7799 Part 2 de 2002
 - Base des règles de certification ISO 27000
- **ISO 27002:2005** - Code des bonnes pratiques décrivant un ensemble cohérent d'objectifs de contrôles de la sécurité.

- **ISO 27003** : 2010 - Guide de mise en œuvre pour l'implantation du SMSI.
- **ISO 27004** : 2009 - Base de métriques de sécurité et d'indicateurs de pilotage
- **ISO 27005** : 2008 - Gestion des risques
- **ISO 27006** : 2007 - Exigences pour les organismes procédant à l'audit
- **ISO 27007** - Instructions pour les audits accrédités
- **ISO 27014** - Cadre de gestion de la sécurité de l'information



Évolution de ITIL



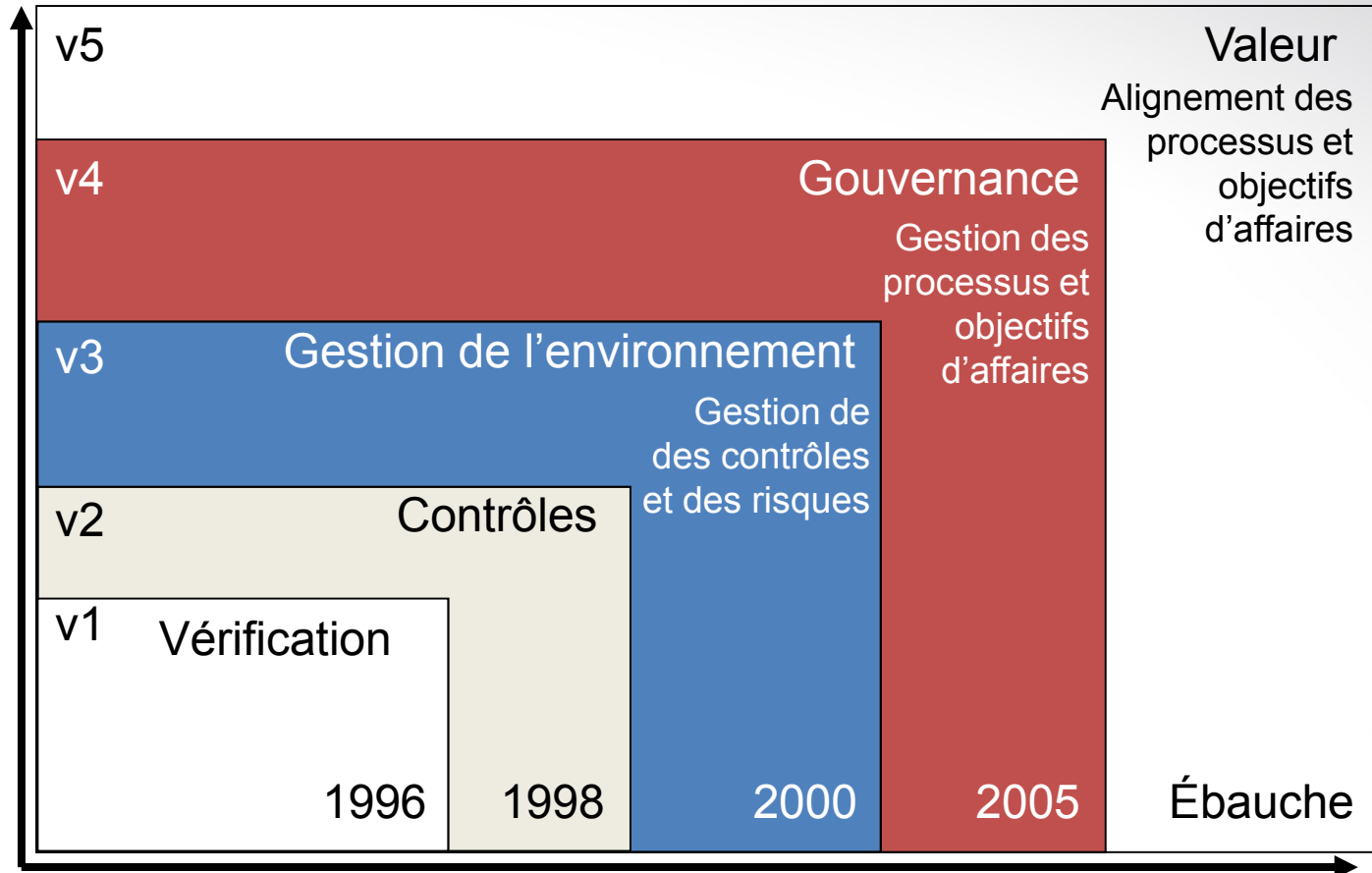
Positionner la sécurité comme un 'facilitateur'



Soutenir le respect des exigences en matière de sécurité



Évolution de COBIT



COBIT[®] version 4

- Cadre de gestion
 - 4 domaines
 - 34 processus
 - Liste des contrôles
 - Quoi faire et non comment le faire
- Outils
 - Équipe de gestion
 - Équipe des TI
 - Vérificateurs
- Forces
 - Public, orienté–affaires
 - Incorpore les meilleures pratiques
 - Modèle de mesure de la performance et maturité
 - Liens avec ISO/IEC 27002, ITIL, CMMI

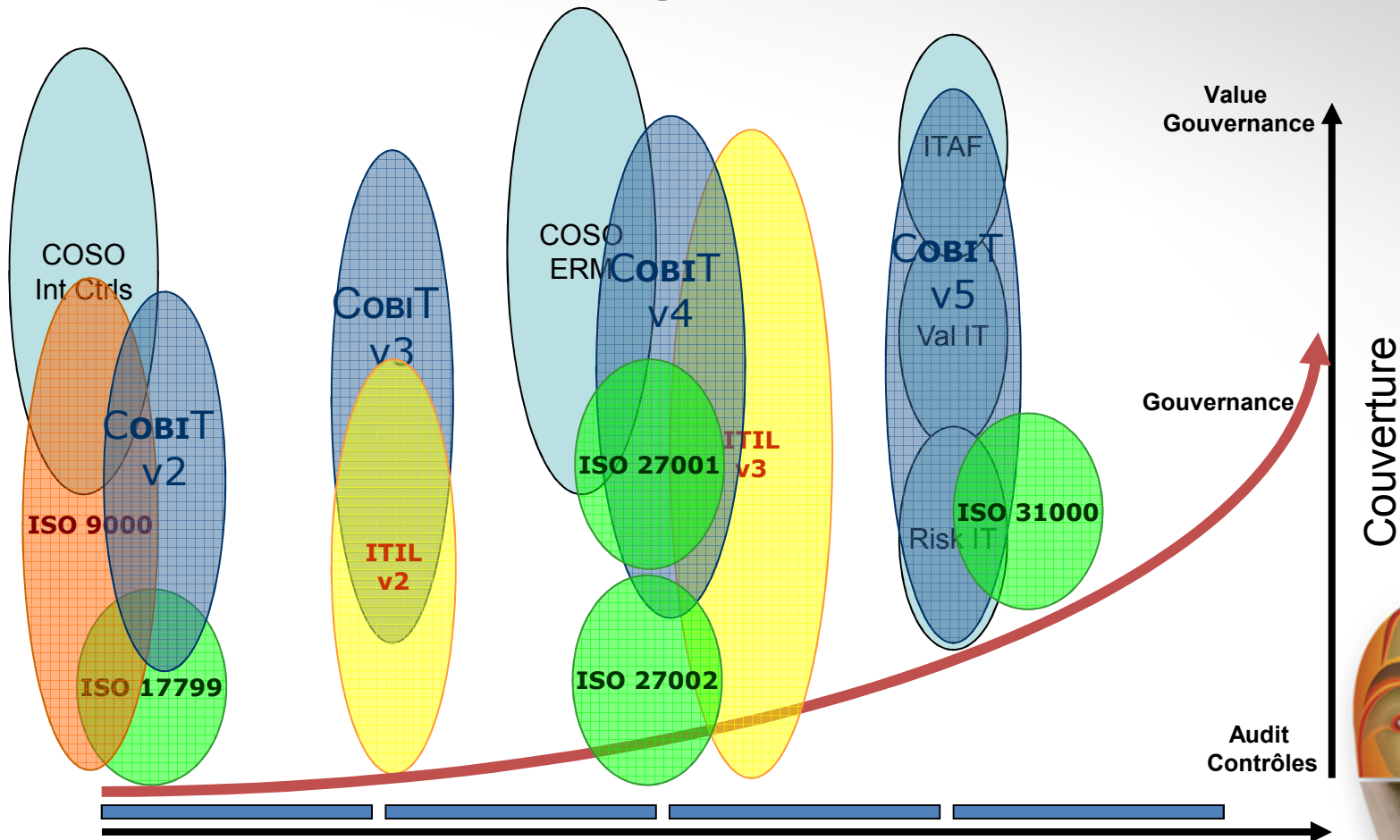


COBIT® version 5

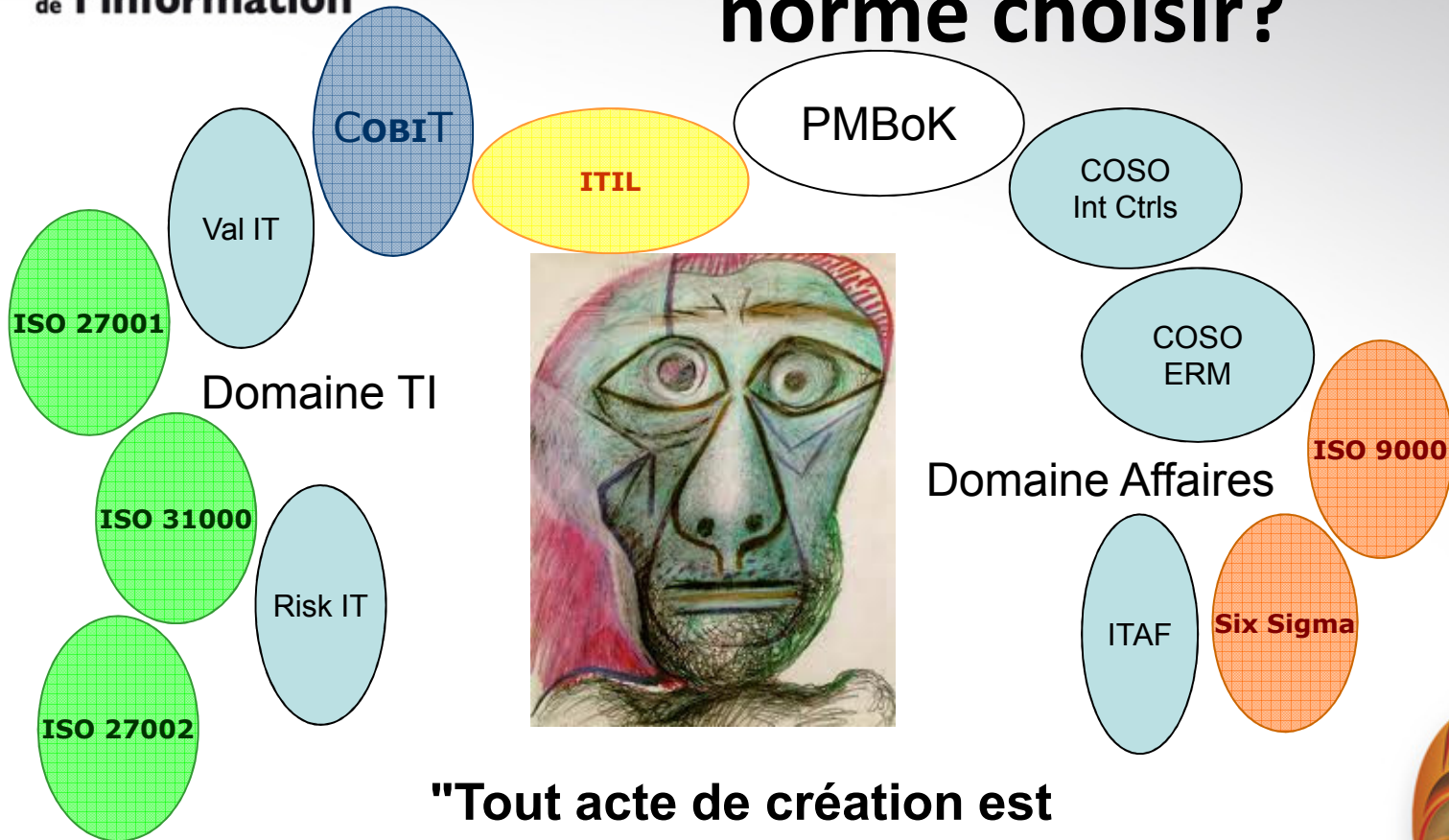
- Renforce les liens entre tous les cadres d'ISACA :
 - IT Assurance Framework™ (ITAF™)
 - *Risk IT Framework*
 - *Val IT™ Framework*
 - Business Model for Information Security™ (BMIS™)
 - *Board Briefing on IT Governance, 2nd Edition*
- Établit aussi des liens vers d'autres cadres de gestion et normes (ITIL, ISO standards, etc.)
- Ajout des préoccupations tel que développement durable



Évolution des cadres de gestion et normes



Quelle méthodologie ou norme choisir?



**"Tout acte de création est
d'abord un acte de destruction."**

Pablo Picasso



Outils de mappage

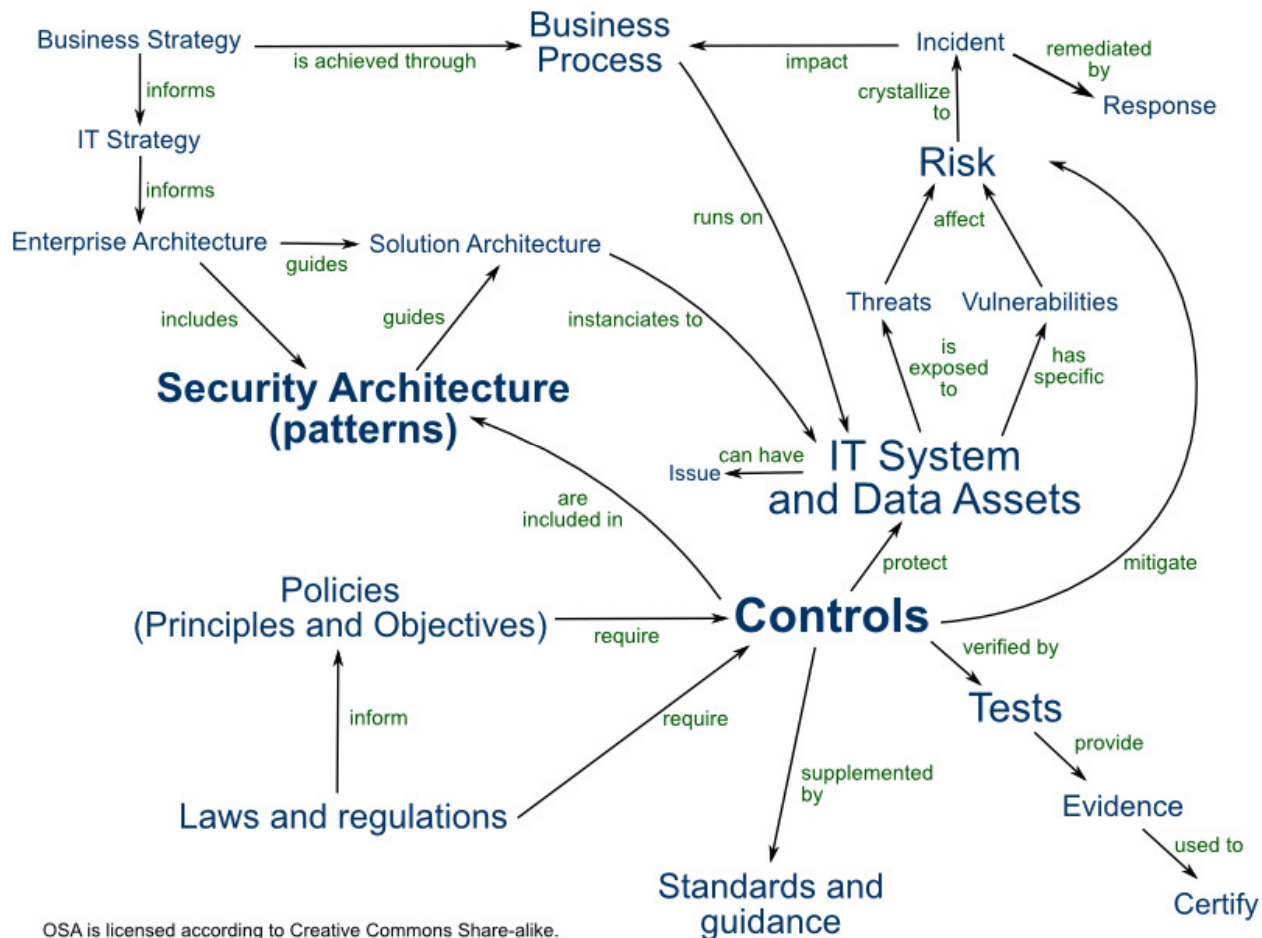
CobiT 4.1 Domain: Plan and Organise (PO) (cont.)			
PO4 Define the IT Processes, Organisation and Relationships (cont.)			
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO4.6 Establishment of roles and responsibilities	<ul style="list-style-type: none"> • Explicit roles and responsibilities • Clear accountabilities and end-user authorities 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SD 6.2 Activity analysis • SD 6.4 Roles and responsibilities • ST 6.3 Organisation models to support service transition • SO 6.6 Service operation roles and responsibilities • CSI 6 Organising for continual service improvement 	<ul style="list-style-type: none"> • 6.1.2 Information security co-ordination • 6.1.3 Allocation of information security responsibilities • 6.1.5 Confidentiality agreements • 8.1.1 Roles and responsibilities • 8.1.2 Screening • 8.1.3 Terms and conditions of employment • 8.2.2 Information security awareness, education and training • 15.1.4 Data protection and privacy of personal information
PO4.7 Responsibility for IT quality assurance (QA)	<ul style="list-style-type: none"> • Responsibility, expertise and placement of QA according to organisational requirements 	<ul style="list-style-type: none"> • CSI 6 Organising for continual service improvement 	

Sécurité des TI ➡ TI ➡ Affaires

Source: Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit



Par où débiter?



OSA is licensed according to Creative Commons Share-alike.
Please see: <http://www.opensecurityarchitecture.org/cms/about/license-terms>.



les visages
de la sécurité

Au-delà des apparences



RSi 2011

Rendez-vous de la **sécurité**
de **l'information**

Pistes de solutions



les visages
de la sécurité
Au-delà des apparences



Modèles de maturité

- ISO 27001
 - PDCA (cycle de Deming)
- COBIT
 - Définition des exigences par niveau de maturité
 - Permet de mesurer la performance
 - En assigner la responsabilité
 - Référenciation aux meilleures pratiques
 - Identifier les écarts
 - Dérivés des niveaux de maturité du SEI CMM
- Val IT
 - Mappage avec les niveaux de maturité de COBIT
- CMMI
 - Mappage avec les niveaux de maturité de COBIT
- ISM3
 - Liens établis avec COBIT
- Forrester
 - 4 domaines, 25 fonctions, 123 composants
 - Combine COSO, COBIT



Modèle de maturité de COBIT



 : Situation actuelle

 : Comparable de l'industrie

 : Cible

0 : processus non appliqués

1 : processus ad hoc ou désorganisés

2 : processus répétables

3 : processus documentés et communiqués

4 : processus surveillés et mesurés

5 : pratiques appliquées et automatisées

Appliquer par cycle PDCA (ISO 27001):

- Processus et contrôles de sécurité
- Indicateurs clés du risque (KRIs)
 - Nouvelle métrique
 - Nouvelle cible
- En fonction de l'analyse de risques

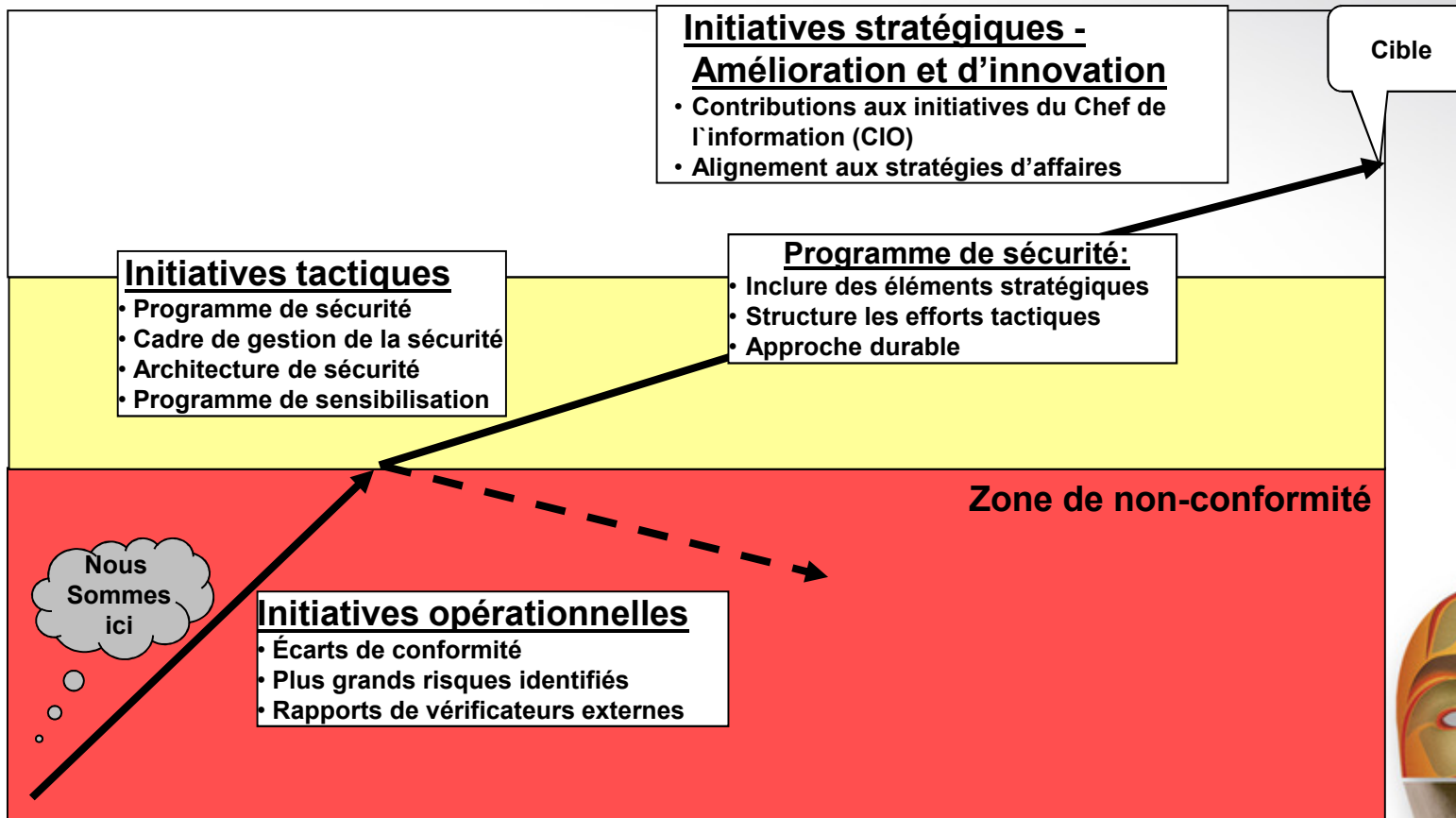


Étapes d'implantation

- Évaluations du niveau actuel de maturité
- Analyse d'écart
- Sélection des métriques
- Priorisation des projets
- Documentation
- Implantation des projets
- Évaluation
- Itération



Sécurité et maturité: Feuille de route



Meilleures pratiques et Innovation

TI Tactique

Activités journalières pour
garder l'organisation à flot:

- Gestion de projets
- Gestion des journaux

Meilleures pratiques:

- CMMI
- ITIL
- ISO 27001
- Six Sigma

*Mieux faire que
vos rivaux*

TI Stratégique

Fonctions stratégiques qui
valorisent l'organisation:

- Gestion de programme
- Gestion de la fraude

Meilleures pratiques:

- Val IT
- Gestion de risque d'entreprise

*Faire de meilleures
activités que vos rivaux*



Plan de réalisation des bénéfécies

Project / Initiatives	Activity Type	Business Value										Risk Value					Financial Value				Business Value	Risk Value	Financial Value	Total Value	PDCA phase	Strategic Tactical Operational	Fiscal Year
		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	1	2	3	4							
Politique 1 (Analyse Écarts)	Projet de sécurité	4	3	5	5	2	3	1	1	5	5	4	1	1	1	1	1	3	5	1	24	15	13	52	Tactical	2011	
Politique 2 (Analyse Écarts)	Projet de sécurité	5	3	5	5	2	3	1	1	5	5	4	1	1	1	1	1	3	4	1	25	15	12	52	Tactical	2011	
Définition politique 3	Projet de									5	4	5	1	1	1	1	1	1	4	1	24	15	10	49	Strategic	2011	
Amélioration du Cadre de gestion	Projet de									3	1	5	2	1	1	1	1	2	4	1	26	11	11	48	Plan	Strategic	2011
Solution 1	Projet de									5	3	4	1	1	1	1	1	1	4	1	23	13	10	46	Tactical	2011	
Solution 2	Projet de									4	5	4	3	1	1	1	1	1	1	1	19	16	7	42	Tactical	2011	
Architecture de sécurité	Projet de sécurité	2	2	2	4	4	3	1	1	4	3	5	2	1	1	1	1	1	2	1	19	14	8	41	Strategic	2011	
Amélioration du site de sécurité	Projet de sécurité	2	2	2	3	3	4										2	1	1	20	7	8	35	Tactical	2011		
Politique 5 définition	Projet de sécurité	3	2	2	3	1	5										1	1	1	18	7	7	32	Strategic	2012		
Projet classification des actifs	Projet de sécurité	3	1	1	3	2	3										1	3	1	15	7	9	31	Strategic	2011		
Définition de la norme 8	Projet de sécurité	3	2	1	3	1	5										1	1	1	17	8	7	20	Tactical	2012		
Évaluation de risques	Projet de sécurité	3	1	1	3	2	3																	Strategic	2011		
Solution 3	Contribution	1	1	1	2	2	1	1	3	3	3	1	1	1	1	1	1	1	1					Operational	2011		
Solution 4	Contribution	1	1	1	1	2	1	1	3	2	3	2	1	1	1	1	1	1					Operational	2011			
Solution 5	Contribution	1	1	1	1	2	2	1	3	1	3	3	1	1	1	1	1	1					Operational	2011			

Valeur Affaires

Valeur Risque

Valeur Financière

Valeur:
+ Affaires, - Risques, + Financière



Approche Itérative

- Basée sur un plan de réalisation des bénéfices
 - Établit l'alignement avec les priorités d'affaires et de sécurité
 - Tient compte
 - Cycle de planification et budgétisation de l'entreprise
 - Dépendances entre les projets et initiatives
- Basée sur un modèle de maturité
 - Permet de mesurer, rapporter l'avancement
 - Influence la sélection et l'évolution des métriques de sécurité
- Basée sur des analyses de risques
 - Influence le choix des projets, initiatives, processus, contrôles



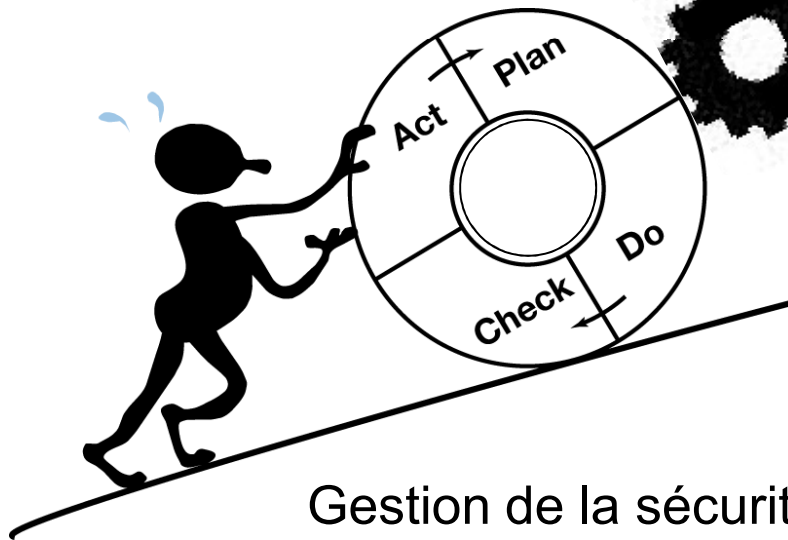
RSi 2011

Rendez-vous de la **sécurité**
de l'**information**

... et intégrée

Affaires

Gestion du Risque



Gestion des TI

Gestion de la sécurité



les visages
de la sécurité
Au-delà des apparences



Gestion de risques

- Intransigent important au plan de réalisation des bénéfices
- Adopter une approche de gestion de risque top-down
 - La gestion des risques d'entreprise (et non simplement les risques TI)
 - Risques stratégiques, environnementaux, des marchés, de crédit, opérationnels, de conformité.
 - S'appuie sur la classification des actifs
 - Inclure les risques des fournisseurs et risques externes



Gestion de risques vs gestion de la conformité

- Unifiez la gestion des cadres de gestion de risques
 - Les audiences diffèrent, les risques pour l'organisation se chiffrent de la même façon
 - TI (contrôles de sécurité) supportent simultanément tous les domaines d'affaires
 - La gestion de risque doit apporter de la valeur à l'organisation
- Ne pas unifier
 - Mène à une prolifération des contrôles
 - Risques, coûts, compromis, difficultés de conformité
- Convaincre les vérificateurs du bien fondé des contrôles appliqués



La communication est clé

- Dirigeants
 - Connaissez les actifs et leurs criticité (risques)
 - Unifiez la gestion des cadres de gestion
 - Facilitez la coopération entre les propriétaires des processus d'affaires
 - Intégrez la sécurité aux objectifs d'affaires
- Professionnels des TI
 - Intégrez les analyses de risques dans vos activités courantes
 - Intégrez les contrôles et métriques à vos activités
 - Mettez l'emphasis sur la gestion du changement
 - Automatisez les contrôles
- Gestionnaires de programme de sécurité
 - Assurez l'alignement entre les processus d'affaires et la stratégie de sécurité



La communication est clé

- Professionnels de la sécurité
 - Comprenez votre industrie
 - Collez-vous aux objectifs d'affaires
 - Apprenez à positionner vos projets en terme de valeur à votre organisation
 - Apprenez le langage et processus des affaires
 - Cycle de planification des budgets
 - Assurez-vous que les risques sont connus
 - Pensez solutions mais aussi contrôles, métriques et indicateurs de performance



Le mot de la fin

- Gouvernance
 - Leadership
 - Structure organisationnelle
 - Processus
- Communications
- Ayez du plaisir, les méchants sont dans l'autre camp



Références

- *2010 Data Breach Investigations Report, Verizon, 2010*
- *Information Technology Governance and Service Management—Frameworks and Adaptations , Aileen Cater-Steel, University of Southern Queensland, Australia*
- *Unified frameworks, Moshav Bnei Zion, STKI.info*
- *Leading in Times of Transition: The 2010 CIO Agenda, Gartner 2010*
- <http://www.iso.org/iso/home.htm>
- *ISO 27001, ISO 27002*
- *ITIL*
- *Evolution of governance practices, The Mantra Group*
- *Risk IT Framework, ISACA*
- *Val IT Framework, ISACA*
- *Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit, ITGI and OGC*
- *COSO: How Key Risk Indicators can Sharpen Focus on Emerging Risks, Dec 2010*
- *A Practical Approach to the Successful Practice of 5S By Pradeep Mahalik*
- *ISACA CISM Review Manual 2009*



RSi 2011

Rendez-vous de la **sécurité**
de **l'information**



Benoit Renaud, CISSP, PMP, P.Eng., ITIL v3
Conseiller de direction
Gestionnaire - Programme de sécurité
benoit.renaud@cgi.com



les visages
de la sécurité

Au-delà des apparences

