Quels sont les risques opérationnels de l'Entreprise qui incombent à la Direction Informatique, et comment les traiter de manière efficace ?

Pierre G. Noel
Worldwide Enterprise Risk & Information Security
IBM Corp
Pierre.noel@hk1.ibm.com

TENDANCES LOGICIELLES D'ÉTÉ 2008

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

Qu'est-ce qu'un Risque Opérationnel?

- *Un événement dû à un processus, un système, un personnel insuffisant ou inexistant, qui a causé – ou pourrait potentiellement avoir causé - une perte matérielle ou un impact négatif pour l'organisation*
- *Le risque de dommages survenant lors d'un accident induit par un mauvais fonctionnement ou des erreurs, délibérés ou non*

Source: "Sound Practices for the Management and Supervision of Operational Risk"; Basel Committee on Banking Supervision

Importance des Risques Opérationnels

- Stratégies Défectueuses
  - Mauvaises décisions
  - Défauts de décision
- Performances de la société
  - Agilité, Dynamisme
  - Coût du Crédit (Rating)
- Régulations
  - Violations (Amendes)
  - Conformité (Gains)

Responsabilités du Département de Gestion des Risques Opérationnels

Classification des types de Risques Opérationnels

Fraude Interne

- e.g. intentional misreporting of positions, employee theft, and insider trading on an employee's own account.

Fraude Externe

- e.g robbery, forgery, check kiting, and damage from computer hacking.

Interruption de service et pannes de système

- e.g hardware and software failure, telecommunications problems, and utility outages.

Clients, produits et politiques commerciales

- e.g. fiduciary breaches, misuse of confidential information, improper trading activities on the bank's accounts, money laundering, and sale of unauthorized products.

Dommages causés aux biens physiques

Pratiques en matière d'emploi, de sécurité du lieu du travail

Exécution, livraison et contrôle des processus

Gestion des Risques Opérationnels

Connaître ses Risques

- Quelle est la situation dans l'entreprise en terme d'incidents opérationnels?
- Peuplement de la base de données des Incidents

Gestion des Risques - Création d'un Modèle

- Quels sont les risques à éliminer, comment?
- Quels sont les risques à réduire, comment?
- Quels sont les risques à accepter?
- Mise en place d'une politique ainsi que de contrôles spécifiques

Surveillance et Évaluation

- Quelle est la situation actuelle, quelle sera son évolution?
  - Plus d'incidents, moins d'incidents, nouveaux incidents?
- Quelle interprétation donner en terme de gestion des risques?

Rapporter la situation auprès des instances adéquates

- Haute direction, organismes de contrôles

Déterminer la marche à suivre

- Rapporter la situation par rapport au modèle de gestion des risques opérationnels
- Adapter la politique et les contrôles si nécessaire

Implications du Département Informatique

Fraude Interne

- e.g. intentional misreporting of positions, employee theft, and insider trading on an employee's own account.

Fraude Externe

- e.g robbery, forgery, check kiting, and damage from computer hacking.

Interruption de service et pannes de système

- e.g hardware and software failure, telecommunications problems, and utility outages.

Clients, produits et politique commerciale

- e.g. fiduciary breaches, misuse of confidential information, improper trading activities on the bank's accounts, money laundering, and sale of unauthorized products.

Dommages causés aux biens physiques

Pratiques en matière d'emploi, de sécurité du lieu du travail

Exécution, livraison et contrôle des processus

Le Challenge

La Pyramide Risque repose sur une bonne connaissance et interprétation des risques

Les résultats sont fort souvent en dessous des attentes

La collecte des Incidents incombe aux business units

Responsabilités du Département Informatique

En tant que Business Unit

- Evaluation des Risques Associés
- Remontée des Incidents des systèmes d'Information

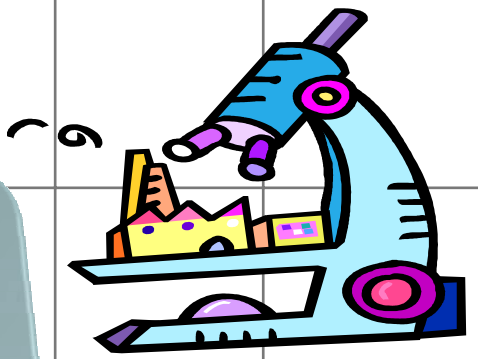
En tant que centralisateur des activités de l'entreprise

- Position exceptionnelle pour collecter et corréler les incidents dans l'entreprise
- Immense valeur ajoutée du DSI

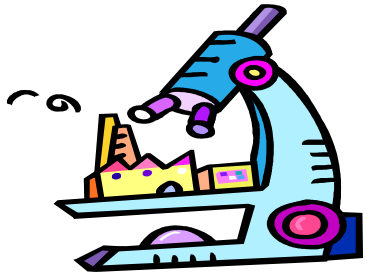
Systèmes d'Information et Risques Opérationnels

	Fraude Interne	Fraude Externe	Interruption de Service et Panne de Système	Clients, Produits et Politique Commerciale	Exécution, livraison et contrôle du processus	Pratique en matière d'emploi, de sécurité du lieu de travail	Dommages causés aux biens physique
Établir et déployer la politique							
Rassembler et archiver les données							
Surveiller & évaluer les risques							
Rapporter les risques & incidents							

Département Systèmes D'Information



Exemple – Conformité SOX



Select Priority Elements & Document Processes

- Consider significance to financial reporting and risk of misstatement
- Document the transaction flows that materially impact the priority financial reporting elements

Source Risks

- Use financial reporting assertions to source "what can go wrong" within the processes

Document Controls

- Document entity controls ("tone at the top")
- Document the controls at the source of the risk (preventive) or downstream in the process (detective and corrective)

Assess Design

- Assess effectiveness of controls design at entity and process levels

Validate Operation

- Test effectiveness of controls operation at entity and process levels

Intégrer DI & ERM

Matrice des Risques	• Analyse des Risques actualisés
BdD des Pertes	• Collecte des incidents et impacts
Contrôles & Protections	• Technologies & Politiques, Education
Mesures	• Incidents et Efficacité des Contrôles
Reporting	• Rapports ERM et de Conformité

Technologies IBM Tivoli

Compliance Insight Manager
Security Compliance Manager

- Visibilité et remontée des Incidents,
- Evaluation de performances des contrôles
- Génération des rapports pour l'ORM

Identity Manager
Access Manager

- Contrôles et automatisation des procédures de gestion des identités et autorisations
- Réduction des risques de type *Fraude interne & externe, clients, produits et contrôle des processus*

Conclusions

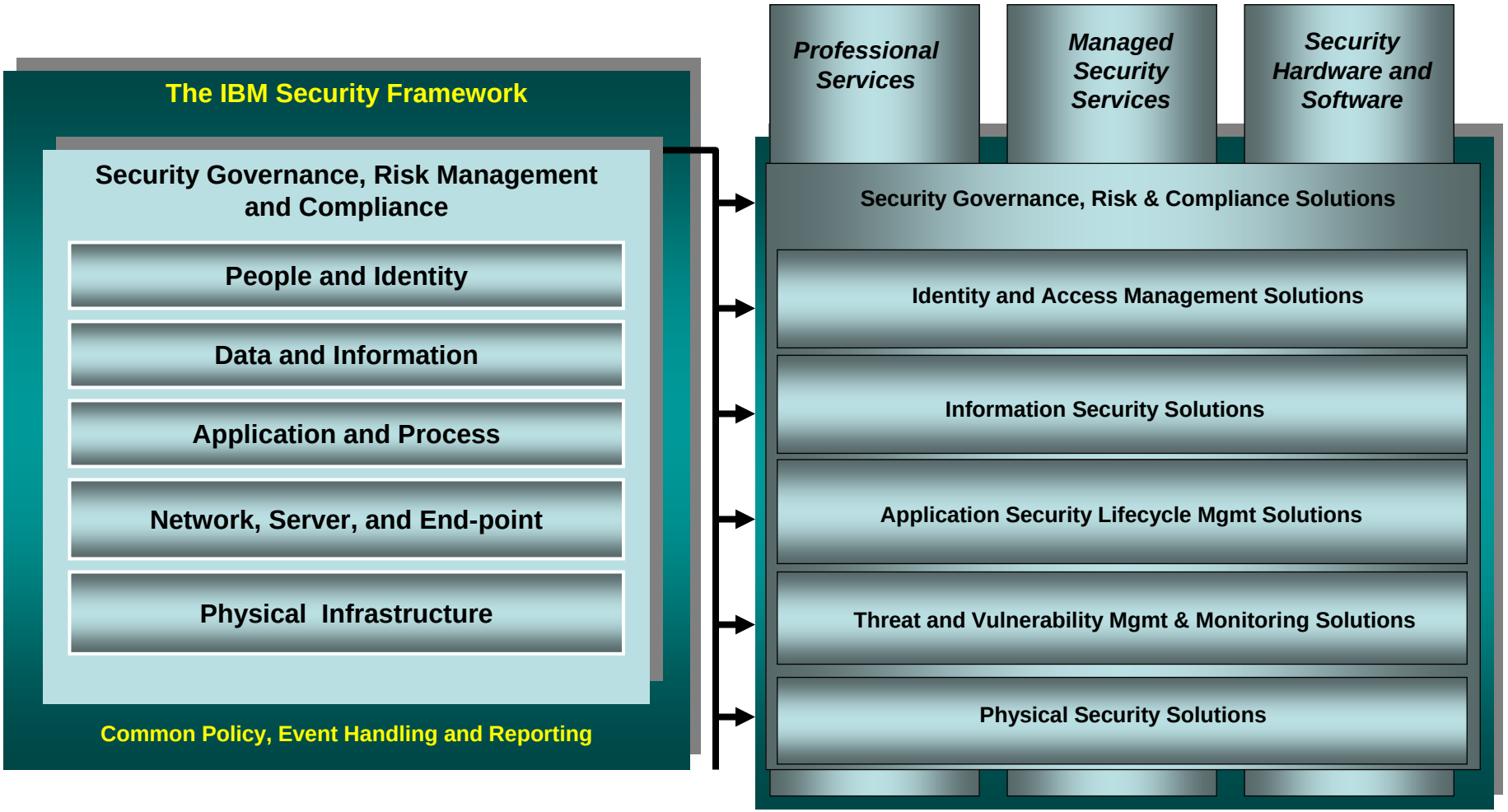
La gestion des risques opérationnels est un composant primordial de la bonne gouvernance d'entreprise

Les DI/DSI sont en position d'apporter une contribution essentielle dans le déploiement de la gestion des risques opérationnels

- Les technologies actuelles permettent le déploiement des mécanismes de visibilité et de contrôles

Cette relation est absolument bénéficiaire pour les DI/DSI

Qui Sommes-nous? IBM Governance & Risk Management

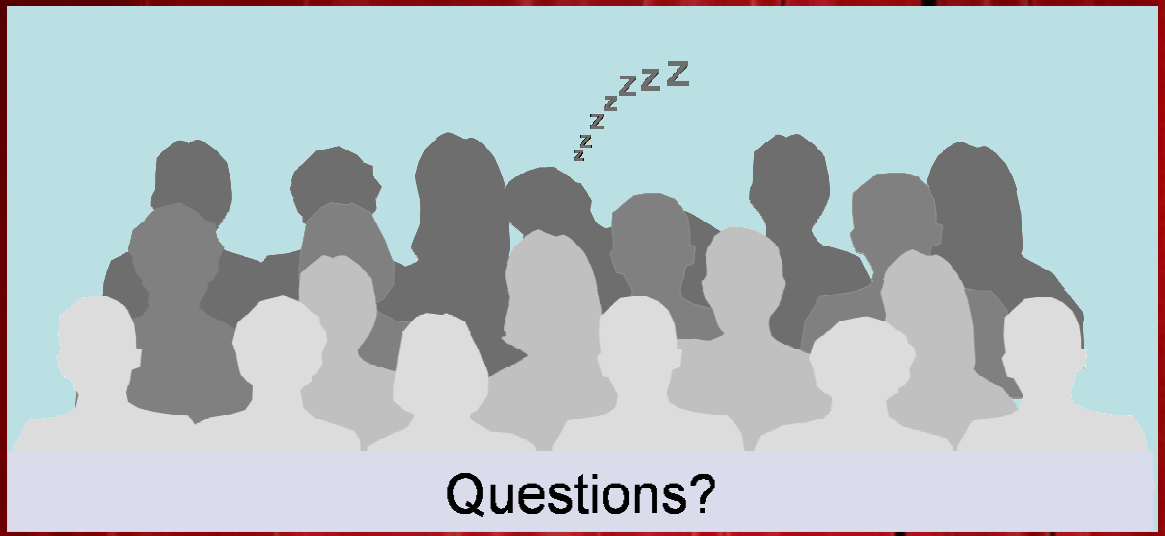


Les perspectives des Analystes sur nos Performances

	Title	2007 Status
FROST & SULLIVAN	Identity Management (TIM , TAM, FIM, TDI, TDS)	**Leader**
FORRESTER®	Wave: User Account Provisioning (TIM)	**Leader**
FORRESTER®	Wave: Enterprise Security Information Management (Consul InSight)	**Leader**
Gartner	MQ: User Provisioning (TIM)	**Leader**
Gartner	MQ: Security Information & Event Management (TSOM, TCIM)	**Challenger**
Gartner	Market share: Web Access Management, Worldwide, 2005 (FIM, TAM)	**Ranked #1**
Gartner	MQ: Web Access Management (FIM, TAM)	**Leader**
IDC Analyze the Future	Marketshare: Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vendor Shares	**Ranked #1**

IBM

Quels sont les risques opérationnels de l'Entreprise qui incombent à la Direction Informatique, et comment les traiter de manière efficace ?



Pierre Noel
WW Risk Management & Information Security
IBM Corp
Pierre.Noel@hk1.ibm.com

TENDANCES LOGICIELLES D'ÉTÉ 2008

SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS