Deloitte.

La gestion des risques TI

Conférence ISACA Québec

9 février 2016

Préface

- Le risque est la possibilité que des événements, prévus ou imprévus, peuvent avoir un effet négatif pour l'entreprise, sa valeur ou sa réputation.
- Les TI sont au cœur de toute entreprise et ainsi les pratiques de gestion TI aide à créer et à protéger la valeur d'une entreprise.
- Du point de vue de la gestion risques, la gestion des risques TI est un sous-ensemble d'un programme de gestion des risques d'entreprise. La sécurité / cyber sécurité est un domaine de risque important, mais comme beaucoup d'autres, il est un sous-ensemble dans la gestion des risques TI.
- Notre présentation vise à vous présenter les différents cadres conçus pour aider à résoudre des besoins en matière de gestion des risques TI. Bien entendu, l'application de ces éléments doivent être adaptés selon vos besoins et exigences spécifiques.

La gestion des risques TI aide à créer et à protéger la valeur d'une entreprise.

Perception côté « affaire »:

- Avons-nous la stratégie informatique liée à mes objectifs d'entreprise?
- Avons-nous une stratégie numérique qui utilise les médias sociaux, le mobile, l'analyse de donnée, le « cloud », etc.?
- Est-ce que notre technologie est suffisamment agile pour s'adapter rapidement à l'évolution de l'entreprise et des objectifs stratégiques?
- Sommes-nous prêts à répondre aux questions du comité d'audit et de nos clients sur notre capacité à gérer les risques d'actualité tel que les risques de cyber sécurité?
- J'ai vu beaucoup d'article et nouvelle sur des incidents de cyber sécurité; sommes-nous prêts si jamais nous avons un incident similaire?
- Comment est-ce que nos systèmes informatiques nous permettent de répondre aux exigences règlementaires et/ou gouvernementales?

Perception côté TI:

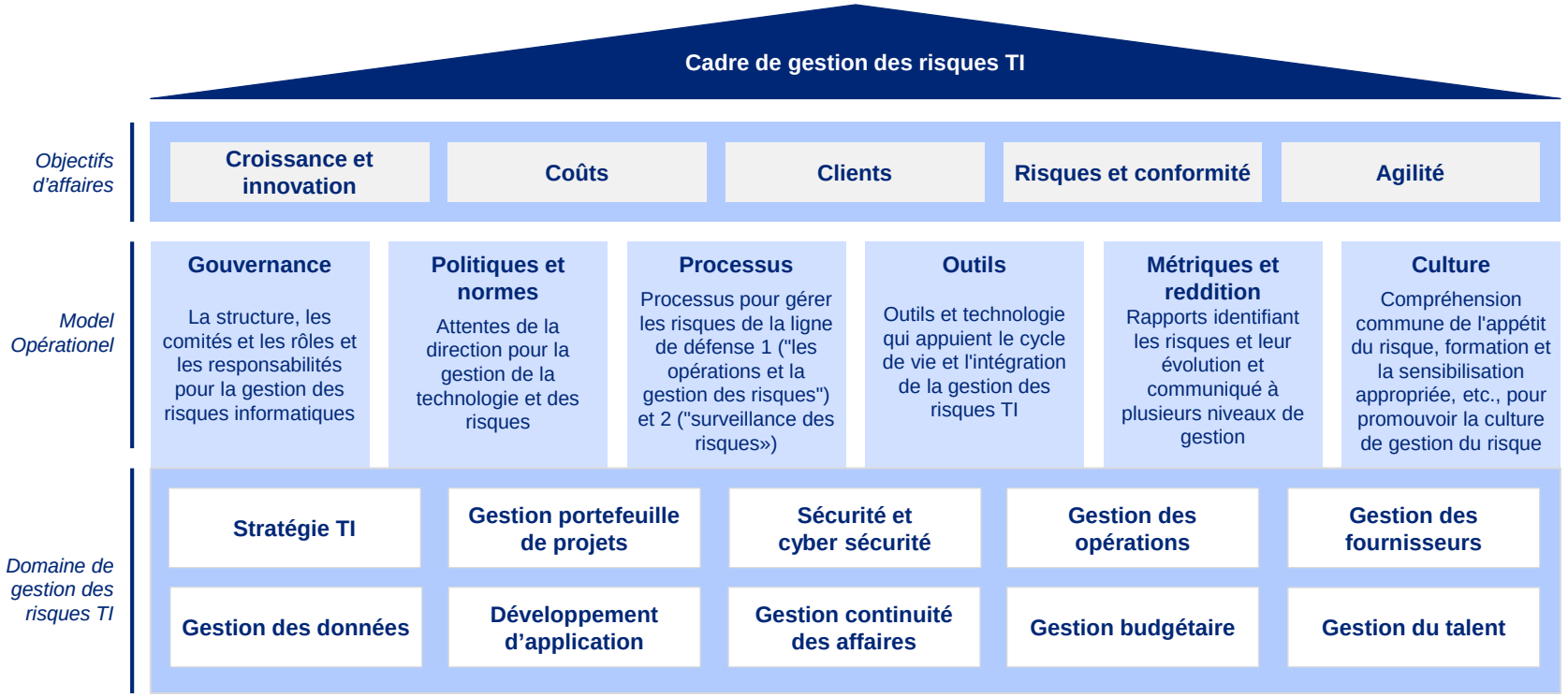
- Comment puis-je m'assurer que ma gestion du risque est liée à ma stratégie TI?
- Comment puis-je garder une longueur d'avance sur les menaces et risques ?
- Comment puis-je gérer les risques TI et opérationnels tout en réduisant les coûts de manière constante?
- Ai-je la bonne stratégie et les bonnes ressources pour gérer les risques de sécurité / cyber sécurité?
- Est-ce que mes mesures de résiliences seront efficaces en cas de crise?
- Est-ce que nous mesurons efficacement nos risques clés? Comment puis-je me compare à l'industrie?
- Est-ce que j'ai les mesures nécessaire pour respecter les exigences réglementaires et/ou gouvernementales?

Le niveau de maturité des pratiques de gestion des risques doit être proportionnel aux risques actuels, à l'industrie, à la taille et à la complexité de l'entreprise

Principes généraux

Cadre et rôles

Un cadre de gestion des risques informatiques / stratégie peut aider une organisation à optimiser à la fois les risques et les coûts tout en répondant aux exigences réglementaires



Les mesures mises en oeuvre pour mitiger les risques doivent être déterminées selon leur importance et votre industrie

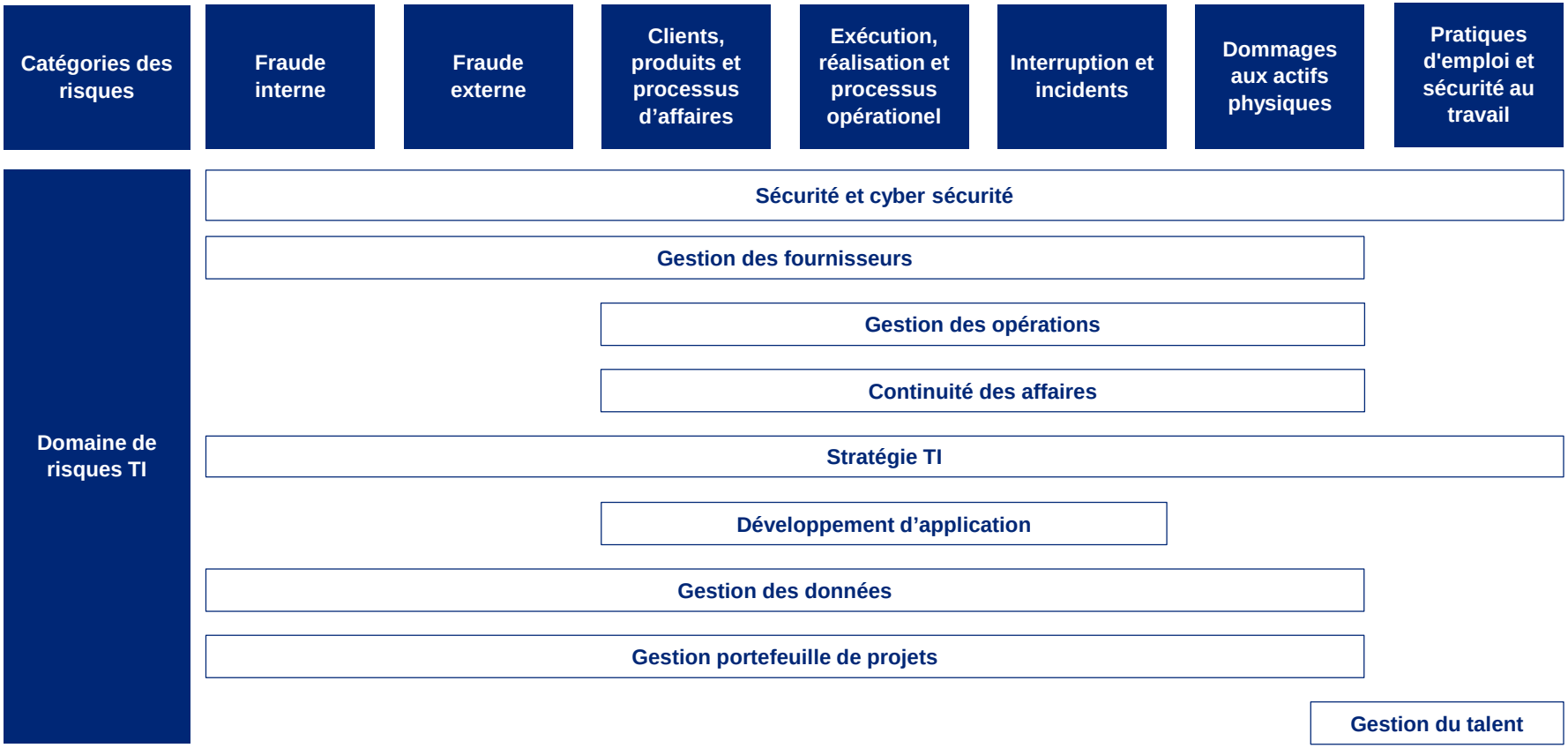
Domaines TI liés aux cadres TI reconnus

Thèmes des cadres généralement reconnus	Sécurité de l'information	Gestion des risques TI	Gouvernance TI	Gestion des TI	Information « privée »
Cadres gestion des risques TI et domaines de risques TI	Pratiques reconnues				
	ISO 27001 NIST 800-53 PCI DSS BS 25999	COSO ISO 27005 ISO 31000	COSO ISO 27005 ISO 31000	ISO 20000 ITIL	GAPP Principles SOC2 ISO 15489
Stratégie TI	■	■	■	■	
Gestion portefeuille de projets	■	■	■	■	■
Sécurité et cyber sécurité	■		■	■	■
Gestion des opérations	■		■	■	
Gestion des fournisseurs	■	■	■	■	■
Gestion des données	■	■			■
Développement d'application	■		■		
Gestion continuité des affaires	■		■	■	
Gestion budgétaire		■	■	■	
Gestion du talent	■		■	■	

Peu importe le cadre de contrôle TI utilisé,
il faut s'assurer de couvrir tous les domaines pertinents

… et liés aux risques d’affaires

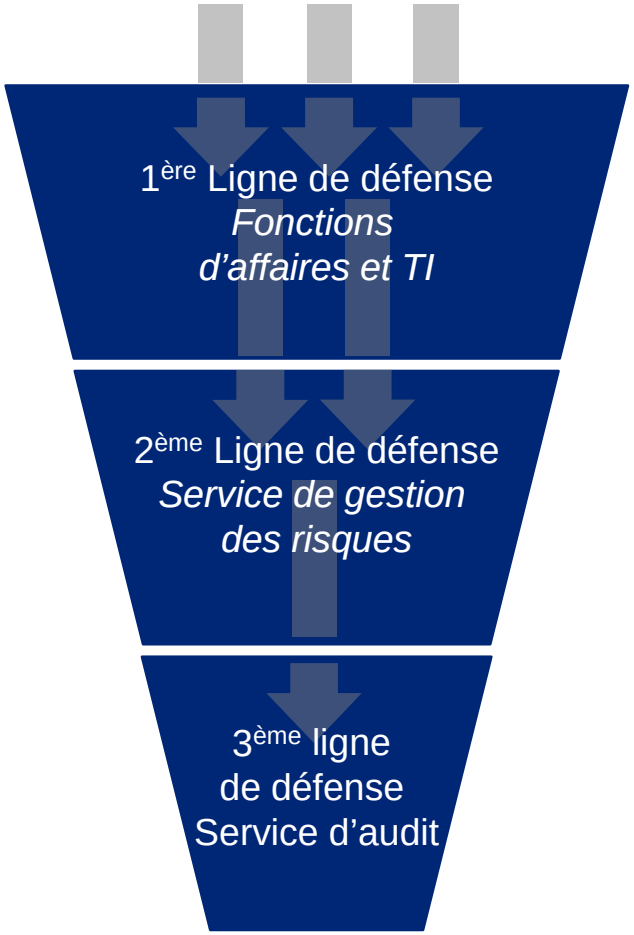
De nombreuses entreprises considèrent la gestion des risques TI comme un sous-ensemble de la gestion des risques opérationnels. La réalité est que les risques TI vont au-delà des risques opérationnels, il doit faire partie des risques d’affaires.



Les risques TI ont un impact sur plusieurs domaines de risques organisationnels, qu’ils soient financiers, liés aux clients, à la réglementation ou la réputation

La gestion des risques TI nécessite une coordination à divers niveaux

La gestion des risques TI est le produit de plusieurs lignes de « défense ». Les fonctions d'affaires et TI sont imputables de la première ligne, donc RESPONSABLE de leurs risques.



Rôles et Responsabilités

- Intégrer la gestion des risques avec la prise de décisions dans les opérations quotidienne afin d'avoir un processus de gestion des risques pleinement intégré aux opérations
- Définir l'appétit du risque et les mesures d'escalade si les risques dépassent les niveaux jugés « acceptable »
- Atténuation des risques à un niveau acceptable

- Détermine les principes de gouvernance
- Définis les politiques, procédures et normes de gestion des risques
- Mise en œuvre des processus et d'outil de gestion des risques
- Surveillance et gestion des mesures correctives
- « Guide » ou consultant sur les politiques et processus

- Fonction indépendante qui valide l'efficacité de la gestion des risques
- Fourni une assurance à la direction sur l'efficacité de la gestion des risques
- Utilise la gestion des risques pour des besoins de planification d'audits

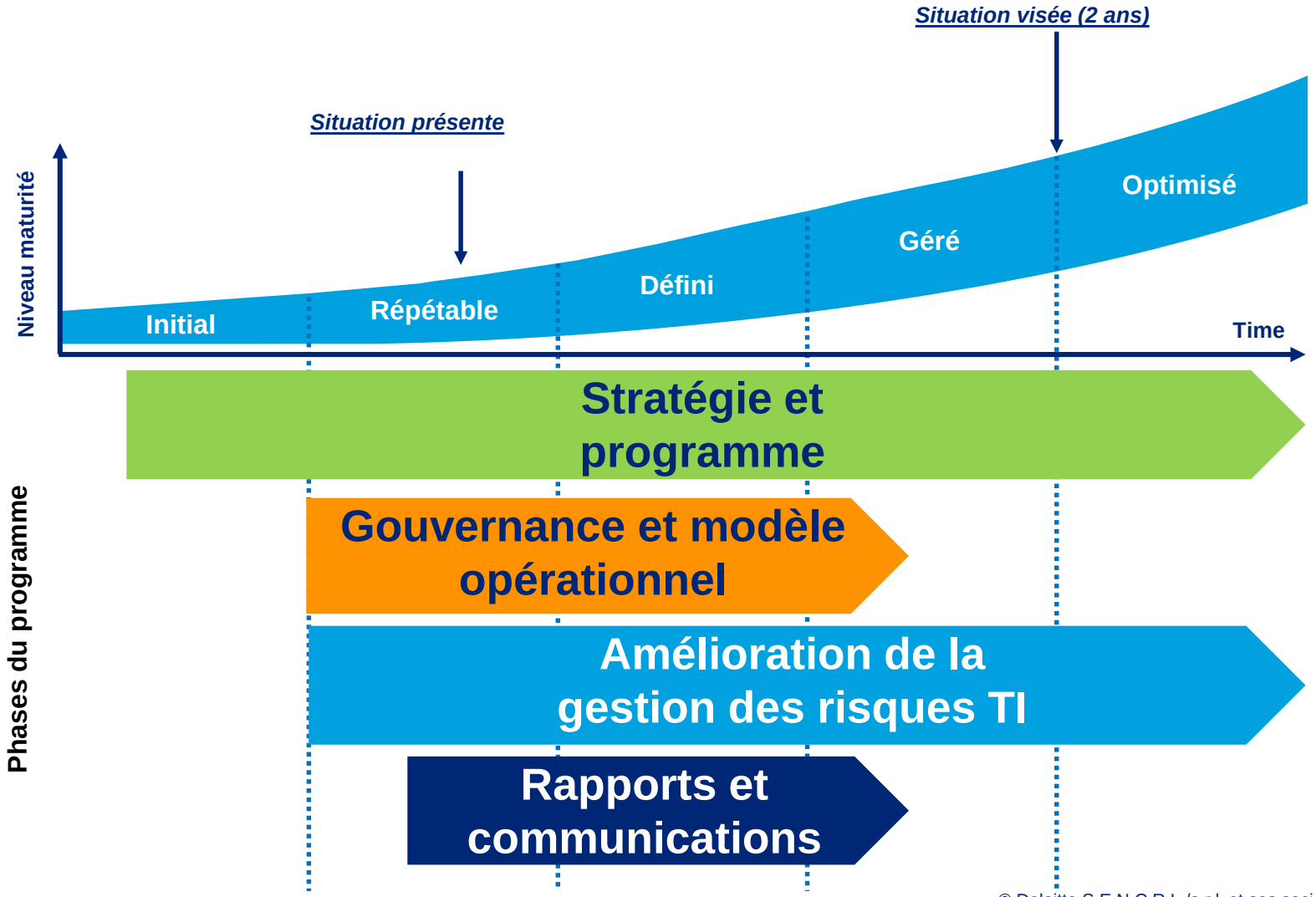
Toutes les fonctions doivent comprendre leur rôle dans la gestion des risques TI – une coordination inefficace peut entraîner des coûts inutiles

Niveau de maturité

Où? Quand? Comment?

Des programmes de gestion des risques TI “mature” débutent par une compréhension des capacités et des exigences réglementaires

Les objectifs varient selon les entreprises et les industries. Un programme « typique » nécessite 3 à 6 mois pour mettre en œuvre un programme de base et 12 à 24 mois (ou plus) pour un programme optimisé.



Les composantes de l’échelle de maturité

Stratégie / Programme	Gouvernance et modèle opérationel	Amélioration de la gestion des risques TI	Rapports et communications

• Aligner les objectifs d’affaires et les objectifs des risques d’affaires
• Identifier les « capacités » manquantes (ressource, processus et technologie)
• Comprendre les besoins réglementaires et autres attentes de conformité (ex. PCI)
• Développer une stratégie de gestion des risques (objectifs, tâches, date ciblées, etc.)
	• Définir le modèle opérationnel
	• Définir les rôles et responsabilités de chaque fonctions (opérations, légal, TI) sur l’ensemble des lignes de défense
	• Définir les politiques et procédures de gestion des risques
		• Mise en œuvre des politiques et procédures définies
		• Mis en œuvre des processus et des outils
		• Mise en œuvre de la surveillance des risques
		• Analyse de la corrélation entre les événements et les risques – apprendre le “pourquoi”
			• Développement de rapport pour les
			  • TI
			  • les unité d’affaires
			  • la direction
			  • organismes réglementaires
			  • audit interne
			• Programme de formation formelle
			• Session d’information sur les processus et les résultats

Exemples

Évaluation des risques

Exemple de définition impact et vulnérabilité

Impact - On suppose que l'événement sous-jacent s'est produit (valeurs indiqués à titre d'exemple).

Faible	Moyen	Elevé
• Les **conséquences** sont susceptibles de se répercuter sur un ensemble limité d'activités de l'organisation. • Les impacts **financiers** ne sont pas évalués ou ne sont pas significatifs (- 1.5M$). • La situation n'est pas rapportée dans les **médias**.	• Les **conséquences** sont susceptibles de se répercuter sur un ensemble significatif d'activités de l'organisation, sans pour autant affecter toute l'entreprise ou ses activités les plus critiques. • Les impacts se font **sentir** durant une période prolongée (- 5 jours). • Des impacts **financiers** modérés sont anticipés (- 5M$). • La situation fait la manchette dans les **médias locaux**.	• Les **conséquences** sont susceptibles de se répercuter sur l'ensemble des activités de l'organisation ou affecter ses activités les plus critiques • Les impacts se font **sentir** durant une période prolongée (+ 5 jours). • Des impacts **financiers** significatifs sont anticipés (+ 5M$). • La situation fait la manchette dans les **médias nationaux**.

Peu importe l'échelle et les définitions utilisées, elles doivent être les mêmes que celles utilisées par la gestion des risques d'affaires

Définition de l’impact et de la vulnérabilité

Vulnérabilité - Probabilité que l’événement sous-jacent se produise en tenant compte des mesures de contrôle interne mises en place actuellement

Faible	Moyen	Elevé
• Il est peu probable que le risque se **matérialise**. • Les contrôles préventifs et détectifs en place ont été **bien conçus, mis en œuvre et fonctionnent** de manière efficace en tout temps afin de réduire le risque à un niveau acceptable. • Les processus concernés sont **simples** et les personnes qui en ont la responsabilité **maitrisent** adéquatement les risques. • Pas connaissance que ce risque se soit **matérialisé** dans le passé.	• Il est probable que le risque se **matérialise**. • Les contrôles préventifs et détectifs en place ont été **bien conçus et mis en œuvre** mais **ne fonctionnent efficacement**. • Les processus concernés sont **modérément complexes** et les personnes qui en ont la responsabilité **ne maitrisent** pas adéquatement les risques. • Connaissance de quelques situations où ce risque s’est **matérialisé**.	• Il est certain que le risque se **matérialise**. • Aucun contrôle préventif ou détectif n’a été conçu pour réduire le risque à un niveau acceptable. • Les processus concernés sont **très complexes** et il **manque** de **compétences** à l’interne pour maitriser adéquatement les risques. • Connaissance de situations fréquentes où ce risque s’est **matérialisé**.

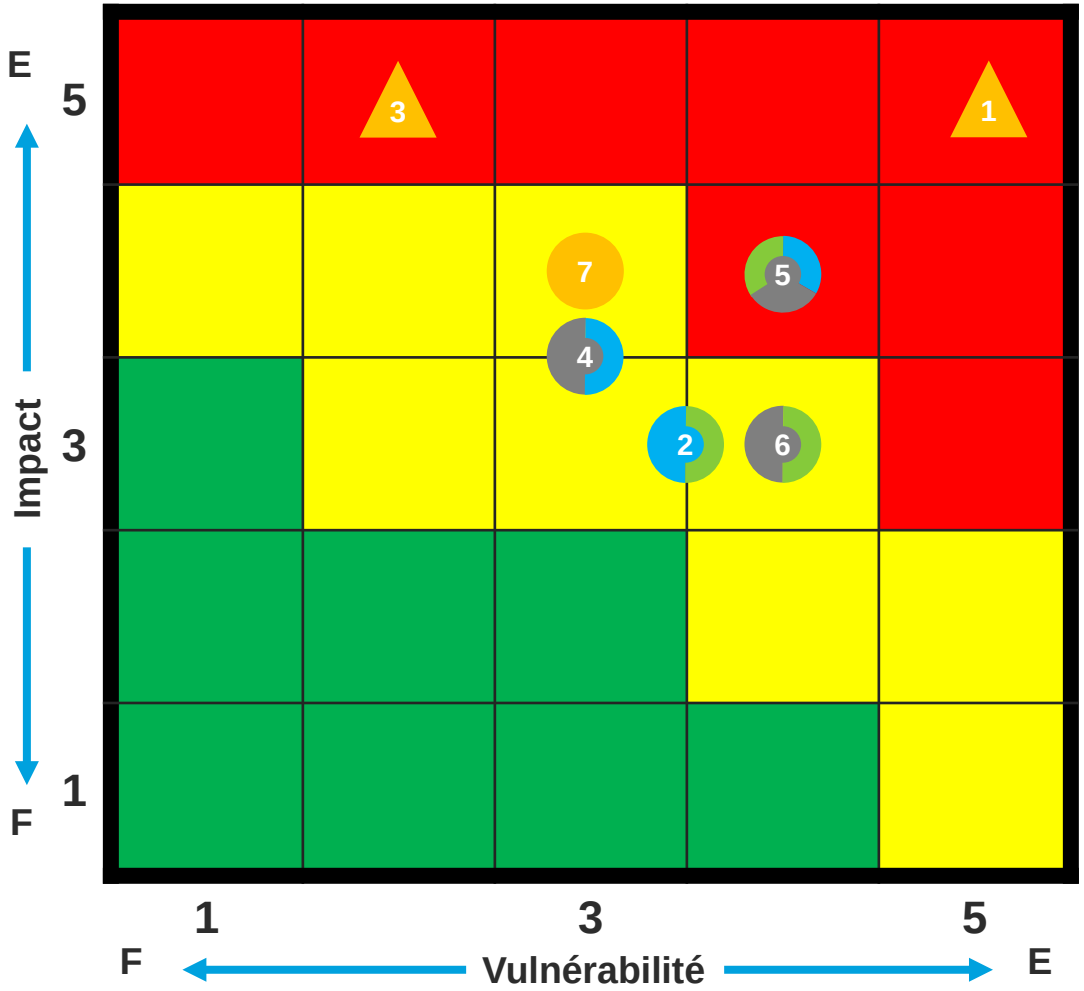
Prenez en considération l’appétit pour le risque
Deux risques avec une vulnérabilité élevée n’auront pas la même importance

Grille d’évaluation des risques

#	Domaine	Risque	Contrôles	Appétit	Objectifs d'affaires	Imp.	Vul.	Cote
IT-PRMG-1	Gestion portefeuille de projets	Risque est que ceci ne fonctionne pas bien	PGM-1	Faible	Innovation Coûts	4	3	12
IT-PRMG-2	Gestion portefeuille de projets	Risque est que ceci ne fonctionne pas bien	PGM-12	Elevé	Innovation	3	1	3
IT-PRMG-3	Gestion portefeuille de projets	Risque est que ceci ne fonctionne pas bien	PGM-1	Elevé	Coûts Clients	5	5	25
IT-PRMG-4	Gestion portefeuille de projets	Risque est que ceci ne fonctionne pas bien	PGM-2	Moyen	Agilité	4	2	8
IT-PRMG-5	Gestion portefeuille de projets	Risque est que ceci ne fonctionne pas bien	PGM-3	Faible	Coûts Clients	1	5	5

#	Responsable	Plan d'action	Date cible	Mesure
IT-PRMG-1	Direction ABC	Direction ABC	Date	Indicateur 1
IT-PRMG-2	Groupe 123	Groupe 123	Date	Indicateur 2
IT-PRMG-3	Équipe A	Équipe A	Date	Indicateur 3
IT-PRMG-4	Direction ABC	Direction ABC	Date	Indicateur 4
IT-PRMG-5	Groupe 123	Groupe 123	Date	Indicateur 5

Exemple – Cartographie des risques



#	Titre
1	Fuite des données confidentielles système XYZ
2	Risque 2
3	Risque 3
4	Risque 4
5	Risque 5
6	Risque 6
7	Risque 7

Objectifs d'affaires impactés

- Réduction des coûts
- Croissance et innovation
- Agilité
- Client

Priorité du risque

1 ▲ 2 ● 3 ■

Exemple de communication et de gestion des risques

Risque

# 1	Fuite des données confidentielles	Propriétaire : David Liberatore	Élevé

Description : Il y a un risque de fuite des données clients classées “confidentielles” suite à une brèche des mesures de sécurité.

- Impact : 5
- Vulnérabilité : 5

Priorités stratégiques impactées :

Réduction des coûts	Agilité	Croissance Innovation	Clients

Plan d’action

1. Mise en œuvre du projet Alpha – Février 2016
2. Revue politique ABC – Juillet 2016
3. Projet XYZ – Décembre 2016

Estimés :


Moyen (200 j/p)


Elevé ($1.5M)


Elevée


10 mois


Ressource


Coûts


Complexité


Durée

Leçons apprises

Partager nos expériences

Utilisation de la gestion des risques

Cas vécu

Besoin 1	Analyse de dépendance envers la technologie de l'information et ses ressources
Besoin 2	Analyse des risques liés à la sécurité de l'information et des contrôles en place pour atténuer ces risques
Contexte	Client avec ressources syndiquées et avec effectif limités (petite équipe)

Nos apprentissages – Gestion des risques TI

- Une bonne compréhension de la tolérance au risque (appétit) de l'entreprise est nécessaire pour vous permettre d'innover, augmenter les revenus et réduire les coûts tout en protégeant votre valeur. La conformité ou la simple identification des risques n'est suffisante
- La gestion des risques TI n'est souvent pas prise en charge par la direction des TI. Les risques n'ont pas de « propriétaire » TI responsable de leur gestion
- Avec la maturité des programmes de gestion des risques TI, les organisations ont tendance à se diriger vers la 2ème ligne de défense vs. la 1ère ligne. Avec le temps, la responsabilité devrait tendre vers : 70% opérations (1ère ligne), 20% la surveillance des risques (2ème ligne) et 10% audit (3ème ligne)
- La cyber sécurité, la résilience TI et la gestion des données sont souvent le top 3 des priorités TI pour la plupart des entreprises (dans une perspective de protection de la valeur)
- Un programme des risques TI n'est pas la même chose qu'une stratégie de risque TI; les entreprises ont souvant un programme, mais pas une véritable stratégie
- Si vous ne pouvez pas mesurer, vous ne pouvez pas améliorer; identifier des indicateurs de risques TI mesurables
- Le responsable de risque TI est un partenaire qui travaille à la surveillance des risques TI et son indépendance est souvent un sujet de préoccupation réglementaire
- La gestion de la conformité n'est pas la gestion du risque; souvent des entreprises qui ont été compromises sont "conformes aux normes"
- Les unités d'affaires sont les propriétaires des données; les TI sont les gardiens de données

Nos apprentissages – sécurité et cyber sécurité

- Les entreprises dépensent des millions de dollars sans comprendre pleinement les risques réels et comment les mitiger. De nombreux contrôles traditionnels ne sont pas suffisantss pour protéger contre les menaces actuelles. Ils doivent être améliorés ou de nouveaux contrôles doivent être ajoutés
- Il est nécessaire pour les entreprises de définir et à mettre à jour sa stratégie de sécurité de l'information / cyber sécurité sur une base régulière (ex. bi-annuelle) et investir de manière appropriée
- La direction des TI doit s'approprier les risques liés à la sécurité ou cyber sécurité. Le gestionnaire de risque TI est un acteur important, mais ne peut pas être responsable des mesures de contrôle et du plan d'action
- Ne pas négliger le maillon faible dans les processus, sites ou opérations car ces derniers sont souvent les cibles des « hackers »
- Le périmètre est maintenant très étendu (média sociaux, « cloud », solutions mobiles et autres nouvelles technologies). Bien que des risques légitimes soient introduits avec ces nouvelles technologies, méfiez-vous de la surévaluation des risques. Il faut déterminer des solutions réalistes et facilement applicable selon le contexte de l'entreprise
- Les contrôles préventifs ne sont plus suffisant; des contrôles défectifs sont requis
- Fixez des objectifs pour les indicateurs de risque et assurez-vous que les responsables des risques les respectent
- La formation et la sensibilisation est importante et souvent négligée. Des exercices de simulation peuvent jouer un rôle clé dans la sensibilisation des entreprises, ressources humaines, juridique, etc

Nos coordonnées

David Liberatore, M.Sc., CPA, CA, CISA, CISSP
Directeur de service | Service Risques d’entreprises
Ligne directe : 514-393-7817
dliberatore@deloitte.ca

Marco Spagnoli, CISA
Directeur principal | Service Risques d’entreprises
Ligne directe : 514-393-5247
mspagnoli@deloitte.ca

Deloitte.

Deloitte, l’un des cabinets de services professionnels les plus importants au Canada, offre des services dans les domaines de la certification, de la fiscalité, de la consultation et des conseils financiers. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l’Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

L’information contenue dans le présent document ne peut remplacer les conseils d’un spécialiste.

.