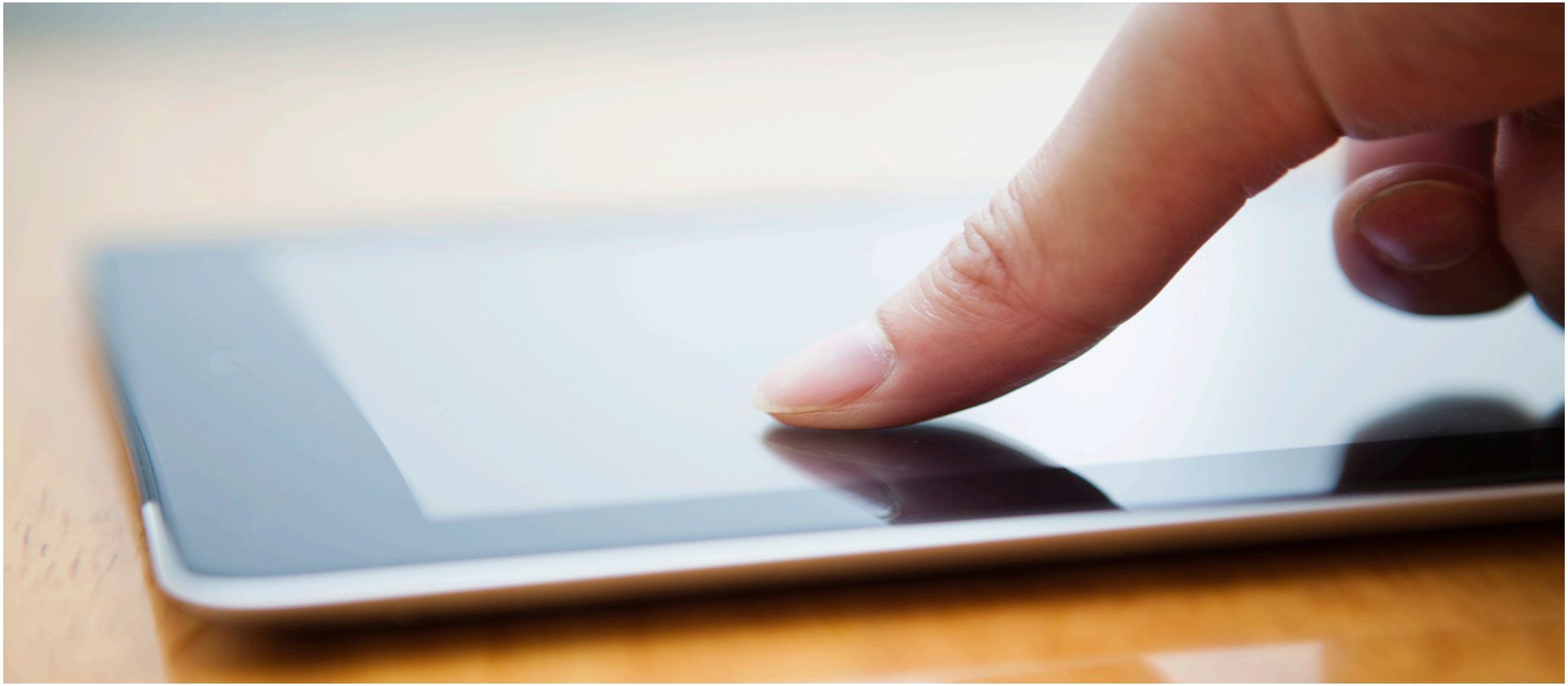
ISACA
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec



LES RISQUES TI DES PROCESSUS D'AFFAIRES: UNE PERSPECTIVE DE BDO

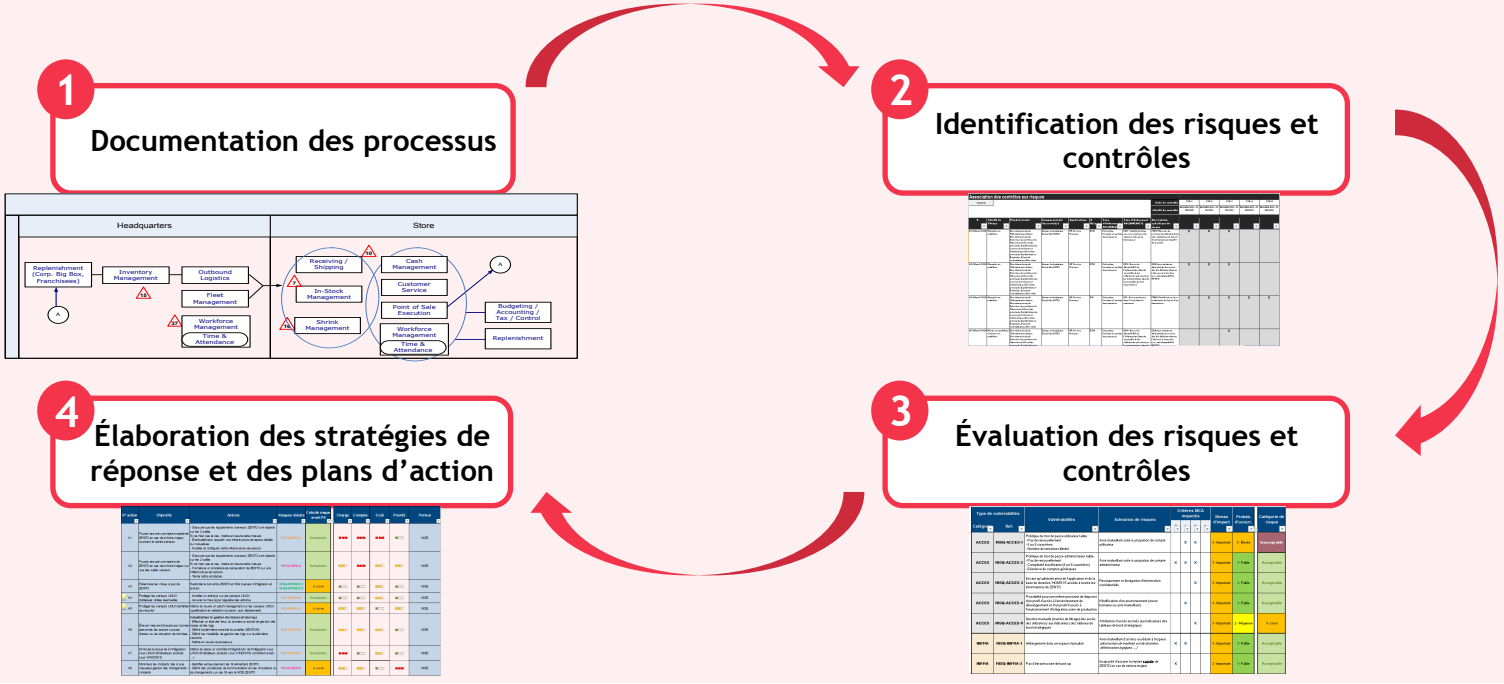
Le 9 février 2016

BDO

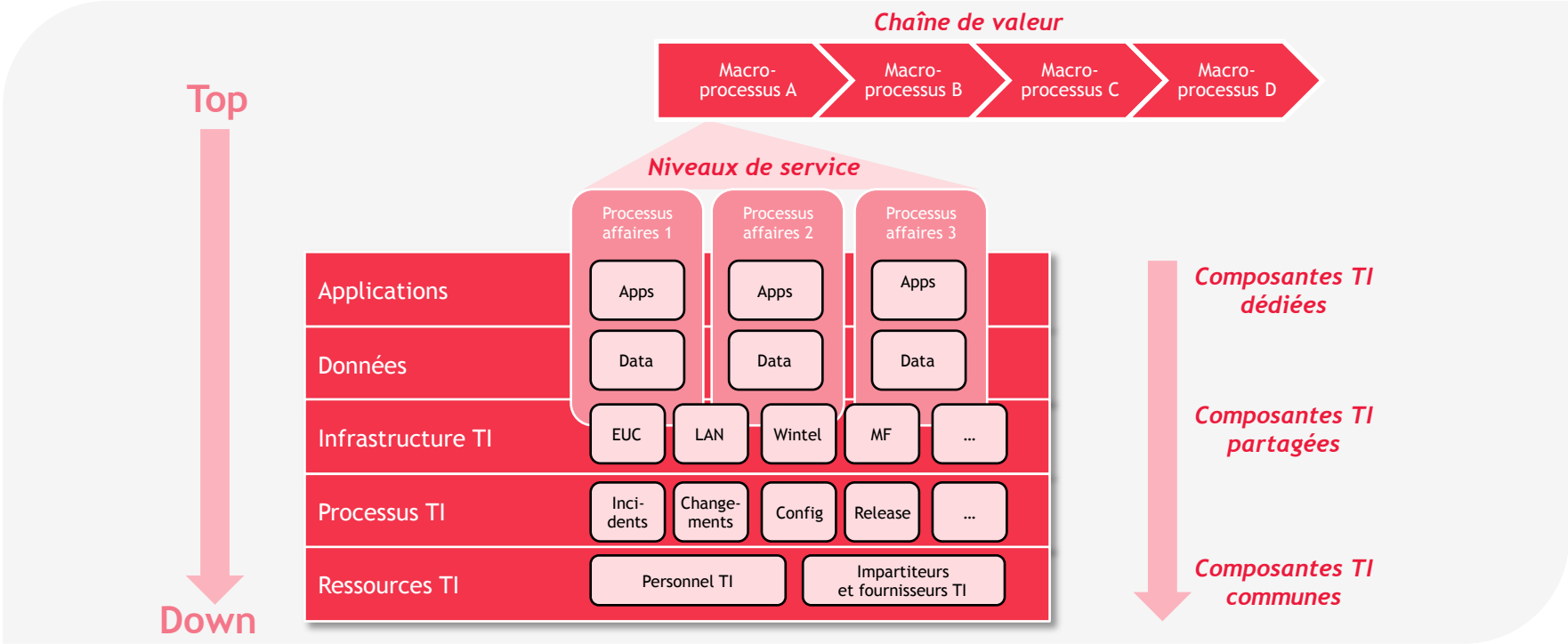
Table des matières

Définition pragmatique d'analyse de risques par processus

- Un processus est un **enchaînement d'activités** qui produit un **résultat attendu** à partir d'**intrants** et de **capacité de réalisation**
- L'analyse de risques vise ainsi à :
  - Déterminer les **impacts et la probabilité** d'évènements reliés à ce processus, qui pourraient affecter sa mission
  - Identifier les **mesures** de minimisation de ces risques au travers d'activités de contrôles permanents spécifiques
  - Évaluer le **niveau de risque résiduel** du processus
  - Déterminer les **stratégies de réponse** au risque résiduel et les plans d'actions en découlant



Introduction à l'architecture d'entreprise, intrant indispensable à la gestion des risques par processus



- Pour exécuter une démarche de gestion des risques par processus, il est nécessaire de connaitre la **décomposition de ces processus**
- L'**architecture d'entreprise** permet de décomposer les processus d'affaires selon une **vue "Top-Down"**, en partant des processus d'affaires, puis en déterminant les **applications et l'infrastructure les supportant** et en prenant en compte les **données et ressources traitées** par ces derniers

1.
LA GESTION DES RISQUES TRADITIONNELLE

La gestion des risques des processus d'affaires

Définition

- Un processus d'affaires est un **élément de la chaîne de valeur** de l'entreprise qui produit une **valeur ajoutée** pour l'organisation et/ou les parties prenantes
- Dans le cas d'un processus d'affaires, **on évalue généralement** les **risques d'affaires** et les **activités de contrôles d'affaires** pour minimiser ces risques
- Le portefeuille de contrôles **visant à minimiser les risques** est généralement constitué d'activités de **contrôles permanents :**
  - **manuels** ou **applicatifs**
  - **préventifs** ou **détectifs**

Exemple 1

Processus d'affaires : **octroyer un prêt hypothécaire**
Risque d'affaires : insolvabilité du client hypothécaire
Contrôles d'affaires rattachés au risque :

- Historique du client
- Score de crédit
- Prêts hypothécaires en cours auprès d'autres établissements financiers

Exemple 2

Processus d'affaires : **traiter les cartes de débit**
Risque d'affaires : usurpation de compte ou d'identité
Contrôles d'affaires rattachés au risque :

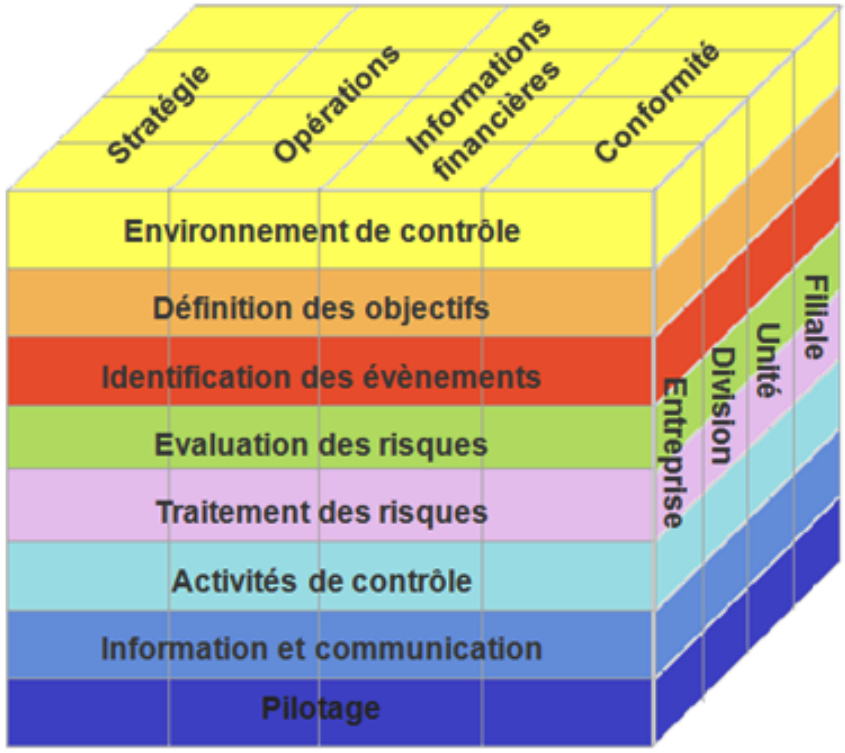
- Contrôle de supervision à l'ouverture de compte
- Envoi séparé de la carte et du NIP
- Vérification des appels des conseillers quand une fraude est constatée

La gestion des risques des processus d'affaires
Cadres de contrôle

Plusieurs **référentiels** sur le marché offrent des **cadres de contrôles d'affaires permanents**, à **exécuter régulièrement** pour s'assurer d'une **bonne performance** des processus d'affaires:

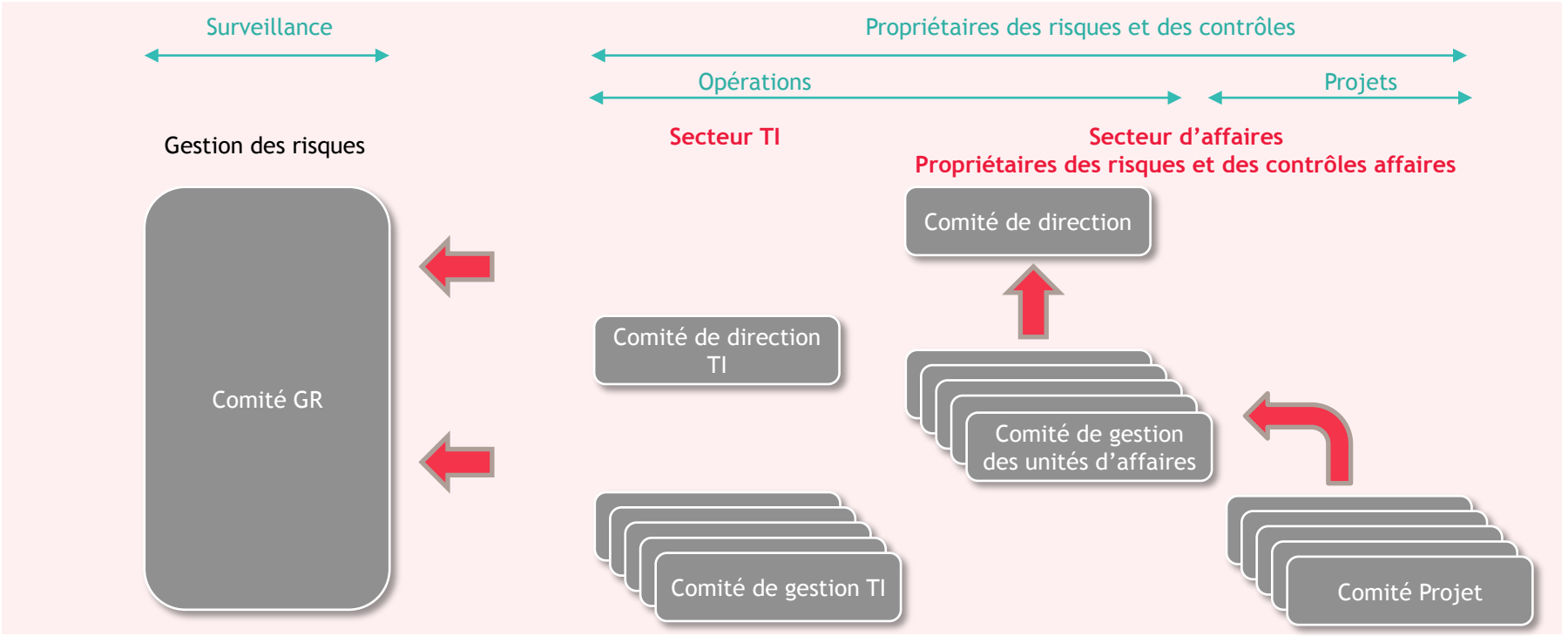
- Bâle
- SOX / 52-109
- COSO
- ISO 31000

COSO 2



Gouvernance de la gestion des risques des processus d'affaires

Le secteur d'affaires effectue sa propre reddition de comptes directement aux instances de gestion des risques et de conformité



La gestion des risques des processus TI

Définition

- Les processus TI permettent de **concevoir, produire, maintenir et supporter l'ensemble des actifs technologiques** de l'organisation (ses applications, ses données et son infrastructure). C'est un **cas particulier du processus d'affaires,** qui est en même temps un « **facilitateur** » de tous les autres processus d'affaires
- Dans le cas d'un processus TI, **on évalue généralement les risques TI** et les **activités de contrôles TI** pour minimiser ces risques
- Le portefeuille de contrôles **visant à minimiser les risques** est généralement constitué d'activités de **contrôles permanents :**
  - **manuels** ou **applicatifs**
  - **préventifs** ou **détectifs**

Exemple 1

Processus TI : **gestion des changements**
Risque TI : mise en production de changements inadéquats
Contrôles TI de minimisation du risque :

- Réalisation de tests unitaires, intégrés et d'acceptation
- Environnements de test copiés des environnements de production
- Validation des tests par un tiers non impliqué

Exemple 2

Processus TI : **gestion des problèmes**
Risque TI : interruption ou dégradation de service dues à la défaillance d'un fournisseur
Contrôles TI de minimisation du risque :

- Niveaux de performance évalués de façon régulière
- Contrats d'exploitation précisant les niveaux de service documentés et approuvés
- Copies de sauvegardes des données des systèmes effectuées régulièrement

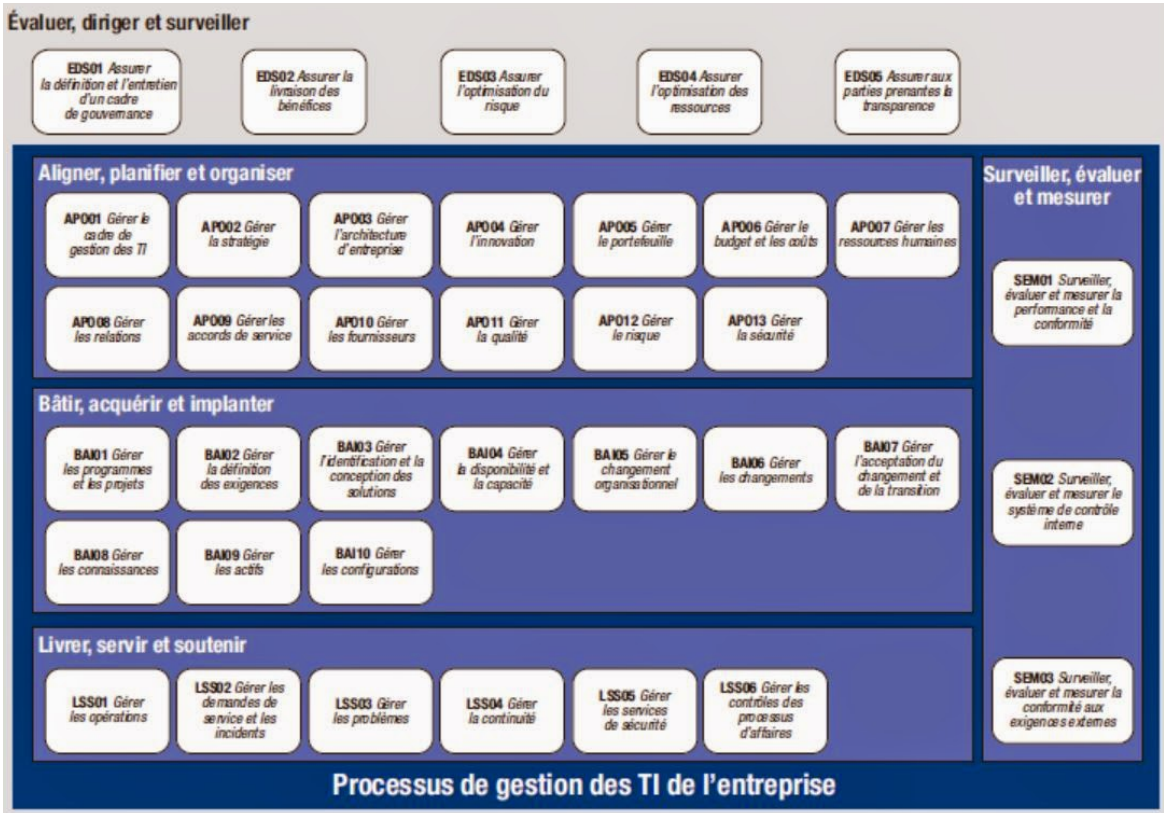
La gestion des risques des processus d'affaires

Cadres de contrôle

Plusieurs **référentiels** sur le marché offrent des **cadres de contrôles TI permanents**, à **exécuter régulièrement** pour s'assurer d'une **bonne performance** des processus TI:

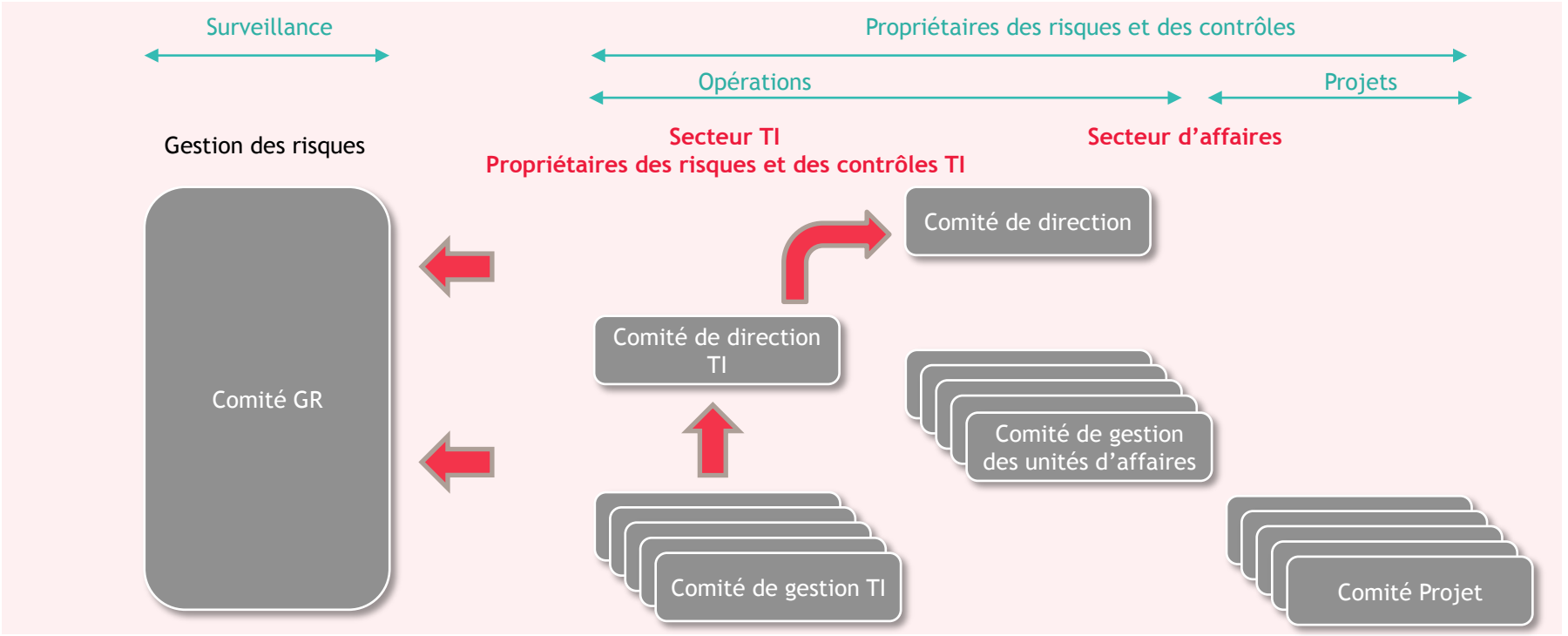
- COBIT
- ISO 27001/2
- ITIL
- CMMI

COBIT 5

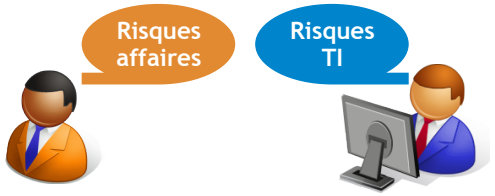


Gouvernance de la gestion des risques des processus TI

Le secteur TI effectue également sa propre reddition de comptes directement aux instances de gestion des risques et de conformité



Constats



- La **gestion des risques** sur les processus d'**affaires** et la gestion des risques sur les processus **TI** arrivent **à maturité**, chacune dans leur **univers respectif**.
- Cependant, ces 2 disciplines restent encore trop **cloisonnées** :
  - Chaque "univers" s'appuie sur des **référentiels propres** et identifie ses **propres risques et contrôles**, indépendamment les uns des autres
  - Chaque "univers" fait sa **propre reddition de comptes** aux propriétaires de risques et de contrôles ainsi qu'aux comités de gestion des risques
- Les secteurs d'affaires et TI collaborent souvent **sur un mode réactif** en cas de problèmes ou d'incidents sur les TI, et **pas suffisamment sur un mode préventif**, afin de prévenir ces problèmes et incidents, en gérant mieux les risques TI.
- Ainsi, dans la mesure où **les TI sont de plus en plus au cœur de l'exécution - et donc des risques - des processus d'affaires**, la gestion des risques TI des processus d'affaires devient **incontournable**

2.
UNE GESTION DES RISQUES À REPENSER : LA GESTION DES RISQUES TI DES PROCESSUS D'AFFAIRES

La gestion des risques technologiques des processus d'affaires
Définition

- **Un processus d'affaires est de plus en plus souvent supporté par des actifs TI** (applications et infrastructure notamment), qui facilitent son exécution
- **Si l'un de ces actifs TI fait défaut**, **certaines activités du processus** qu'il supporte **peuvent se retrouver en péril**, ne plus être exécutées convenablement et occasionner des **pertes de** revenus, des **coûts additionnels** ou des **déficits de réputation**
- Dans ce contexte, l'identification et l'évaluation **des mesures de mitigation des risques TI** (mesures que nous appellerons **contrôles TI**) spécifiques à ces actifs TI s'avèrent **indispensables**

Exemple 1

Processus d'affaires : **octroyer un prêt hypothécaire**
Risque TI : indisponibilité des services permettant cet octroi
Contrôles TI rattachés au risque :

- Qualité technologique de l'application
- Existence d'un contrat de maintenance à jour
- Redondance de l'infrastructure

Exemple 2

Processus d'affaires : **traiter les cartes de débit**
Risque TI : perte, vol, corruption de données ou fuite d'informations
Contrôles TI rattachés au risque :

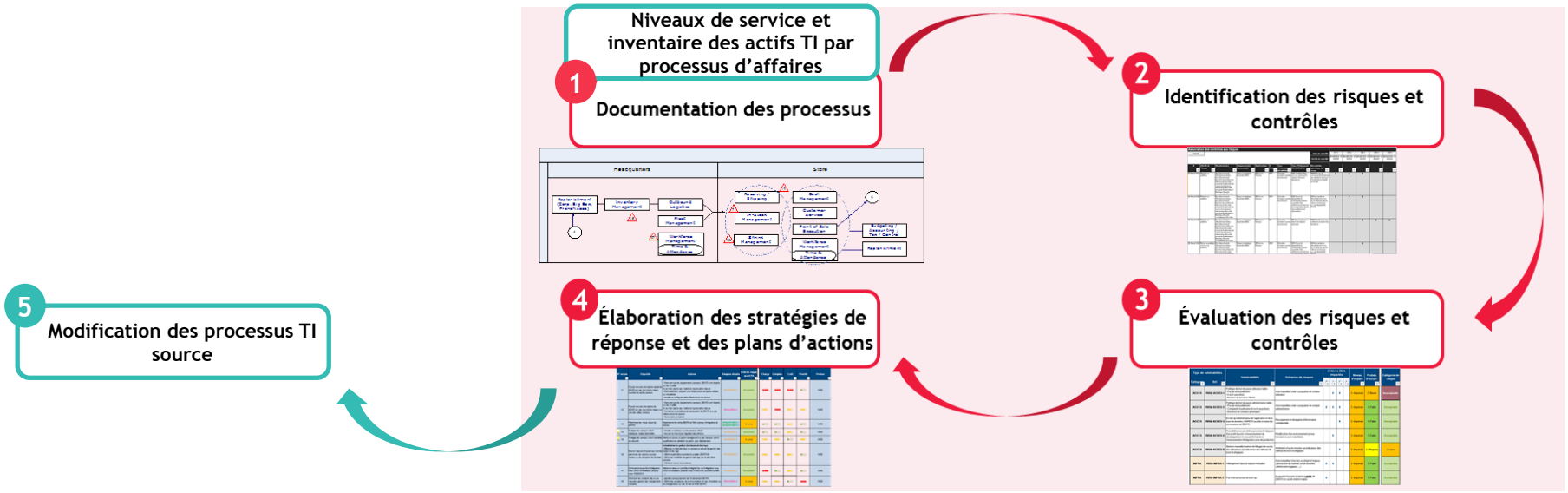
- Accès en écriture aux fichiers critiques surveillés de façon régulière
- Tests d'intrusion internes et externes effectués de façon périodique
- Analyses de vulnérabilités internes et externes périodiquement

3.
L'ÉVALUATION DES RISQUES TI DES PROCESSUS D'AFFAIRES

Méthodologie et outils de la gestion des risques TI des processus d'affaires

L'évaluation des risques TI des processus d'affaires peut suivre une méthodologie identique à celle présentée précédemment, mais **ne peut être déployée immédiatement**. Elle nécessite certains **prérequis**, tels que:

- L'**identification des niveaux de service TI** attendus par les affaires dont découle la **priorisation** des processus d'affaires et des actifs TI critiques
- La **décomposition** des processus d'affaires **en actifs TI**
- La **compréhension des dépendances entre ces actifs**



Approche de gestion des risques TI des processus d'affaires

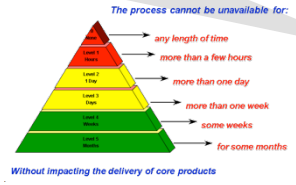
Illustration avec le processus de gestion des cartes de débit

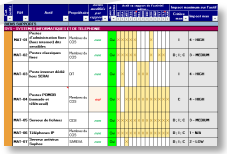
1 Documentation processus, niveaux de service inventaire des actifs TI

L'**identification des niveaux de service** et l'**inventaire des actifs TI** par processus peuvent s'avérer **laborieux**.
Ces activités peuvent **donc être une étape préliminaire** (« intrant ») à l'étape de documentation des processus, dépendamment du **niveau de maturité de l'organisation.**

Approche par niveau de disponibilité:
Combien de temps le processus peut-il être arrêté sans impact d'affaires inacceptable ?

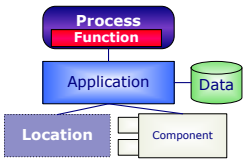
Approche par niveau de confidentialité:
Quels sont les niveaux de confidentialité des données traitées et/ou échangées dans le processus?





Analyse d'impacts d'affaires (BIA)

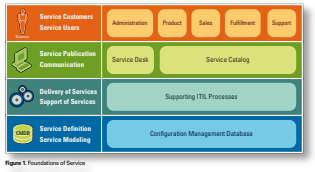
Classification des actifs



Architecture d'entreprise

Niveaux de services et inventaire des actifs TI par processus d'affaires

Base de données de configuration (CMDB)



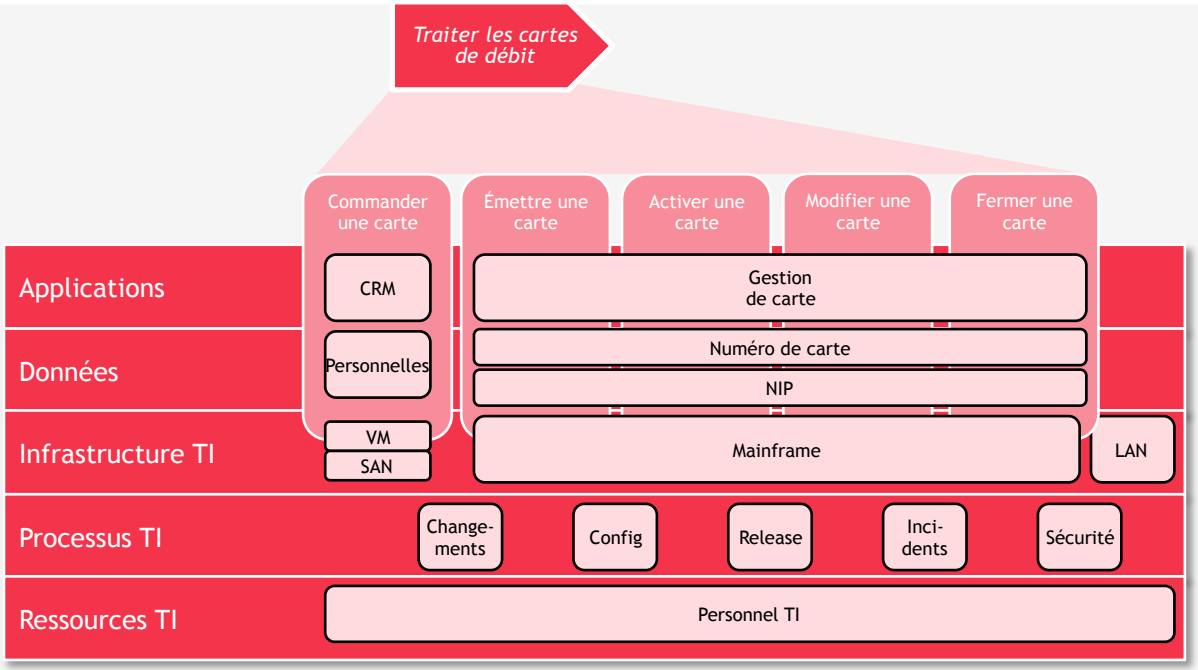
Approche "Top-Down "
(vision d'affaires)
Comment le processus est-il décomposé ?
(quels et combien d'actifs)

Approche "Bottom-up "
(vision opérationnelle TI)
Comment interagissent les actifs entre eux ?

Approche de gestion des risques TI des processus d'affaires

Illustration avec le processus de gestion des cartes de débit

1 Documentation processus, niveaux de service inventaire des actifs TI



- **Niveaux de services attendus sur le processus (criticité):**
  - *Disponibilité des services applicatifs:*
    - ✓ *Durée maximale d'interruption admissible (RTO): **1 h***
    - ✓ *Durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne (RPO): **1 h***
  - *Confidentialité et intégrité des données : **données personnelles, numéro de carte et NIP***

Cette analyse ne se veut pas exhaustive et permet uniquement d'illustrer nos propos

Approche de gestion des risques TI des processus d'affaires

Illustration avec le processus de gestion des cartes de débit

2 Identification des risques et contrôles

Risques TI *(tirés de l'univers des risques TI)*	Niveau de service	Actifs TI	#	Contrôles TI
Perte, vol, fuite d'informations, délibérée ou accidentelle	Confidentialité des donnés personnelles - forte	SAN argent (EMC)	1	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin
		Base de données Progress	2	Les données sont encryptées selon un protocole xxx
		Interfaces	3	Les interfaces de données en clair sont sécurisées selon un mode SHTP
	Confidentialité des donnés numéro de carte et NIP - ultra sensible	Stockage or (IBM)	4	Les disques de stockage sont situés dans un voute sécuritaire dédiée
			5	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin
		Base de données DB2	6	Les données sont encryptées selon un protocole WPA 256bits à clé publique
			7	Les copies de sauvegardes des données sont stockées dans une voute sécuritaire dédiée
		Interfaces	8	Les interfaces de données cryptées sont sécurisées selon un mode SHTP
Interruption ou dégradation du service	Disponibilité du service applicatif et de données 99,99%	Application CRM (Siebel)	9	La version 10.3 de Siebel en production est supportée par Oracle jusqu'en 2020 et bénéficie d'un contrat de maintenance annuel
			10	Le niveau de personnalisation de Siebel est de l'ordre de 5% et les précédents upgrades n'ont pas occasionné d'incident ou d'enjeu de non-régression
		VM Unix	11	La VM dédiée à Siebel dispose d'une capacité de 4 core, utilisés en moyenne à 45% dans les derniers 6 mois
			12	La VM est répliquée en temps réel sur un second site, en failover, selon une architecture miroir
		SAN argent (EMC)	13	L'infrastructure SAN est en mode RAID et est répliquée en temps réel sur un second site, en failover, selon une architecture miroir
			14	Le SAN est dédié pour une capacité de 50 GB et son utilisation est passée de 35% à 90% dans les 6 derniers mois
		Application Gestion de Carte (développement maison)	15	L'application de gestion de carte est écrite en COBOL et date des années 80. Elle dispose de 2 millions de lignes. La documentation d'affaires et technique est très limitée, l'expertise de développement COBOL est toujours présente à l'interne
		Mainframe (zOS)	16	Le MF est répliqué en temps réel sur un second site, en failover, selon une architecture miroir et garantit un niveau de service de 99.99%, insuffisante pour atteindre un niveau de service applicatif global de 99.99%
		Stockage or (IBM)	17	L'infrastructure de stockage dispose de disques redondants et est répliquée en temps réel sur un second site, en failover, selon une architecture miroir

Cette analyse ne se veut pas exhaustive et permet uniquement d'illustrer nos propos

Approche de gestion des risques TI des processus d'affaires

Illustration avec le processus de gestion des cartes de débit

3 Évaluation des risques et contrôles

Risques TI *(tirés de l'univers des risques TI)*	Niveau de service	Probabilité	Impact	Type d'impact	Risque inhérent	Actifs TI	#	Contrôles TI	Efficacité contrôles	Probabilité	Impact	Risque résiduel réel	Risque résiduel attendu
Perte, vol, fuite d'informations, délibérée ou accidentelle	Confidentialité des données personnelles - forte	Peu probable	Faible	Réputation	Très faible	SAN argent (EMC)	1	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin	Adéquat	Improbable	Très faible	Très faible	Très faible
						Base de données Progress	2	Les données sont encryptées selon un protocole xxx	Adéquat				
						Interfaces	3	Les interfaces de données en clair sont sécurisées selon un mode SHTP	Adéquat				
	Confidentialité des données numéro de carte et NIP - ultra sensible	Peu probable	Très élevé	Financier	Élevé	Stockage or (IBM)	4	Les disques de stockage sont situés dans un voute sécuritaire dédiée	Adéquat	Improbable	Modéré	Modéré	Faible
							5	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin	Inadéquat				
						Base de données DB2	6	Les données sont encryptées selon un protocole WPA 256bits à clé publique	Adéquat				
							7	Les copies de sauvegardes des données sont stockées dans une voute sécuritaire dédiée	Adéquat				
						Interfaces	8	Les interfaces de données cryptées sont sécurisées selon un mode SHTP	Partiel				
Interruption ou dégradation du service	Disponibilité du service applicatif et de données 99,99%	Probable	Très élevé	Financier	Très élevé	Application CRM (Siebel)	9	La version 10.3 de Siebel en production est supportée par Oracle jusqu'en 2020 et bénéficie d'un contrat de maintenance annuel	Adéquat	Probable	Élevé	Élevé	Très faible
							10	Le niveau de personnalisation de Siebel est de l'ordre de 5% et les précédents upgrades n'ont pas occasionné d'incident ou d'enjeu de non-régression	Adéquat				
						VM Unix	11	La VM dédiée à Siebel dispose d'une capacité de 4 core, utilisés en moyenne à 45% dans les derniers 6 mois	Adéquat				
							12	La VM est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	Adéquat				
						SAN argent (EMC)	13	L'infrastructure SAN est en mode RAID et est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	Adéquat				
							14	Le SAN est dédié pour une capacité de 50 GB et son utilisation est passée de 35% à 90% dans les 6 derniers mois	Inadéquat				
						Application Gestion de Carte (développement maison)	15	L'application de gestion de carte est écrite en COBOL et date des années 80. Elle dispose de 2 millions de lignes. La documentation d'affaires et technique est très limitée, l'expertise de développement COBOL est toujours présente à l'interne	Partiel				
						Mainframe (zOS)	16	Le MF est répliqué en temps réel sur un second site, en failover, selon une architecture miroir et garantit un niveau de service de 99.99%, insuffisante pour atteindre un niveau de service applicatif global de 99.99%	Inadéquat				
						Stockage or (IBM)	17	L'infrastructure de stockage dispose de disques redondants et est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	Inadéquat				

Le service de gestion de carte a été indisponible 3 fois dans les 6 derniers mois pendant une durée de 3 heures en moyenne

Cette analyse ne se veut pas exhaustive et permet uniquement d'illustrer nos propos

Approche de gestion des risques TI des processus d'affaires

Illustration avec le processus de gestion des cartes de débit

4 **Stratégies de réponse et plans d'action**

Risques TI *(tirés de l'univers des risques TI)*	Niveau de service	Actifs TI	#	Contrôles TI	Efficacité contrôles	Probabilité	Impact	Risque résiduel réel	Risque résiduel attendu	Stratégie de réponse	Plan d'actions
Perte, vol, fuite d'informations, délibérée ou accidentelle	Confidentialité des données personnelles - forte	SAN argent (EMC)	1	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin	Adéquat	Improbable	Très faible	Très faible	Très faible	*Accepter*	-
		Base de données Progress	2	Les données sont encryptées selon un protocole xxx	Adéquat						-
		Interfaces	3	Les interfaces de données en clair sont sécurisées selon un mode SHTP	Adéquat						-
	Confidentialité des données numéro de carte et NIP - ultra sensible	Stockage or (IBM)	4	Les disques de stockage sont situés dans un voute sécuritaire dédiée	Adéquat	Improbable	Modéré	Modéré	Faible	Atténuer	-
			5	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin	Inadéquat						Configurer les disques de sauvegarde avec une double authentification (user ID + psw + jeton RSA) pour l'accès des SysAdmin
		Base de données DB2	6	Les données sont encryptées selon un protocole WPA 256bits à clé publique	Adéquat						-
			7	Les copies de sauvegardes des données sont stockées dans une voute sécuritaire dédiée	Adéquat						-
		Interfaces	8	Les interfaces de données cryptées sont sécurisées selon un mode SHTP	Partiel						Crypter les interfaces selon le protocole WPA 256bit à clé publique
Interruption ou dégradation du service	Disponibilité du service applicatif et de données 99,99%	Application CRM (Siebel)	9	La version 10.3 de Siebel en production est supportée par Oracle jusqu'en 2020 et bénéficie d'un contrat de maintenance annuel	Adéquat	Probable	Élevé	Élevé	Très faible	Atténuer	-
			10	Le niveau de personnalisation de Siebel est de l'ordre de 5% et les précédents upgrades n'ont pas occasionné d'incident ou d'enjeu de non-régression	Adéquat						-
		VM Unix	11	La VM dédiée à Siebel dispose d'une capacité de 4 core, utilisés en moyenne à 45% dans les derniers 6 mois	Adéquat						-
			12	La VM est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	Adéquat						-
		SAN argent (EMC)	13	L'infrastructure SAN est en mode RAID et est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	Adéquat						-
			14	Le SAN est dédié pour une capacité de 50 GB et son utilisation est passée de 35% à 90% dans les 6 derniers mois	Inadéquat						- Augmenter la capacité du stockage à 200GB - Mettre en œuvre un monitoring de la capacité du SAN et un kpi au comité de gestion TI
		Application Gestion de Carte (développement maison)	15	L'application de gestion de carte est écrite en COBOL et date des années 80. Elle dispose de 2 millions de lignes. La documentation d'affaires et technique est très limitée, l'expertise de développement COBOL est toujours présente à l'interne	Partiel						- Documenter les fonctionnalités d'affaires de l'application - Mesurer la stabilité de l'application de façon régulière
		Mainframe (zOS)	16	Le MF est répliqué en temps réel sur un second site, en failover, selon une architecture miroir et garantit un niveau de service de 99.99%, insuffisante pour atteindre un niveau de service applicatif global de 99.99%	Inadéquat						Mettre en place une architecture de balance de charge ("load balancing") entre les 2 sites miroir
		Stockage or (IBM)	17	L'infrastructure de stockage dispose de disques redondants et est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	Inadéquat						

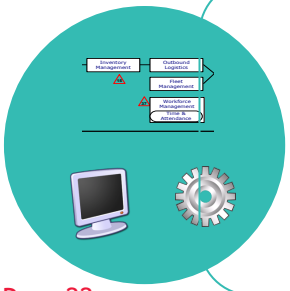
Cette analyse ne se veut pas exhaustive et permet uniquement d'illustrer nos propos

Approche de gestion des risques TI des processus d'affaires

Illustration avec le processus de gestion des cartes de débit

5 Modification des processus TI source

Risques TI *(tirés de l'univers des risques)*	Niveau de service	Actifs TI	#	Contrôles TI	Plan d'actions	Processus TI en jeu
Perte, vol, fuite d'informations, délibérée ou accidentelle	Confidentialité des donnés personnelles - forte	SAN argent (EMC)	1	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin	-	-
		Base de données Progress	2	Les données sont encryptées selon un protocole xxx	-	-
		Interfaces	3	Les interfaces de données en clair sont sécurisées selon un mode SHTP	-	-
	Confidentialité des donnés numéro de carte et NIP - ultra sensible	Stockage or (IBM)	4	Les disques de stockage sont situés dans un voute sécuritaire dédiée	-	-
			5	Les disques de sauvegarde sont configurés avec une authentification normale (user ID + psw) pour l'accès des SysAdmin	Configurer les disques de sauvegarde avec une double authentification (user ID + psw + jeton RSA) pour l'accès des	Gestion des accès
		Base de données DB2	6	Les données sont encryptées selon un protocole WPA 256bits à clé publique	-	-
			7	Les copies de sauvegardes des données sont stockées dans une voute sécuritaire dédiée	-	-
		Interfaces	8	Les interfaces de données cryptées sont sécurisées selon un mode SHTP	Crypter les interfaces selon le protocole WPA 256bit à clé publique	Gestion de la sécurité
Interruption ou dégradation du service	Disponibilité du service applicatif et de données 99,99%	Application CRM (Siebel)	9	La version 10.3 de Siebel en production est supportée par Oracle jusqu'en 2020 et bénéficie d'un contrat de maintenance annuel	-	-
			10	Le niveau de personnalisation de Siebel est de l'ordre de 5% et les précédents upgrades n'ont pas occasionné d'incident ou d'enjeu de non-régression	-	-
		VM Unix	11	La VM dédiée à Siebel dispose d'une capacité de 4 core, utilisés en moyenne à 45% dans les derniers 6 mois	-	-
			12	La VM est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	-	-
		SAN argent (EMC)	13	L'infrastructure SAN est en mode RAID et est répliquée en temps réel sur un second site, en failover, selon une architecture miroir	-	-
			14	Le SAN est dédié pour une capacité de 50 GB et son utilisation est passée de 35% à 90% dans les 6 derniers mois	- Augmenter la capacité du stockage à 200GB - Mettre en oeuvre un monitoring de la capacité du SAN et un kpi au comité de gestion TI	Gestion de la capacité - SDLC / Gestion de projet (livrable d'architecture de solution)
		Application Gestion de Carte (développement maison)	15	L'application de gestion de carte est écrite en COBOL et date des années 80. Elle dispose de 2 millions de lignes. La documentation d'affaires et technique est très limitée, l'expertise de développement COBOL est toujours présente à l'interne	- Documenter les fonctionnalités d'affaires de l'application - Mesurer la stabilité de l'application de façon régulière	Gestion des incidents
		Mainframe (zOS)	16	Le MF est répliqué en temps réel sur un second site, en failover, selon une architecture miroir et garantit un niveau de service de 99.99%, insuffisante pour atteindre un niveau de service applicatif global de 99.99%	Mettre en place une architecture de balance de charge ("load balancing") entre les 2 sites miroir	Gestion de la capacité - SDLC / Gestion de projet (livrable d'architecture de solution)
		Stockage or (IBM)	17	L'infrastructure de stockage dispose de disques redondants et est répliquée en temps réel sur un second site, en failover, selon une		

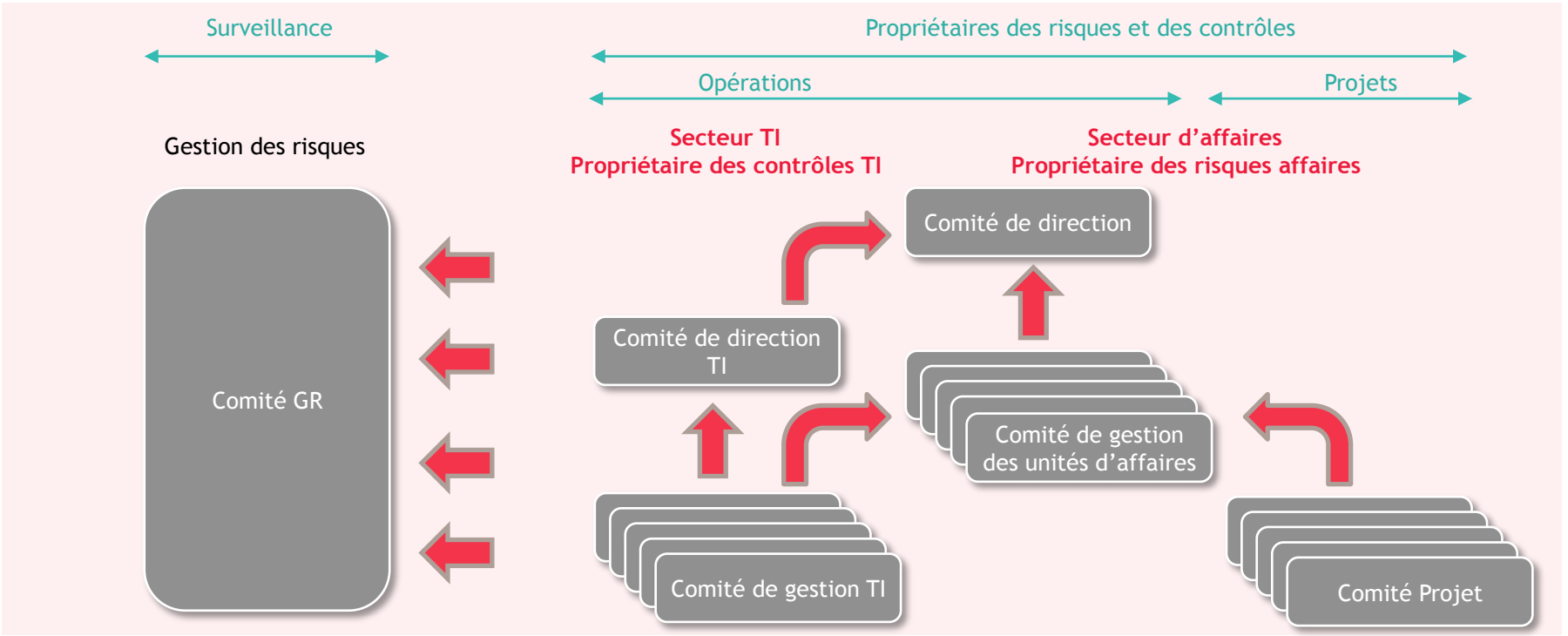


- En réalisant l'analyse de risques TI sur les actifs TI supportant des processus d'affaires, il est possible:
  - *D'identifier certains risques technologiques non identifiés*
  - *De constater une mauvaise gestion de ces actifs et/ou une mauvaise conception des contrôles TI, entrainant un mauvais fonctionnement du processus TI dans sa globalité*
- Ces processus et contrôles TI pourront ainsi être optimisés afin d'assurer une meilleure standardisation de leurs « extrants », servant de support aux processus d'affaires

Cette analyse ne se veut pas exhaustive et permet uniquement d'illustrer nos propos

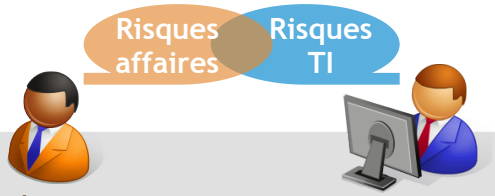
Gouvernance de la gestion des risques TI des processus d'affaires

Une **meilleure collaboration** entre les secteurs d'affaires et TI passe par une **reddition de comptes commune** aux instances de gestion des risques et de conformité et la présence de **représentants TI aux comités des secteurs d'affaires** pour adresser les aspects de risques technologiques



4.
CONCLUSION

Une meilleure collaboration affaires/TI nécessaire



- La démarche croisée affaires/TI s'inscrit réellement dans une **optique d'amélioration continue** à ne pas négliger
- Les secteurs d'affaires et TI ont tout intérêt à **collaborer davantage** sur leur manière de gérer leurs risques, et à agir sur un **mode préventif plutôt que réactif**
- **Les TI représentent un mandataire clé** de beaucoup de processus d'affaires; il convient donc de **les intégrer dans la gestion opérationnelle** des processus d'affaires et de sortir progressivement d'un mode de gestion par projet
- Le rôle des secteurs d'affaires, et plus particulièrement celui des **propriétaires des processus d'affaires**, est d'établir une **collaboration durable et continue avec les TI.** Et ce, dans le but de toujours être **au fait des évolutions TI** et ne pas les découvrir lors de problèmes ou d'incidents
- **Connaitre les évolutions TI**, et **surtout celles des actifs supportant leurs processus d'affaires**, leur permettra d'**identifier en amont les impacts** potentiels sur ces processus
- Les propriétaires pourront ainsi **ajuster leur évaluation** des risques, **modifier les contrôles** en place et ainsi **mieux minimiser leurs risques**

Avec vous ce matin

ÉRIC AUBAILLY, MBA
DIRECTEUR EXÉCUTIF, SERVICES-CONSEILS TI

Profil

- Éric est directeur exécutif à notre bureau de Montréal, leader national services-conseils en TI. Il possède plus de 25 années d'expérience professionnelle en Europe, au Moyen-Orient et au Canada, dont 19 années en services-conseils en TI (audit interne, conformité TI, gestion des risques TI, services-conseil stratégiques TI). Il a mené de nombreux mandats d'audit interne TI et de projets et a notamment assuré, en mode co-sourcing, la direction de l'audit interne TI pour un grand distributeur d'outillage pendant 7 ans

- Auparavant, Éric avait assumé les fonctions de contrôleur international puis de Vice-président Finance & Administration pour un manufacturier en télécommunications

Coordonnées

- eaubailly@bdo.ca
- Cell: 514-928-9751

DIANE FUGÈRE, CPA, CA

VICE-PRÉSIDENTE, BUREAU DE QUÉBEC, SERVICES-CONSEILS

Profil

Diane est vice-présidente du bureau de Québec de BDO Canada. Comptable professionnel agrée elle possède plus de 25 ans d'expérience professionnelle dont 15 années en services-conseils. Au cours de ces années, elle a développé une solide expertise en gestion du risque et des contrôles, en révision et amélioration des processus de gestion, et en réalisation de diagnostic organisationnel.

La diversité de ses interventions lui a permis de développer une capacité d'adaptation rapide à de nouveaux environnements. Ainsi, au cours de sa carrière, elle a réalisé de multiples interventions auprès de ministères et organismes provinciaux et fédéraux. Elle est aussi intervenue auprès d'entreprises de services, dans les secteurs du transport de marchandises et de personnes, de la construction, de l'automobile, du manufacturier ainsi que du commerce au détail. Le client est au cœur de ses interventions.

Coordonnées

- dfugere@bdo.ca
- bureau: 418-658-6915