Historique de la gestion des risques

Cours #1

CF 170 Gestion des risques de l'information

Polytechnique Montréal

Pierre-Luc Pomerleau, MBA

Mes coordonnées

Adresse courriel: pierre-luc-2.Pomerleau@polymtl.ca

Numéro de téléphone : 514-717-9670

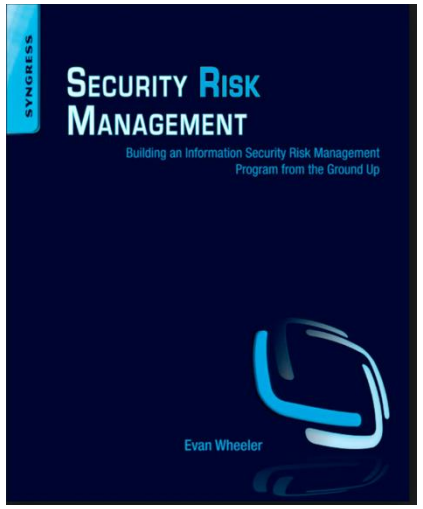
Méthode de communication: courriel pour questions et prise de rendez-vous au besoin

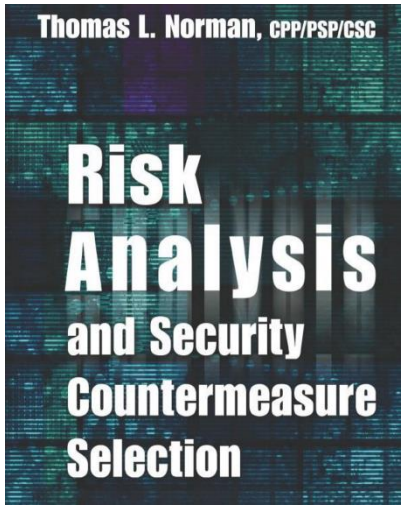
3

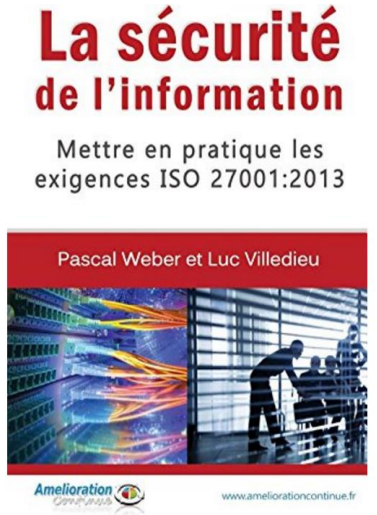
Mon expérience professionelle
&
Déroulement du cours

Les livres recommandés et description du plan de cours

4







Norman, T. L. (2010). *Risk Analysis and Security Countermeasure Selection*. Boca Raton: CRC Press

Weber, P., Villedieu, L. (2014). *La sécurité de l'information : mettre en pratique les exigences ISO 27001 : 2013*. Retrouvé sur le lien :https://www.amazon.ca/s%C3%A9curit%C3%A9-linformation-Mettre-pratique-exigences/dp/1502713098/ref=sr_1_1?s=books&ie=UTF8&qid=1499783858&sr=1-1&keywords=securite+de+l%27information

Wheeler, E. (2011). *Security risk management; building an information security risk management from the ground up*. Waltham, MA. Syngress.

Objectif d'apprentissage

- L'étudiant sera en mesure de:
  - Comprendre l'origine de la gestion de risque
  - Comprendre la notion de risque dans les différents domaines
  - Comprendre les grands événements qui définissent l'histoire du domaine

Perspectives historiques

L'analyse de risque et la gestion des risques sont utilisés aujourd'hui dans de nombreux domaines où les risques représentent une préoccupation importante.

Au sein d'une organisation publique, privée ou même d'un gouvernement, nous sommes de plus en plus confrontés à des enjeux variés, notamment, à l'égard de la sécurité des personnes, de l'information et des biens.

La gestion des risques s'impose donc comme une solution pour faire face de façon méthodique aux risques et aux conséquences potentielles leur étant associées.

C’est au milieu de l’assurance que l’on doit le développement, au cours des années 1960 et 1970, du concept de gestion de risques. Avec l’objectif de réduire les pertes, les compagnies d’assurance ont commencé à cette époque à inciter leurs clients commerciaux à accroître la sécurité de leurs installations contre les risques extérieurs à l’entreprise.

Par la suite, la gestion des risques s’est étendue à d’autres aspect du fonctionnement des entreprises tels que la santé et la sécurité au travail et l’adoption de spécifications visant à assurer la qualité des produits fabriqués.

Assurances

- Dans le domaine de l'assurance, le risque est défini comme étant :
  - « Événement, préjudice aléatoire, indépendant de la volonté des personnes, contre la survenance duquel l'assuré veut se prémunir. »

- Assurance:
  - Contrat par lequel une partie (l'assuré) se fait promettre moyennant une rémunération (la prime), pour lui ou pour un tiers, une prestation par une autre partie (l'assureur) qui, prenant en charge un ensemble de risques, les compense en cas de réalisation d'un événement préjudiciable (décès, incendie, accident, etc.). [Institut Canadien des Comptables Agréés, 2006]

Au tournant des années 1990, devant les évidences toujours plus grandes de l'impact des activités humaines sur le milieu naturel, les préoccupations se sont aussi portées sur la protection de l'environnement.

La gestion des risques abordée dans une perspective globable et systémique comme on la connaît aujourd'hui, s'est développée à partir du milieu des années 1990.

L'analyse et la gestion des risques sont maintenant utilisées dans une multitude de domaines d'activités tels que ceux associées aux investissements, aux placements et à la vérification. Son utilisation en matière de sécurité civile pour gérer les risques de sinistres remonte à moitié des années 1990.

10

Dans un monde de plus en plus complexe où les interdépendances entre les différents éléments de fonctionnement de nos sociétés sont en constante augmentation, un consensus s'établit désormais selon lequel ***une gestion efficace des risques nécessite de briser les silos et d'adopter une perspective globale, systémique et permanente.***

L'approche récente de gestion des risques s'appuie sur l'idée que la préoccupations et les enjeux relatifs aux risques sont l'affaire de tous.

Chaque membre d'une société ou d'une organisation doit donc se sentir concerné par les risques et leurs conséquences potentielles

11

"La gestion des risques est une pratique solidement établie au sein des secteurs de l'assurance, du génie, des finances et du risque politique. Il est clair cependant que la gestion des risques manque relativement de maturité dans la façon dont elle est appliquée dans le domaine de sécurité intérieure. Certains pourraient faire valoir que la mise en oeuvre de l'évaluation et de la gestion des risques dans le domaine de la sécurité intérieure et du contre-terrorisme est sans doute plus complexe que dans ses applications industrielles dont l'objectif primordial est de protéger les gens contre les pertes financières".

Department of Homeland Security's Risk Assessment Methodology : Evolution, Issues, and Option for Congress. Congressional Research Service. Février 2007

Principes

L’analyse des risques associés à l’information est essentielle à plusieurs niveaux:

Entreprises publiques, privées;

- ✓ International
- ✓ National
- ✓ Provincial
- ✓ Territorial
- ✓ Gouvernemental
- ✓ Organisationnel

Les organisations prennent un certain nombre de mesures afin d'atténuer les risques de leurs activités en combinant:

La planification stratégique
L'évaluation des risques
La planification et la gestion des urgences
Les méthodes et continuité des opérations
Les mesures de sécurité

14

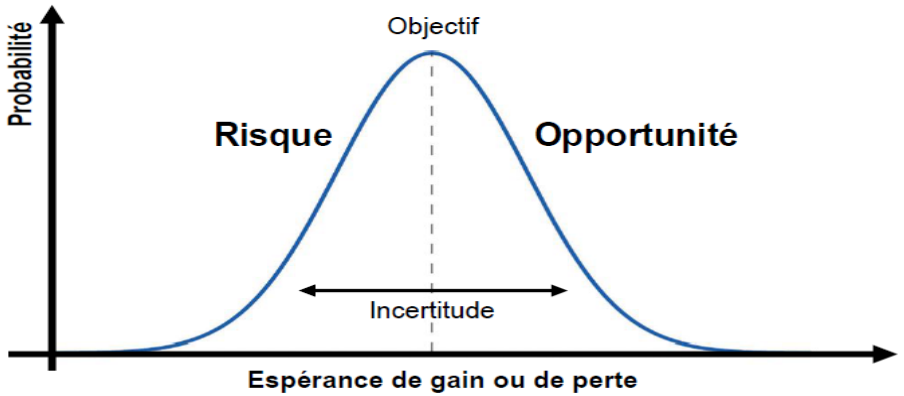
Malgré ces mesures, d'importantes lacunes persistent au sein de certaines organisations….

Risque

- Grec:
  - « rhiza »; relatif à la navigation autour d'une falaise.
- Pourquoi parle t-on de risque ?
  - Pour orienter la prise de décision
  - Arrimer ce que nous savons avec ce que nous jugeons pour atteindre l'objectif

Risque

- Définition :
  - Probabilité que survienne un événement nuisible et éventualité qu'existe une menace plus ou moins prévisible pouvant influer sur la réalisation des objectifs d'une organisation [Office québécois de la langue française (OQLF)]
  - Effet de l'incertitude sur l'atteinte des objectifs [ISO Guide 73]



Assurances

- Types d'assurance disponibles:
  - Assurance collective, assurance crédit, assurance des titres de propriété, assurance détournement et vol, assurance dommages, assurance globale, assurance individuelle, assurance invalidité, assurance maladie, assurance mixte, assurance multirisque, assurance personne-clé, assurance perte d'exploitation, assurance rachat de parts, assurance responsabilité civile, assurance responsabilité civile professionnelle, assurance risques divers, assurance tous risques, assurance vie, assurance vie avec participation, assurance vie entière, assurance vie temporaire, assurance-dépôts,

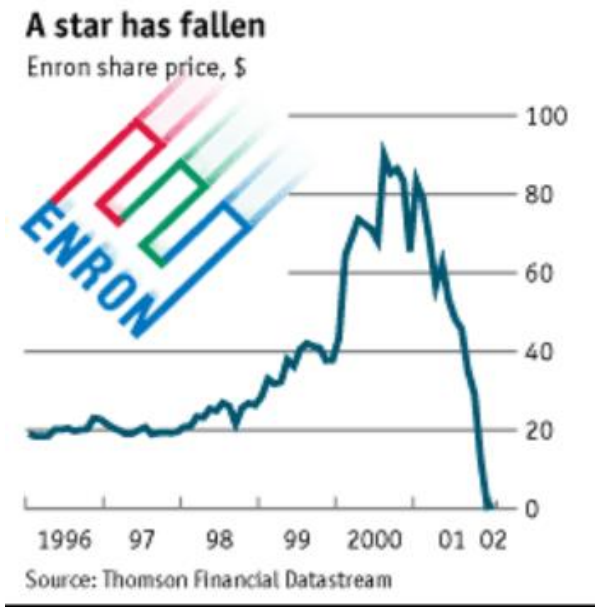
Risque dans le domaine financier

- Dans les entreprises, la gestion du risque financier se présente habituellement en trois catégories, soient:
  - risque de crédit
  - risque de marché
  - risque de liquidité

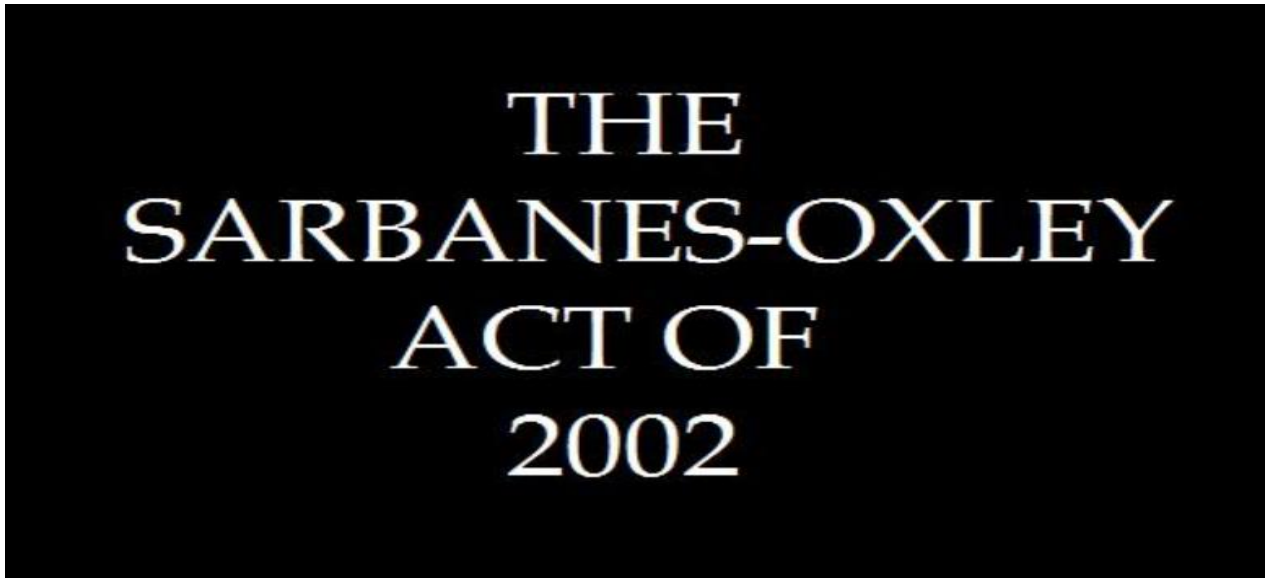
Risque financier - fraude

Gestion des risques financier – Accord de Bâle

Scandales financiers



Scandales financiers - réglementation



Notation du credit – gestion des cotes de crédit

Fitch Ratings

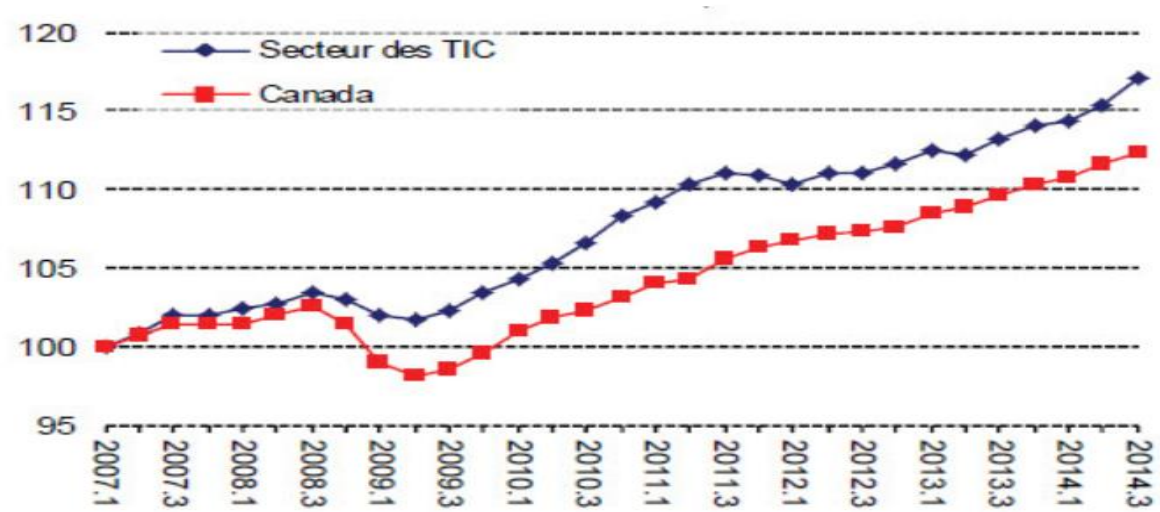
S&P Global
Ratings

Risque opérationnel

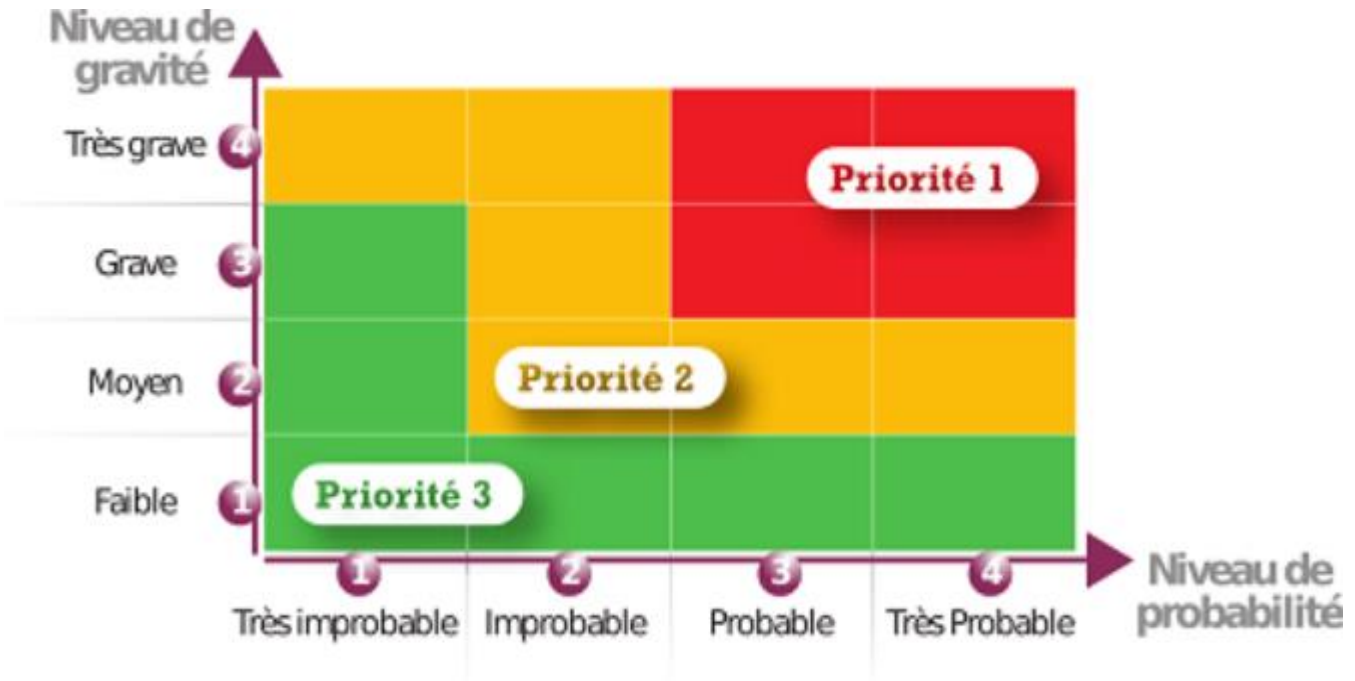
Risque opérationnel

Risque et technologie de l'information

Figure 1 : PIB réel : Secteur des TIC et économie canadienne, indice de croissance, 2007T1 = 100



Risque de projet



Risque de réputation

28

Risque de sécurité de l’information

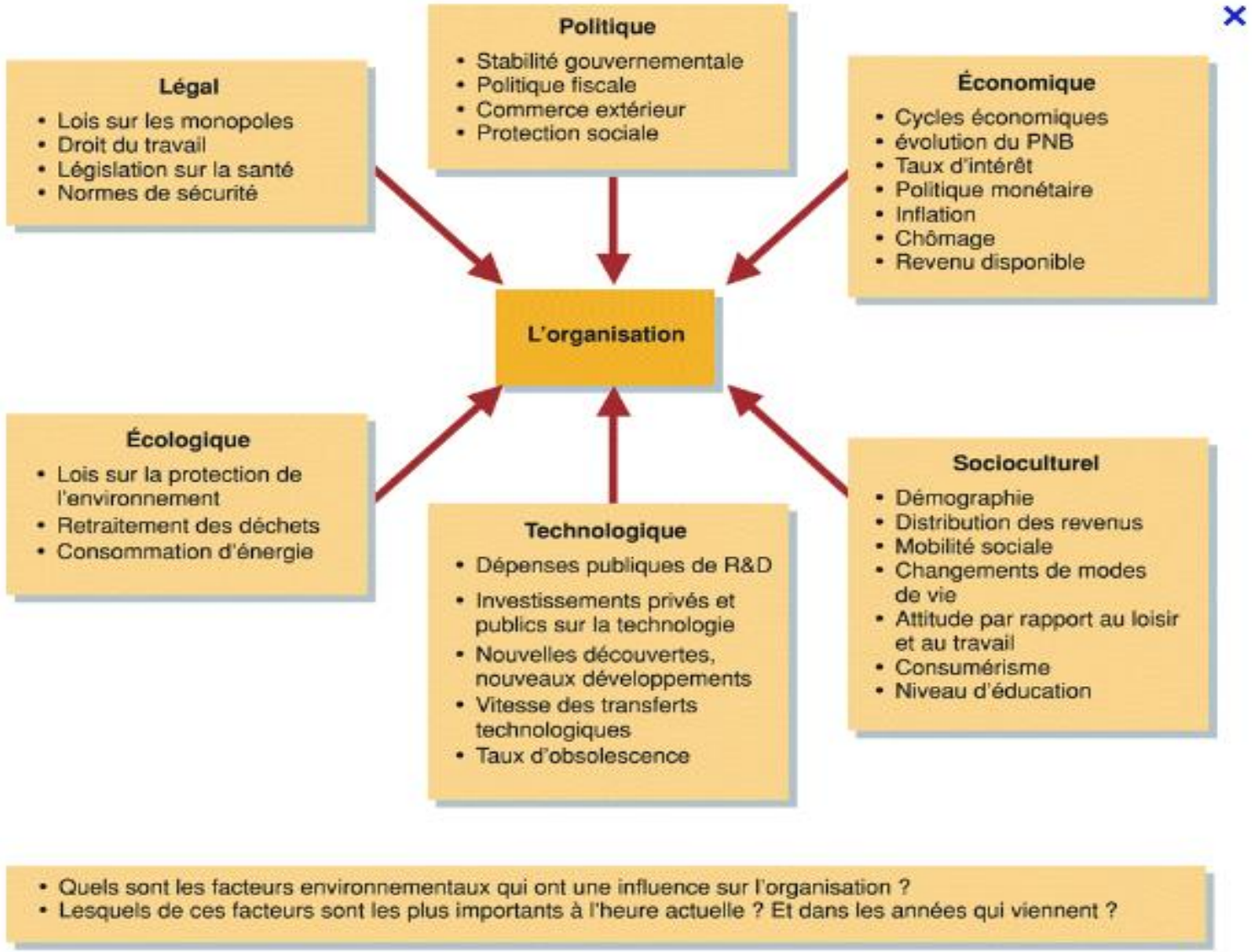
Les cyberattaques

Analyser l'environnement externe et interne de l'organisation : Le PESTEL, les Parties Prenantes & FFOM

Connaître l'organisation

- L'analyse de la situation prend du temps et de l'énergie mais cette étape est la base d'une évaluation adéquate de l'organisation:
- Mission, Vision et Valeurs de l'organisation
- Objectifs stratégiques, tactiques et opérationnels
- Les activités de l'organisation
- Les politiques et procédures
- Réglementations
- Responsabilités de la sécurité des personnes, des biens et de l'information
- Qui fait quoi au sein de l'organisation
- Relations de travail (syndicat?)
- Santé et Sécurité
- Aspects Légaux

Quelques outils pour bien connaître l'environnement de l'organisation, ses forces & ses faiblesses



© Pearson Education France

Le Pestel

- PESTEL Consiste à identifier les facteurs :

- Politiques,
- Économiques,
- Sociaux,
- Technologiques
- Environnementaux et
- Légaux

Politique

- Force du gouvernement (minoritaire?)
- Lois reliées à la compétition
- Politiques de taxation
- Dépenses de l'État
- Privatisation
- Régulation des marchés financiers
- Lois du travail
- Accords bilatéraux et multilatéraux

Économique

- Taux d'intérêt
- Taux de change
- Déficit-surplus budgétaire
- Déficit, surplus commercial
- Inflation
- PNB ou PIB/capita
- Revenu, dépenses et niveaux de dette du consommateur
- Chômage
- Productivité de la main-d'œuvre
- Taux d'épargne

Socio culturel

Culture:

- Coutumes distinctives
- Façons d'être
- Rites
- Réussites
- Héros
- Produits
- Récompenses et sanctions
- Les manières de vivre, d'être d'un pays, région

Société:

- Population
- Âge, croissance
- Groupe ethnique
- Famille
- Style, niveau de vie
- Mobilité sociale
- Éducation
- Religion
- Attitude vis-à-vis le travail, la technologie

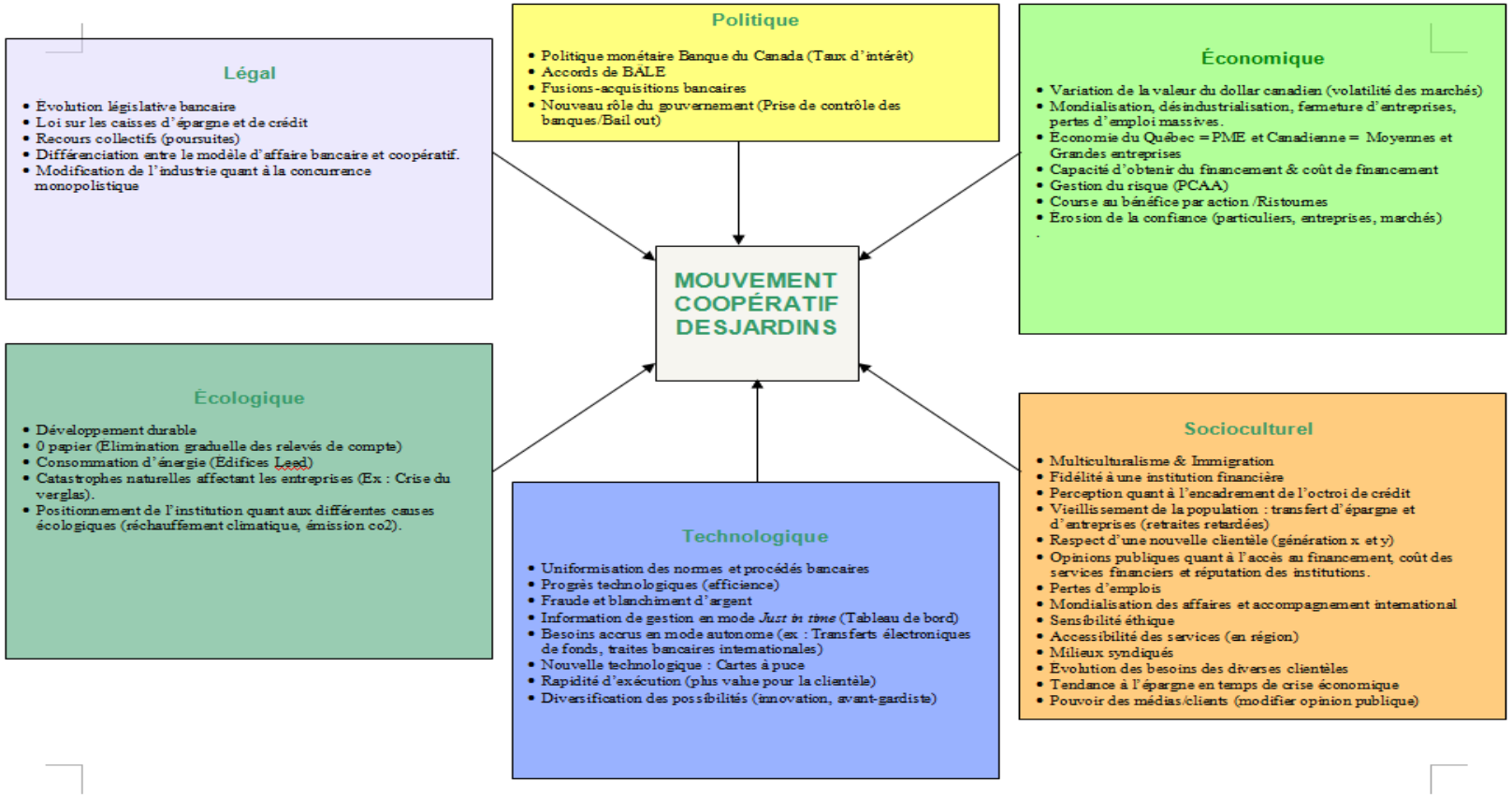
Technologie

- Technologie de l'information
- Dépenses en R&D
- Nouveaux produits
- Grappes industrielles
- Fabrication, robotique
- Transport
- Internet
- Nouvelles technologies
- Ruptures
- Biotechnologie
- Médecine

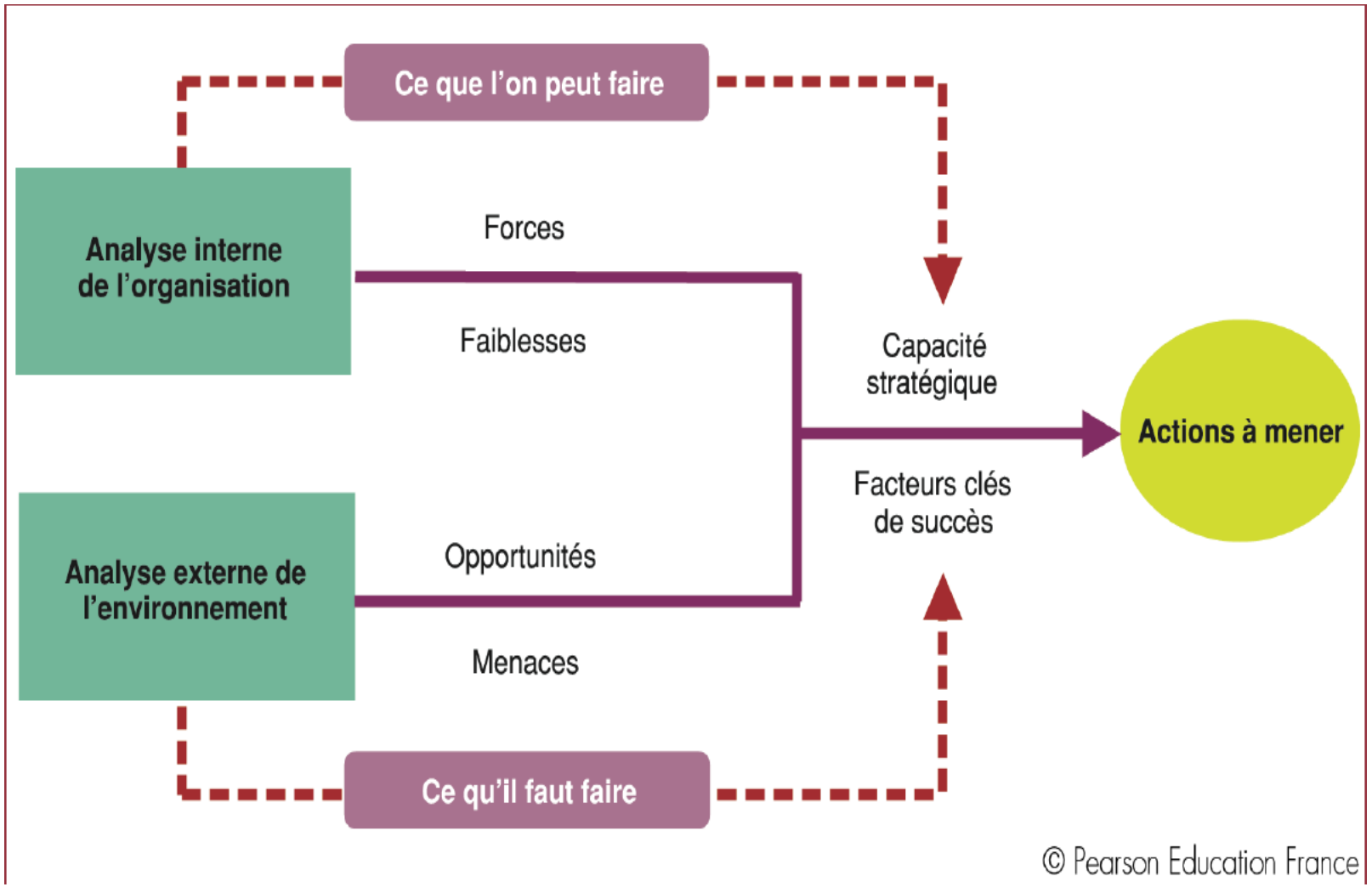
Légal

- Cadres légaux
- État de droit (lois, tribunaux, sanctions)
- Normes réglementaires
- Lois sur les monopoles
- Pratiques commerciales
- Protection du consommateur

Exemple d'un Pestel



L'analyse FFOM ou SWOT



SWOT et matrice de confrontation

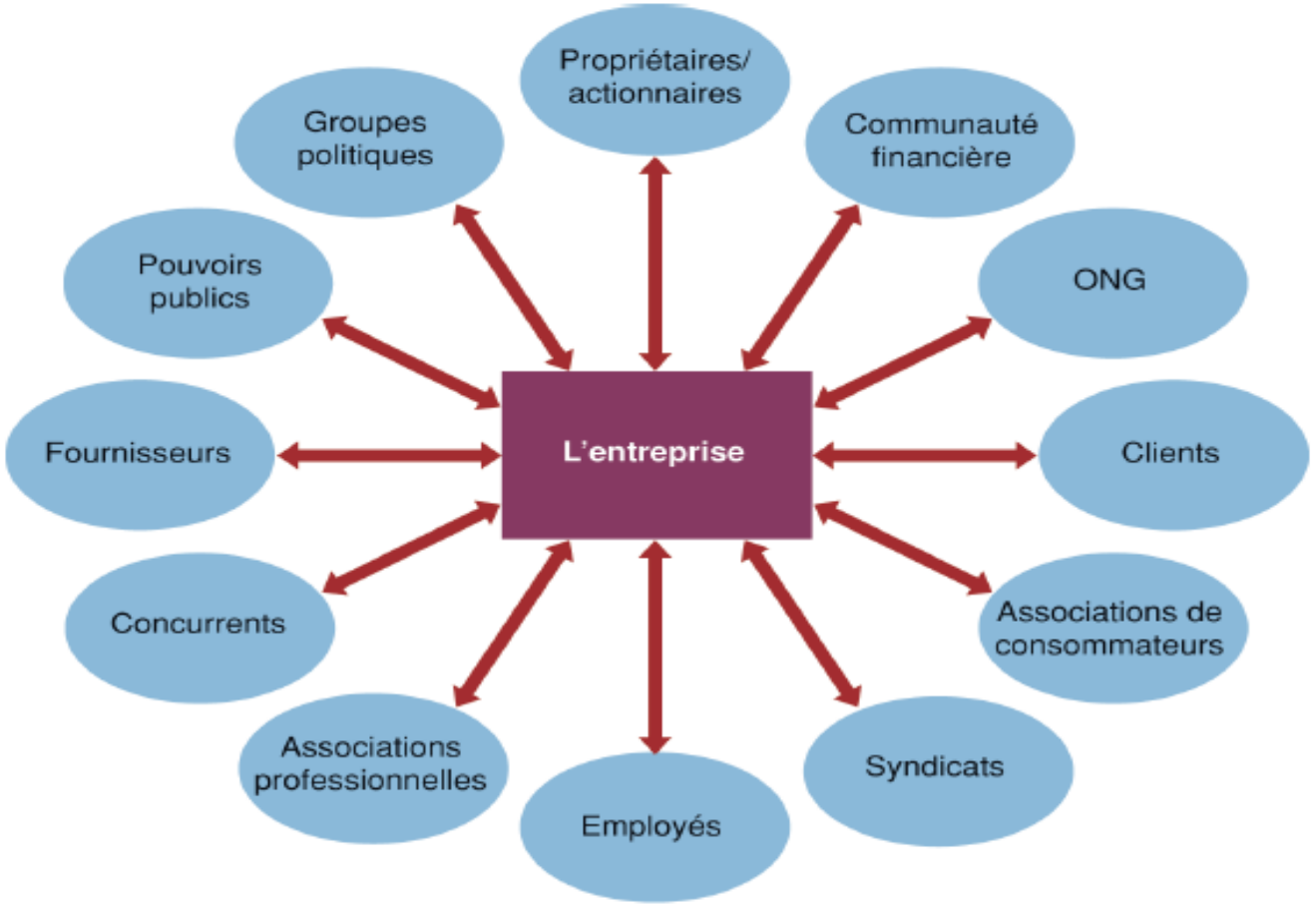
	Opportunités	Menaces (Threats)
Points forts (Strenghts)	Attaque	Défense
Faiblesse (Weaknesses)	Ajustement	Survie

Exemple d'une analyse FFOM

ANALYSE FFOM	
FORCES	**FAIBLESSES**
1. Aménagement (la cours à bois avec l'accès avec leur auto) 2. Nombre de produits 3. Service à la clientèle 4. Modèle d'affaires unique 5. Fortement ancrée sur le marché québécois (Parts de marché au Québec) 6. Croissance annuelle de son chiffre d'affaires 7. Management ; Vision de son PDG 8. Croissance organique, intégration et acquisition 9. Pouvoir d'achat 10. Programme de financement Accord D de Desjardins 11. Programme de fidélisation Air Miles 12. Engagement social (Prix de distinctions) 13. Politique en matière d'achats écologiques et développement durable 14. Respect des employés et gestion de la relève (30% des employés de Rona ont plus de 50 ans) 15. Notoriété	1. Certains employés sont syndiqués 2. Perte de profitabilité crise économique 3. Productivité des centres de distribution (rejoindre régions éloignées/transport) 4. Ventes par magasins comparables 5. Coût de la main-d'œuvre 6. Coûts liés aux inventaires et logistiques 7. Position de marché actuelle Ontario et Ouest
OPPORTUNITÉS	**MENACES**
1. Acquisitions de franchisés provinces canadiennes (Ontario et Ouest) et optimisation des actifs. 2. Reprise économique au Canada 3. Augmentation parts de marché par la croissance client 4. Développer le marché commercial et professionnel au Canada (Bannière Noble Trade) 5. Faible taux d'intérêt de la Banque du Canada (augmentation des constructions et achats de propriétés) 6. Optimisation chaîne d'approvisionnement et TIC 7. Avantage compétitif; recrutement de marchés affiliés indépendants qui s'approvisionnent aux centres de distributions Rona (Partenariats avec les marchands) 8. Exploitation de magasins grandes surfaces et de proximité	1. Fusion-acquisition par autre joueur du marché 2. L'économie canadienne et américaine 3. Capacité d'importation 4. Diversité des produits de la concurrence (outils, pièces secteur automobile électroménager, etc.) 5. d'installation limitée et récente. 6. Concurrence directe et indirecte en croissance (Parts de marchés, nouveaux produits & services) (Arrivée de Lowe's et croissance Home Dépôt) 7. Augmentation des taux d'intérêt de la Banque du Canada 8. Économie canadienne et américaine 9. Retard des fournisseurs provenant de l'extérieur du Canada (Chine, etc.) 10. Innovation du commerce électronique au niveau des produits de rénovation 11. Épidémie affectant le bois (Ex. : Tordeuse d'épinette)

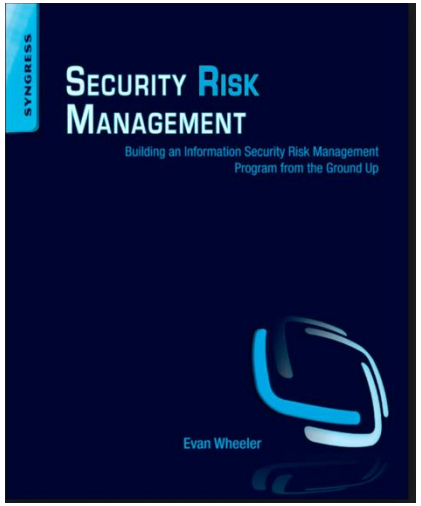
15

Les parties prenantes



© Pearson Education France

Lecture pour le prochain cours Chapitre 1; The security evolution



Avez-vous des questions?