

How to build a company risk profile: a methodology based upon the risks disclosed by Fortune 500 companies

C. Dumitriu

*School of Management Science,
University of Quebec in Montreal (UQAM), Canada*

Abstract

In the volatile environment in which we are living, new risks can emerge faster than our ability to manage them. The purpose of this paper is to present a framework for identifying the *total risk of a company*. Our model is based upon specific criteria organized in a *data collection instrument* (DCI) that researchers and managers could use to gather information on potential risks, and to select relevant risks for building the enterprise risk-profile. This paper presents the structure of our DCI, including a descriptive analysis of all incorporated risk categories, followed by the global, cross-sector and inter-sector results from our DCI verification, using the risks disclosed by Fortune 500 companies (2004).

Keywords: risk categories, risk identification, risk disclosure, company risk profile, Fortune 500 companies.

1 Introduction

The scientific community is rather divided in its approach towards risk management. Advocates of the market risk model focus exclusively on analysing the systematic risk, assuming that investors can eliminate specific risk through a diversified portfolio. Advocates of the strategic risk model adopt a different view, that of company managers, and thus focus instead on the total risk of the enterprise.

In one of our previous researches, we adopted the *market risk* model, assuming that a portfolio's return depends solely of the ex-ante measure of its beta. We investigated the ex post risk-return relationship for the Fortune 500 companies for the period 2000 to 2003. Almost all of these high performing



companies assumed high risks, in managing large international operations in various sectors rated by Coface as being “high-risk sectors”. Consequently, we hoped to find empirical evidence of a positive relationship between expected return and risk. Our results indicated that this relationship, while positive but not statistically significant for the entire Fortune 500 sample, was in fact negative and consistently significant for some sectors. These results were not consistent with the Capital Asset Pricing Model, but were confirming, to a certain extent, the paradox of Bowman.

As a consequence, we have taken a complementary position in this study, and adopted a strategic approach to risk that focuses on *total company risk*. We sought to answer a number of questions. What are the complex risks that constitute the “total risk” and how are they interrelated? What are their main sources? Are they different from one sector to another, and if so, how? Is management taking a holistic view of these risks and of the way in which these risks correlate, or do they only pay attention to the main sources of systematic risk?

2 Purpose

In order to successfully assess risks, managers and researchers need accurate and complete information of all the categories of potential risks, organized in a single comprehensive picture. Appropriate risk categories for such a framework should meet two important criteria: (1) each risk category should represent a collection of non-redundant risks that are well defined according to their various sources; and (2) each risk category should eventually be cross-referenced to several other interrelated risk categories. Such a holistic approach to risk should also consider new risk categories that have emerged in recent times in response to new network economies and business models, as omitting certain “new-age” risks could lead to skewed results in the risk assessment process.

The purpose of this paper is to present a framework for identifying the *total risk* of a company. Our framework is based upon specific criteria organized in a *data collection instrument* (DCI), which could be used by researchers and managers to effectively gather information on potential risks, and to select relevant risks for the enterprise risk-profile. This paper presents the structure of our DCI, including a descriptive analysis of all incorporated risk categories. Furthermore, it presents the global, cross-sector and inter-sector results from our DCI verification using the risks disclosed by Fortune 500 companies (2004), and identifies the most frequently disclosed risks.

3 Methods, sample selection and data collection

Our initial DCI design was based on a revue of scientific literature and various risk databases, an analysis of best practices in risk management, and personal interviews with North American managers. In order to further refine our DCI, we subsequently reviewed the annual reports filed by almost all Fortune 500



companies (2003) and their risk disclosures from 2001 to 2003 (as indicated in the 10-K, 10-Q, 8-K, and 11-K forms, for American companies).

In order to test our DCI, we firstly classified the risks disclosed by Fortune 500 Companies (2004) according to the risk categories included in our DCI. The 100 companies in our sample were chosen from the top Fortune 500 companies, and did not include financial companies due to their specific risk profile. Secondly, we performed the same test using different sectors. Each company was assigned to a sector according to the Industry Classification Benchmark (ICB) used by the New York Stock Exchange (NYSE). From the 50 types of risks included in our DCI we verified 46, with the remaining risks being very specific (such as 6.4 “nuclear risk”) or needing to be tested on specific companies (such as 8.4, “risks related to mergers and acquisitions”). Finally, the disclosed risk-related information was sorted and classified in a matrix form (table 1).

Table 1: Collecting and classifying the disclosed risks according to our DCI.

	C ₁C _kC _L			
	C ₁₁	C _{1j}	C _{1m1}	C _{k1}	C _{kj} ..	C _{kmk}	C _{L1}	C _{Lj}	C _{LmL}	D
F1										D1
.. Fi ..					R _{ikj} (0/1)					Di
Fn										Dn
P _{kj}	P ₁₁	P _{1j}	P _{1m1}	P _{k1}	P _{kj}	P _{kmk}	P _{L1}	P _{Lj}	P _{LmL}	

3.1 Notations used

L is the number of risk categories included in our DCI (L = 11); C_k (k = 1...L) identifies the category k of risks, as defined in our DCI; C_{kj} identifies a specific risk j included in the category C_k; m_k (k=1...L) is the maximum number of risk subcategories (risks and their main sources) included in the respective category (C₁,... C_k,... C_L) - for example according to the information provided in table 2 m₁=5, m₂=7 etc.; n is the number of F500 companies in the sample; R_{ikj} = 1 if the company i discloses the risk C_{kj}, and 0 if this risk is not disclosed by the company i; Di is the total number of DCI risks disclosed by the company i (the sum of all matrix elements in a row); and P_{kj} is the percentage of F500 companies disclosing a specific risk C_{kj} (the sum of all elements in a column divided by n).

We define the *frequency of disclosure* of a particular risk C_{kj} as being the number of times the disclosure of this risk occurs in our data set, as represented in the following formula:

$$F_{kj} = \sum_{(i)} R_{ikj} \text{ and } F_{kj} (\%) = F_{kj} / (\sum_{(i)} D_i); i = 1 \dots n$$

According to our definition, F_{kj} (%) measures the importance of a particular risk C_{kj} compared to the other risks included in our DCI.



Our method differs slightly from the frequency table and contingency table based methods. This is because our main objective was to verify the accuracy and completeness of the information included in our DCI, and to design a generic map of risks, rather than to establish relationships between variables using statistical techniques.

4 Data collection instrument for total risk identification

4.1 The main DCI structure

The main structure of our DCI is presented in table 2.

Table 2: The main structure of our DCI.

Risk Category: 11 categories and 50 sub-categories	L/M/H/NA
C1. Operational Risk: 1.1 to 1.5	
C2. Network Risk: 2.1 to 2.7	
C3. Market Risk: 3.1 to 3.3	
C4. Financial and Liquidity Risk: 4.1 to 4.3	
C5. Credit Risk: 5.1	
C6. Technological Risk: 6.1 to 6.7	
C7. Risk of Outsourcing: 7.1 to 7.5	
C8. Risk of Vertical Integration: 8.1 to 8.4	
C9. Risk of International Contract (Exporting): 9.1 to 9.5	
C10. Risk of Changing Contexts: 10.1 to 10.5	
C11. Country Risk: 11.1 to 11.5	
L=Low; M=Medium; H=High; NA = Not Applicable.	

Every risk category included in our DCI contains a certain number of risk subcategories. Each risk subcategory refers to a particular risk and to its main sources. To further assist managers and researchers in correctly identifying each risk, we developed questionnaires for each risk subcategory. The questions included in these questionnaires are not related directly to the risk itself, but rather to the sources of this risk. Thus we encourage decision makers to go beyond cognitive limitations, proactively revealing potential and previously unforeseen risks instead of making decisions based on known risks from past experiences.

4.2 A brief description of the risks in our DCI and their main sources

C1 Operational Risk: includes risks related to a company’s regular operations.

C1.1 Supplier risk: a) supplier can’t maintain supply continuity and ensure on-time delivery; b) nonconforming items; c) supplier bargaining power (“Captive Buyer”); d) poor financial stability of supplier; e) poor supplier competitiveness in its sector/industry.



C1.2 Risks related to the continuity and quality of the processes, services and operations: a) internal breakdowns; b) human errors; c) other failures in operating processes and systems.

C1.3 Product recalls: a) design and use of the product; b) raw materials or parts (defective/ poor quality): risk C1.1 being the main source; c) information exchanged in product labelling: misinformation/ incomplete or inaccurate information/ no common “Product Identifier” throughout the supply chain: logistic risk C1.4 being the input; d) errors in data entry; e) absence of security procedures; e) absence of a Public Relations Plan (PRP) for dealing with product recalls.

C1.4 Logistical risk: lack of a good traceability system; lack of compliance with national/international standards for the Tracking and Tracing of different products (paper-based; bar code; RFID technology).

C1.5 Risk related to customer payment delays

C2. Network risk: in this category we include the risks related to the company’s strategic relations with different “actors” in a networked economy.

C2.1 Industry and competitors: a) failing to evaluate the industry structure, dynamics and new competition drivers: entry and exit costs; projected growth versus historical growth; production versus demand; industry cost structure versus company’s cost structure (labour/capital/inputs); b) overcapacity (failing to adapt to the minimum efficient scale (MES) of the industry); c) inappropriate growth strategy: organic growth versus mergers and acquisitions versus joint ventures versus strategic alliances, franchising, licenses, etc.; d) inappropriate diversification: being too focused or too diversified; e) failing to protect intellectual property (competitors could legally challenge patents); f) risk 10.1 being the input.

C2.2 Customers: a) failing to attract new customers: poor quality; poor *on-time delivery* performance (risk C1.4 being the main source); contracts too restrictive (high switching costs); b) failure in retaining customers: non-competitive “quality/price” ratio; non-competitive after-sales service; failing to understand changing customer needs; failing to prevent customer data from being leaked to competitors (industrial espionage; risk C2.7 (b) being the main source).

C2.3 Shareholders, government, and financial markets: a) risk of new product development (lack of a “commercial” market; high R&D costs incurred, and obsolescence of the newly launched product); b) the risk that actual return on investments will differ from the expected return c) regulatory risk (concerning products regulated by government bodies); d) risk of “management paralysis” (reluctance to take risks by executives and boards under intense pressure to comply with new codes of business ethics and governance rules); e) ethical risk: criminal conduct and corruption scandals (ignoring directors’ conflict of interest; failing to monitor executive compensation); unfair treatment of workers and labour abuses (sweatshops and child labour); e) risks related to rumours, disinformation and false perceptions; f) risk related to the reaction of capital markets to financial results, stock split and dividend announcements.



C2.4 Employees: a) risk of losing key personnel; b) unrealistic pension and health care commitments or loss of control over retirement costs and pension scheme benefits; c) poor motivation and absenteeism; d) union bargaining power and strike risk; e) vandalism; f) discrimination; g) harassment.

C2.5 Civic society: a) environmental catastrophe (any environmental risk greater than the acceptable risk); b) health risks still unknown/unverified (differs from 1.3, which is a controllable risk), for instance: “the economic class syndrome” for the air transportation sector; mobile phone radiation and brain cancer; videogames and child aggressive behaviour or even epilepsy; mad cow disease; toxic building materials such as asbestos etc.; c) risk of product boycott (“hegemonic” attitude towards the local community and local businesses).

C2.6 The legal risk: in this category we include the legal risks related to the relationships mentioned in C2.1-C2.5.

C2.7 Information risk: in this category we include only the information risks related to the relationships mentioned in C2.1-C2.5, such as: loss of system and data integrity, loss of system functionality and/or availability, loss of confidentiality (improper use and disclosure of sensitive information). The other risks related to new technologies are included in the category 6. We found the main sources of these risks to be: a) malicious transactions/ intrusions in Database Systems and/or industrial espionage: internal intruder (risk due to inadequate control over employee access rights) or external intruder (risk due to security design and/or implementation procedures); b) errors, omissions, and mistakes in transactions; c) virus infection; d) service attacks due to weakness in security policies.

C3. Market risk: **C3.1** Commodity risk; **C3.2** Spot exchange rates risk; **C3.3** Long-term and Short-term Interest Rate Risk.

C4. Financial & liquidity risk: **C4.1** Impossibility to meet financial obligations when new projects/investments lead to important cash outflows (risk 2.3 (b), 8.2 and 8.4 being the inputs); **C4.2** Operational, financial and legal risks related to the use of derivative products; **C4.3** Financial fraud.

C5. Credit risk: loss due to the inability of various counterparties to make payments as required.

C6 Technological risk: including all technology related risks.

C6.1 Major industrial accidents (including oil tanker accidents, chemical industry accidents, explosions on site); main sources: a) human error; b) equipment and/or safety device failures; c) poor maintenance; d) communication failures; e) terrorism; f) organisational structure failures; g) malicious actions.

C6.2 Accidents related to the marine transportation industry, including shipping and port activities, as well as marine transportation of dangerous substances (explosives and infectious substances); main sources: a) human error; b)



passenger overload; c) poor maintenance; d) bad weather; e) communication failures; f) “military” or “paternalistic” organizational structure; g) terrorism.

C6.3 Accidents related to road transportation, air transportation, rail transportation (passenger and cargo transportation): a) human error; b) equipment and/or safety devices failure; c) poor maintenance; d) traffic control failures; e) communication failures; f) bad weather; g) terrorism; h) organisational structures; i) airport related risk.

C6.4 Nuclear accidents and radiation leaks: specific risk related to nuclear plants.

C6.5 Building, bridge and dam collapse: a) human error (especially during the excavation and the frame building phases); b) poor maintenance; c) lack of engineering knowledge; d) natural disaster.

C6.6 Business risk related to the emerging technologies: a) B2B (Business To Business commerce): main focus on the technology itself rather than on business needs; strategic alignment gap: there is no IT alignment with the company strategy, gravity centre and core competences, for instance: a company with the gravity centre in supply (“Low Cost buyer”) implements a CRM technology or a company with the centre of gravity in marketing and distribution (“Low Costs distributor”) implements a SCM technology. b) Business to Customer commerce (B2C): risks related to transactional website; c) specific business risks related to new emerging technologies (biotechnologies/ nanotechnologies, genetic engineering, renewable fuels and hybrid engines): long development and approval process and inability to raise sufficient funds; impact on society and life (civilian technology versus military applications).

C6.7 Project-related risks: the newly implemented technology does not produce the projected quantifiable benefits: a) overestimation of the anticipated impact of new technologies on company’s long-term financial performance; b) management inability to capture the whole advantage derived from the newly implemented technologies.

C7 Risk of Outsourcing includes all risks associated with delegating in-house activities to an external firm.

C7.1 The loss of control over the outsourced activity: the business practice shows that the reintegration of an outsourced activity is very costly.

C7.2 The “lock-in” risk: the company locks itself into a service contract, with predetermined service quality and price over a long time period.

C7.3 The social risk related to the transfer of personnel between the two teams: existing differences between working conditions, working contracts, retirement plans and carrier paths may lead to employee discontent, strikes or the boycott of company products.

C7.4 Risk related to the terms of the agreement: a) lack of specific stipulations concerning the mechanisms for quantifying, measuring, and verifying the compliance of services provided within the requirements of the partnership agreement; b) “scope creep” risk: in the absence of specific stipulations regarding the process, a supplementary price may be charged for what the



external company considers “additional work”; c) lack of specific stipulations concerning the performance standards that the partner should maintain over the duration of the partnership (financial and operational performance, cost structure and reputation); d) lack of specific stipulations concerning the communication plan and partner “transparency”; e) lack of specific stipulations concerning knowledge transfer: the timetable and the joint costs.

C7.5 Privacy and security risk related to the service supplier’s power: the newly emerged international “specialists in outsourcing” may share their clients’ strategic information with one of their direct competitors; security risk should be also envisaged when IT activity is outsourced.

C8 Risk of Vertical Integration: in this category we include all the strategic risks related to performing multiple stages of the value chain.

C8.1 Risk of poor overall performance despite good performance in all distinct activities within the organization’s internal value chain: a) arbitrary price transfer between different strategic business units in the value chain; b) different MES of the activities in the value chain; c) different skills and capabilities needed at each stage of the value chain; d) high complexity costs and asymmetry of information; e) lack of coordination mechanisms and no synergy with support activities.

C8.2 Cash flow at risk: longer production cycle for any vertically integrated company: main source of risk being C4.

C8.3 Lack of strategic flexibility: a) high vulnerability in responding to changes in technological, business and economic cycles; b) high vulnerability and lack of strategic flexibility to respond to market demand fluctuations, especially when returns in a company’s various markets/industries/sectors are positively correlated.

C8.4 If integration through a merger or acquisition, other specific risks include: a) pre-merger risks: overestimating value; excessive premium paid; unrealistic expectations of synergies; b) post merger integration risk: large disparity between businesses; conflicting corporate culture; inappropriate timetable; failure to implement rapid changes and to transfer critical capabilities.

C9 Risk of international contract (exporting): we included in this category the risks related to the international contracts according to INCOTERMS regulations: **C9.1** Legal risk; **C9.2** Risk of non-payment; **C9.3** Transportation risk; **C9.4** Custom Duty risk; **C9.5** Quality and or quality control failure.

C10 Risk of Changing Contexts: we classified in this category the risks related to the main changes in *local* contexts as well as those due to company’s failure to anticipate the major trends in the global contexts (risk of “propagation”). These risks are different from the “country-risk” (category C11). The risk subcategories included are the risks related to main changes in: **C10.1** The economic context; **C10.2** Technological context; **C10.3** Demographic and social context including the potential of a world pandemic; **C10.4** Political context; **C10.5** Legal and regulatory context. For each subcategory, we identified a list of risks sources as well as the main connections with risks in other categories.



C11. Country Risk: one section for each foreign country in which the company is present through direct investment (none for “national companies”): C11.1 the 10 political risk components (except sections D and E) as established by the International Country Risk Guide (ICRG); **C11.2** internal conflicts (ICRG, Political Risk, section D); **C11.3** external conflicts (ICRG, Political Risk, section E); **C11.4** the 5 components of the country economic risk as established by ICRG; **C11.5** the 5 components of the country financial risk as established by ICRG.

5 Results from applying our DCI to the risks disclosed by Fortune 500 companies

The average number of our DCI risks disclosed by Fortune 500 companies is 13 (AVGD = 13.06), accounting for 28.3% of the total 46 risks verified. These results differ from sector to sector, with the most sensitive sectors being the “*Technology super-sector*”, composed of the *Software & Computer Services* and *Technology Hardware & Equipment* sectors (AVGD = 22), and the “*Utilities super-sector*” (AVGD=19).

Figure 1 presents the map of risks disclosed by the Fortune 500 companies in our sample.

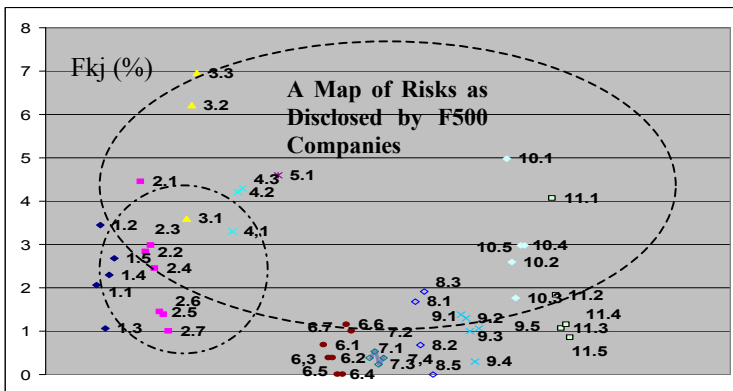


Figure 1: A map of risks F500.

Considering that the total number of risks disclosed by the companies in our sample (i.e. the number of non-null elements in matrix 1) was 1306 (AVGD = 13.06), each risk included in our DCI could have obtained a maximum F_{jk} score of 7.65%. In other words, if a certain risk C_{kj} from our DCI had been disclosed by all companies ($P_{jk} = 100\%$) it would have obtained an F_{jk} score of 7.65%.

In order to accurately access these results, and to establish a comparison within and across sectors, it is important to note that the total number of risks disclosed varies from sector to sector and consequently each sector has its own scale, although this does not affect the sector results. Nevertheless, for the



interpretation of the cross-sectors results one should consider each Fjk value according to the different scales of the compared sectors.

As shown in figure 1, the most disclosed risks are those arising from changes in interest rates, foreign currency exchange rates, and other market changes in the economic context, followed by credit and liquidity risks. This is not a surprising result considering that North American companies must comply with regulations concerning the disclosure of market risk, which is typically affected by economic, political, and socio-demographic factors. Also, the fact that almost all companies in the study are multinationals legitimizes their concern for political country-risk (C11.1).

We note the fact that companies pay little attention to the risks included in category 9, probably because a large part of these risks are currently covered through insurance policies. Nevertheless, the simple fact that a risk is insurable does not eliminate its presence. Because risks are interrelated, companies should be concerned about the growing opportunity costs related to these insurance policies and look for new ways of dealing with some of these risks.

We also note an important concern for network risks, especially for those related to suppliers (2.1). In an era where the process of globalization provokes important changes in the configuration of organisations internal value chains, leading many to focus on their core business and outsource activities that do not directly add value, new risks related to outsourcing emerge. Unfortunately we observed that many companies seem to ignore such risks (Category C7), or simply consider only the tangible risks included in this category (perhaps due to their apparent similarities with already known “supplier risk”). We verified this assumption by classifying the risk disclosure of 24 companies in the sample that outsourced at least one activity, and the same conclusion was drawn.

Other under valued risks are those included in categories C2.5 and C2.2. All companies state that they put the customer at the core of their business, and note the importance of being a “good corporate citizen”, but the risks arising from customer and civil-society relationships are, judging from their risk disclosure, underestimated. Some companies, such as Exxon, seem to have learned from their past experiences, whilst others, such as Wal-Mart, are currently facing “civil society risk”. The majority, however, whether from lack of direct experience or otherwise, do not seem to be preparing themselves for the increasing likelihood of such events.

If companies seem to understand the “hard” components of risks related to technology investment (C4.1), the picture is rather different when we look at the “soft” components of these risks, which we call “new-age risks”. We have already noted the perception that companies seem to have regarding outsourcing risk, and the same “passive attitude” was observed when analyzing their risk disclosures regarding information and new technology related risks (C2.7, C6.6, and C6.7). Once again these risks are related, and consequently information risk may not only cause significant damage on its own, but may also bring down even a large company when accompanied by other risks. For example Air Canada’s bankruptcy, whilst primarily due to its failure to respond to industry dynamics and new competition drivers (C2.1a), was triggered when its managers failed to



prevent customer data from being leaked to its main competitor WestJet (information risk C2.7). We may argue that companies are reluctant to disclose such risks even if they pay particular attention to all of them. However in studying the map of risks disclosed by technology sector firms (figure 2), we may conclude that this is not the case.

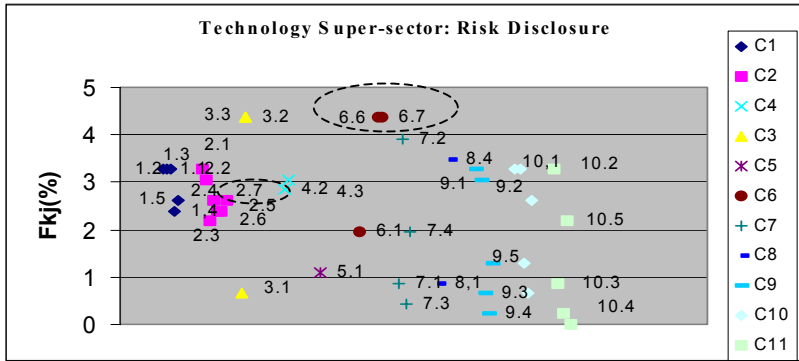


Figure 2: Technology super-sector.

Whilst it is true that technology is their core business, the important score obtained by the risks C2.7, C6.6 and C6.7 are not necessarily related to their core business, since all such risks were classified in the category C1 (operational risk) of our DCI. Considering the crisis that this sector faced in the beginning of the 21st century, we can understand why these companies may be paying special attention to these “new-age” risks whilst other sectors ignore them completely. This suggests that rather than proactively preventing new risks and avoiding failures, companies seem to act in reaction to their past experience.

If we look at the quasi-null *Debt/Equity* ratio of some companies in our technology sector sample, such as Intel and Microsoft, and to Dell’s “Direct Model” based on e-invoice/e-payment, we can explain why the liquidity and credit risks are less important for this sector than for our main sample. For instance, the score obtained by the risk C5.1 is 1.089 on a scale of 0 to 4.5 for this sector, compared to 4.59 on a scale from 0 to 7.65 for the main sample.

6 Conclusions and implications for further research

In this paper we propose a framework for identifying the total risk of a company, namely a Data Collection Instrument (DCI) containing 50 different risks. In applying our DCI to the risks disclosed by Fortune 500 companies, we found that these companies disclosed a significant number of risks beyond those which they are legally obliged to disclose. In fact, at least one company disclosed each of the 46 risks tested, and no company disclosed risks which were not included in our DCI. This result confirms the fact that our DCI is useful and comprehensive



enough for researchers and managers to use when building a company risk-profile.

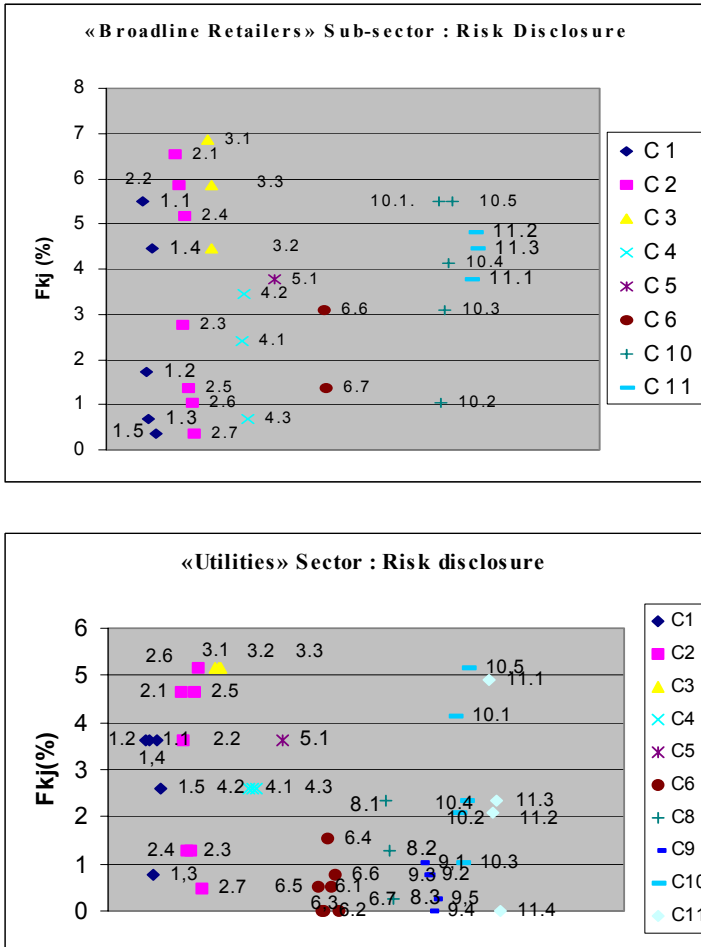


Figure 3: Sectors results (examples).

We also attempted to discover whether companies considered certain risks in our DCI as being more important than others. In order to do this, we assumed that each risk disclosed by a company voluntarily was considered more important than those not disclosed. Based on this assumption, we proposed a measure for the “importance” of each risk included in our DCI, called the Fkj score. Our results indicate that many of the risks in our DCI are very important to almost all companies irrespective of their sector (such as risks C1.2, C1.5, C2.1, C2.2, C3, C4, and C5), albeit to different extents. Furthermore, some risks



selected in our DCI seem to be significantly more important to companies in certain sectors, supporting the findings of Dia and Zégal [2]. Nevertheless, the importance of these risks differs amongst companies according to their business model. For instance, Dell observes the risk C2.2 more carefully than its competitors because of its “Direct Sales” business model. Our study has also identified the fact that companies still appear to ignore some sector specific risks. For instance, various companies in the “Utilities” *super-sector* are very concerned with political country-risk but some of them seem to underestimate the strategic risks arising from their high level of vertical integration (C8.1, C8.2, C8.3; figure 3). Finally, the majority of companies in all sectors except for the technology sector seem to completely ignore “new-age” risks (C2.7, C6.6, C6.7 and C7).

Our DCI, as far as we are aware, represents the first attempt to integrate all the risks of a company in an overall and comprehensive picture, including the main risk sources and their potential relationships. Our framework for risk identification goes beyond existing risk “categorizations” that are based upon Fayol's Five Functions of Management, by crossing existing functional boundaries.

References

- [1] Bandyopadhyay, K., Mykytyn, P. & Mykytyn, K., A Framework for Integrated Risk Management in Information Technology. *Management Decision*, Vol. 5, pp.437-444, 1999.
- [2] Dia, M., Zégal, D., Évaluation floue des profils de risque des entreprises du TSE 300 à partir des informations divulguées dans les rapports annuels, Working Paper (132-05-20), Accounting Research Centre (ARC), University of Ottawa, 2002.
- [3] Dumitriu, C., L'intelligence technologique dans les réseaux de transport et l'acceptabilité sociale des risques. *Proc. of ACFAS Int. Conf., division 633 On Risk and Crisis Management in Networked Economies*, eds. Bombardier Chair: pp.59-79, Montreal, 2004.
- [4] Hodder, L., Koonce L. & McAnally M.L., SEC Market-Risk Disclosures: Implications for Judgment and Decision Making. *Accounting Horizons*, Vol. 15 (1) pp. 49-70, 2001.
- [5] Istrati, C., Dumitriu, C., Crisis Management, Technological Change and Technological Revolutions: The Crisis of the New Economy. *Proc. of 3rd Int. Conf. On Management of Technological Changes*, eds. Venus Publishing: Hania, Greece, pp. 35-44, 2003.
- [6] KPMG, Best Practices in Risk Management: Private and Public Sectors Internationally, The Treasury Board of Canada Secretariat, 1999.
- [7] Linsmeier, T.J. & Pearson N.D, Quantitative Disclosures of Market Risk in the SEC Release, *Accounting Horizons*, Sarasota, Vol. 11 (1), pp. 107-135, 1997.



- [8] Loren Gary, The Right Kind of failure, Newsletter from Harvard Business School, R. U0201B, 2002.
- [9] Meulbroek, L., A Better Way To Manage Risk, Harvard Business Review, F0102B, 2001.
- [10] Securities Exchange Commission (SEC): Release No. 33-8144 (Nov. 4, 2002) [67 FR 68054]; Release No. 33-8056, FR-61 (Jan. 22, 2002) [67 FR 3746]; Release No. 33-8106 (June 17, 2002) [67 FR 42914]; Regulation S-K [17 CFR 229.303; Release No. 33-8176; 34-47226; FR-65; FILE NO. S7-43-02; Release Nos. 33-8182; 34-47264.
- [11] Simons R., How Risky Is Your Company? Harvard Business Review, reprint number 99311, 1999.
- [12] Simons R., A Note on Identifying the Strategic Risk, Harvard Business Review, 9-199-031, November 1999.

