

A Control System Designed to Address the Intangible Nature of Service Risks

Magali Dubosson
Emmanuel Fragnière
Bernard Milliet

Cahier : N° HES-SO/HEG-GE/C--08/4/1--CH

2008

M. Dubosson is with the Haute Ecole de Gestion (HEG) de Genève, 7 route de Drize, 1227 Carouge, Switzerland (phone: 0041-22-388-1709; fax: 0041-22-388-1700; e-mail: magali.dubosson@hesge.ch). She is also part of the Institute for Service Innovation, Essec, Paris, France.

E. Fragnière, *CIA* (Certified Internal Auditor), is with the Haute Ecole de Gestion (HEG) de Genève, 7 route de Drize 1227 Carouge, Switzerland (e-mail: emmanuel.fragniere@hesge.ch). He is also with the University of Bath, School of Management, Bath BA2 7AY, UK (e-mail: e.fragniere@bath.ac.uk).

B. Milliet, *CIA*, is with the Swiss Federal Banking Commission, Schwanengasse 12 / P.O. Box, 3001 Bern, Switzerland (e-mail: bernard.milliet@ebk.admin.ch).

A Control System Designed to Address the Intangible Nature of Service Risks

Magali Dubosson
Emmanuel Fragnière
Bernard Milliet

Cahier de recherche

Mars 2008

Summary

Due to the intangible nature of services, classical control approaches might not provide the relevant safeguards to enable the service company to reach its objectives. Typically, services results from an experience whose value and quality are complex to measure. Additional difficulties arise when the monitoring of risks is implemented in management information systems. Indeed, assuming that most prominent risks encountered in the service industries is the consequence of “invisible threats”, appropriate approaches need to be built. We must also take into account the typical chain of risks that leads to the major damage. To tackle these specific service-type risks, we have designed a qualitative control system that enables auditors to allocate their resources and monitor the sequences of risks. We believe that if properly replaced in the corporate governance context, it could represent a useful tool to manage important categories of service risks. We adopt an internal auditing perspective.

Keywords

Chain of Risks ; Internal Control Systems ; Operational Risk Management ; Perceived Risk

This the working paper version of the following proceeding paper : Dubosson Magali, Fragnière Emmanuel and Milliet Bernard, « A Control System Designed to Address the Intangible Nature of Service Risks », Proceedings of the 2006 IEEE International Conference on Service Operations and Logistics, and Informatics, Shanghai, China, pp. 90-95 June 21-23 2006.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4125557

I. INTRODUCTION

According to the IIA glossary (Institute of Internal Auditors, www.theIIA.org) the term control means: "Any action taken by management, the board and other parties to enhance risk management and increases the likelihood that established objectives and goals will be achieved". Control is thus an important part of managerial activities. However, the design of controls dedicated to services is particularly tedious. Indeed, service activities are traditionally described with the help of the IHIP paradigm (Intangibility, Heterogeneity, Instantaneity and Perishability). Compared to the production of goods, services will typically display a high degree of most of the 4 IHIP dimensions. As such, the intangibility of the service makes that the identification of risks is not easy.

The Marketing discipline has extensively worked on the notion of perceived risk, which can add tremendous value to the practitioners' risk management process. According to the literature, consumers perceive services as riskier than products [1], [2]. Research in [3] has shown that intangibility is positively correlated with perceived risk. As stated by [1] "Intangibility ... greatly increases the degree of perceived risk in the purchase of services by decreasing the certainty with which services can be made". Reference [4] shows that the properties of services may lower consumer confidence and increase perceived risk, mainly by augmenting the degree of uncertainty in the decision.

In this paper, we propose a new type of control whose design makes a distinction among the following states of "risk attributes": the threat, the event(s), the ignorance (unawareness), and the damage. In classical approaches to control, we tend to focus solely on the expected damage. Typically risk mapping (see Section II), is a technique to assess the risk of business activities, which is based on the damage multiplied by the frequency (a formula also used by economists and engineers). Nevertheless perceived risk literature tells us that a person would be more sensitive to the overall consequences than the probability.

Our control design involves 3 types of tests which are: whether the threat is associated with a prevention system, whether the event is associated with a detection system, and finally whether the ignorance of the problem is associated with a protection (or curative) system. Compared to a traditional approach this will foster an ex-ante treatment of risk as opposed to an ex-post one. It is quite well known that acting in an ex-ante manner will cost less and will be more efficient (i.e. "prevention is better than the cure").

Our methodology mixes approaches borrowed from the risk management and audit professions as well as research from services marketing. Most cutting-edge approaches of risk management are based on quantitative models. This is essentially due to the strong influence of the Basel Committee on how to handle financial risks such as market and credit risks in the banking sector. However, qualitative approaches to risk management are recently emerging especially because of the recognition that operational risks, or non-financial risks, are of primary importance. In our case we believe that the expertise (professional judgment) of the auditor will be the main input to assess the risk.

The notion of anticipative control [6] represents the cornerstone of a new auditing philosophy called "Risk-Based Auditing" (RBA). Indeed, audit planning tends to be based on what has already been (or not) audited in the previous years. This way of allocating resources to audit missions does not fit with today's uncertain markets anymore. On the contrary, RBA calls attention that the audit planning should be established upon the importance of the risks faced by the company. It thus represents a paradigm shift for the internal audit function, which must adopt a new auditing philosophy. As said in [5] "Instead of looking at the business process in a system of internal control, the internal auditor views the business process in an environment of risk". Thus, our approach falls into the RBA category. However we suggest using the notion of perceived risk and risk chain to prioritize audit missions.

The paper is organized as follows. In Section II, we recall the risk management process employed by practitioners. In Section III, we explain the notion of Internal Control System (ICS), which enables the company to protect itself against operational and financial risks. Internal auditor of the company are in

charge verifying the adequacy of controls to allow the company to achieve its objectives. On the other hand, external auditors tend to focus on financial audits. We thus present, in Section IV the audit risk model, which assesses the risk taken by the auditors of not discovering risks in the company. In Section V, we introduce the approach of risk-based auditing. It is a planning system that allocates audit resources according to a risk prioritization criterion. We also indicate that damages affecting the company result from a sequence of risk-events and that the prioritization criterion should take into account the corresponding "chain of risks". In section VI, we explain the notion of "perceived risk" and how it can improve risk management in the context of services. In Section VII, we present our model of control system that distinguishes the main steps of the risk materialization: *threat-event-ignorance-damage*. As an illustration, we propose a case where this control is applied in the banking sector.

II. The Risk Management Process

In this section, we refer to professional bodies such as COSO (www.coso.org) and IIA (www.theIIA.org) that are specifically addressing risk control and management issues. We believe that professional guidance is relevant in our context to make our approach more feasible. The sequence of a risk management approach is often stated as follows:

1. *Identification of risks*

This part corresponds to the inventory of risks exposed to the company. Typically a bank decomposes its business risk into credit, market, operational, interest rate and strategic risks. Each major risk is then subdivided into more detailed categorizations of risk. These risks should also be qualified regarding their "nature" such as exogenous and/or endogenous, controllable and/or uncontrollable, financial and/or non-financial, short-term and/ long term.

2. *Prioritization of risks*

From the inventory of risks, a ranking is established from the most important risk to the least important. The most frequently used method of prioritization is called "risk mapping" (see Figure 1). The measure of risk applied in this context is defined as the probability multiplied by the damage done. The most important risks appear in the upper right quadrant. As the resources to manage risks are limited, this enables to assume a "Pareto Law" such as 20% of the identified risks account for 80% of the total risk. The non-financial risks are difficult to assess through this formula in terms of likelihood as well as in terms of financial damage.

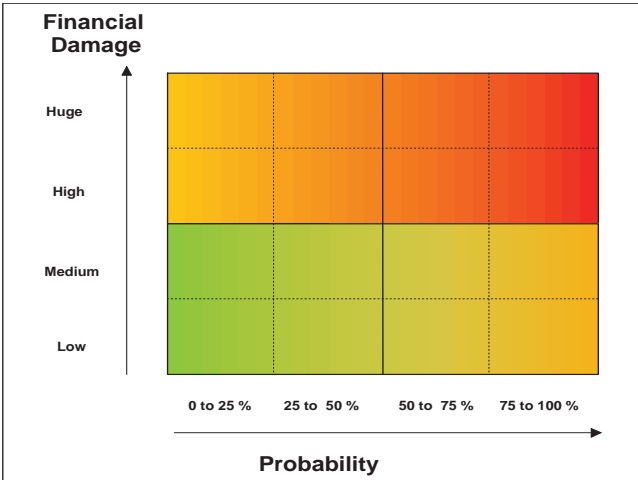


Figure 1. Example of a risk mapping table

3. *Setting up an Internal Control System (ICS) and definition of the risk ownership*

This step is too often omitted from the risk management process. The internal control system enables to monitor the risks and to "exercise" the available options in time whenever a problem happens. Risk ownership is a very touchy topic in risk management. It consists of defining which company members are ultimately responsible (accountable) for the different risks.

4. Risk management per say

There are different ways to tackle the risks. A valuable approach is to decompose the total risk into pieces that can then be handled in distinctive manners:

- Transfer. We include here all the financial measures such as insurance policies, as well as the outsourcing of risk.
- Eliminate. If an activity is considered to be too risky compared to its benefits, then it is abandoned.
- Mitigate. Referring to the formulae: risk equals probability multiplied by damage, it means either reducing the likelihood or the damage.
- Accept. In most cases, there will still be some residual risk that cannot be reduced with the above approaches in a cost effective manner. Here comes the notion of risk tolerance. The tolerance should correspond to what the company is ready to sustain in terms of loss. In our societies we tend to have very low tolerance for risks, which also contributes to increase the cost for risk management.

5. Actions plans

Another step that has to be added to the risk management process is the definition and the implementation of action plans in order to avoid any contagion in case of an undesirable event. Business continuity planning, contingency planning, emergency and crisis management, and disaster recovery fall into this category.

6. Risk communication

Finally the risk communication is accompanying every step of the process. Communication is crucial to spread a culture of risk in the corporation and also to attenuate the disastrous effects of a crisis.

III. Internal Control System (ICS)

The Internal Control System is fundamental to the Audit function, since the role of auditing could be summarized as being "the control of the control". In a quite classical conception of management, it is composed of 4 components:

- Planning, which sets up the long-term objectives of the company and, recursively the mid-term and short-term operations.
- Organization, which is the skeleton of the company and enables to achieve the objectives.
- Involvement, which is the participation of employees towards the accomplishments of the objectives.
- Control, which assures that the first three components are functioning properly.

ICS is more and more linked with the concept of corporate governance (see for instance, www.sarbanes-oxley.com). In this case, the risk criterion can be stated as maximizing shareholders value while protecting the assets of the company. In an ideal scheme, the board should represent the interest of the shareholders, be in charge of the general surveillance of the company thanks to an internal control system, and define the strategy of the company. Regulatory bodies, such as COSO and the SEC, put pressure to include risk information in annual reporting and thus to increase transparencies in the reporting practices.

The process control can be defined by the three following steps:

- Definition of standards
- Measures and communication of results
- Corrective actions (do nothing, reconsider the objective, improve)

There are two kinds of controls. First, there are the "a posteriori" controls such as budgetary controls, where the measure is confronted to the standards once the results are known. Second, the "a priori" (or anticipative control, see [6]) controls have an identical structure except that the measure of results is replaced by a forecast of results. These latter controls are more adapted to the monitoring of risk strategies whose associated decisions will have impacts in the longer term. Control conveys a certain idea of risk, which is known as "adjusted" risk. It makes the implicit assumption that the actual risk is lower than the inherent risk when the internal control in place is of good quality.

IV. The Audit Risk Model

In the auditing profession, a distinction is made between the inherent risk and the actual or residual risk. Indeed it is believed that if the internal control in place is of good quality the risk actually faced by the company is reduced compared to the inherent risk (or “crude risk”). The generally accepted “audit risk model”, even though not much applicable, makes as such the distinction between the inherent risk and the audit risk (or the remaining risk assuming that auditors have completed their work). Reference [7] shows that “the auditors’ knowledge of the client’s industry improves their audit risk assessment and directly influences the nature and the perceived quality of their audit planning decisions”. This is the main reason why we have opted for a qualitative approach (or more formally a Bayesian approach, which relies on subjective information) for prioritizing risks rather than a quantitative one.

Organizational aspects of corporate governance are crucial to understand audit risk. The audit committee, in charge of audit planning, is formed by several non-executive directors who are working in conjunction with external and internal auditors. The main role of external auditors is to audit the financial reports. On the other hand, internal auditors will perform broader types of audit work (e.g. IT audit, see COBIT, www.isaca.org) because of their deeper knowledge of business processes and the organizational structure of the firm. The triangular relationship between the internal and the external auditing functions and the audit committee is still not solved.

The audit risk model is essentially applied to quantify the audit risk of financial audits. It is defined as follows:

$$AR = IR \times CR \times DR \quad (1)$$

IR, the Inherent Risk, represents the risk that might affect the company when there is no ICS. *CR*, the Control Risk, corresponds to the situation where the ICS has been unable to detect a risk. *DR*, the Detection Risk, is the risk that the external auditors will not detect material misstatements in the financial reporting. By extension for internal auditors, it corresponds to the non-detection of operational risks. As every variable of the right hand side of the equation takes a value between 0 and 1, *AR* (Audit Risk) corresponds to a probability. The model is employed as follows: a level of *AR* is chosen (e.g. 10%) then *IR* and *DR* are assessed by the auditor (for instance using a Bayesian approach) and finally the equation is solved for *DR*. Limitations of the audit risk model are obvious, such as the interdependency that exists between *IR* and *CR*. It should be simply seen as a conceptual framework to foster risk-aware approaches when conducting an audit.

As seen above, *DR* has a direct influence on audit procedures. Indeed, if auditors had infinite resources, they would conduct all the possible tests of controls. As such, the detection risk would be 0.

V. Risk-Based Auditing for Event-Risk Chains

"Plans are worthless, planning is priceless" used to say D.D. Eisenhower. Audit Planning is an extremely important step that significantly contributes to reduce audit risk. As resources allocated to auditing are limited, audit missions and associated methodologies should be selected very carefully. “Risk Based Auditing” is the planning of audits based on an assessment of the risks to which the company is exposed. So, the main purpose of RBA is to efficiently allocate limited resources to financial and operational audits in order to significantly improve the quality of the Internal Control System, as well as to reduce the audit risk.

Most of the available approaches meant to deal with risk are model-based. A model is a simplified representation of a real system that attempts to capture its main behavior. Modeling syntaxes might vary from simple diagrams to very complex mathematical formulas. The primary categories of models certainly come from the discipline of quantitative finance. The common factor of those financial models is that they have quantitative variables whose behavior is described by theoretical probability distributions. Just to name a few of them, the mean-variance framework (Markowitz model), the Sharpe ratio (i.e. CAPM model), Value-at-Risk (except for the VaR based on historical simulations). The main advantage of these approaches is to capture correlations which are typically attached to financial risks and thus to devise strategies of diversifications. From this common framework, other parametric methods, such as extreme event theory, have emerged. These are especially useful in performing stress testing simulations (i.e. a simulation of rare and catastrophic events). Relying too heavily on models exposes the company to model risks. This corresponds to the situation where a model, though properly implemented, is applied in a situation where its main assumptions are not

verified. One of the major model risks is that most quantitative models do not take into account cause and effect relationship that is typically associated with risks. Correlation is not causality.

Very often major risks results from a sequence of minor events. Dealing (managing) with easy risks will often prevent a catastrophe to happen. Finally, most modeling approaches tend to rely heavily on Management Systems Information (MIS). The process of implementing is known to be costly and long lasting.

As explained in section II, risk prioritization is usually done through a risk mapping table. Risk is then defined as the probability multiplied by the damage done. As often major risks results from a sequence of minor events, dealing (managing) with easy risks will often prevent a catastrophe to happen. The risk identification should thus be accompanied by dynamic linkages, which exist among risks. Tools such as cause-and-effect diagrams, flow charts, influence diagrams, decision trees, and fault-tree analyses can help. The text ERM (Enterprise Risk Management) COSO (The Committee of Sponsoring Organization of the Treadway Commission, www.coso.org), which was adopted in 2005 and is already a reference in risk management for the accounting, audit, and controlling professions, has introduced the notion of "identification of events". This acknowledges that cause-and-effect is fundamental to the analysis of risk.

VI. The Notion of Perceived Risk

The perception of risk has been found as totally subjective [8], [9]. Perceived risk was considered as a subjective expectation of loss [1],[10]. [11] identified five independent types of risk: financial, performance, physical, psychological and social. [12] added a sixth type of risk: time loss. Therefore, risk mapping takes into account only one type of risk.

Service agents develop relevant strategies to reduce perceived risks and hence augment purchase probabilities as shown in [13]. Therefore, if service companies want to be perceived as delivering good value, they have to adopt strategies to reduce uncertainties and perceived risk at the purchase stage. At the post-purchase stage, risk-reducing strategies are employed to reduce the consequences of a less than satisfactory purchase [14]. To reduce consumer risk, service companies should implement initiatives that directly address the risk (e.g. guarantees) or the factors that contribute to the risk (e.g. increase tangibility) [15]. Risk-reducing strategies can be categorized according to whether they reduce the level of uncertainty, e.g. receiving correct information or investing money on good shares, or reduce the adverse consequences of the adverse outcome, e.g. giving a refund or helping to solve when experiencing annoyances. Indeed, it has been found in [16] that each product has a set of risks associated with its purchase and each consumer has an individual risk tolerance which, if exceeded, one or more risk-reduction strategies will be employed to reduce the amount of risk perceived to a tolerable level. In the literature, these are the most often referenced risk reducing strategies: sales staff knowledge, tangibilization of services, free trials and samples, money-back guarantee, celebrity endorsements, favorable press reports, company and brand reputation.

Contrary to financial risks, such as market and credit risks, it is extremely difficult to aggregate operational risks, and especially when the company produces services like a bank. They are heterogeneous by nature. Let us think about a compliance problem and an Information System (IS) failure. The origin of those risks mostly arises from human interventions, even those related to the IS. The Operational Risk manager will need to work with different functions, processes, persons, at the level of the business units. Manufacturing activities have the great advantage to be organized around production processes. They have thus the ability to trace the operational risk and to handle it with non-financial procedures (e.g. traceability, quality control, redundancy, bottleneck management).

We would like also to mention an interesting and original work on the characterization of the appearance of risk which is due to a French expert in technological risk, Jean-Louis Nicolet. His theory (see [17]) is that most of the time technological accidents are the consequence of human errors. He suggests that seven types of human errors are systematically identified in past technological accidents: perception, decoding, representation (what the operator has understood), non-respect (e.g. of a procedure), communication, timing of decisions, and sequencing of actions.

VII. Control Design for Risk-Event Chains

The previous section about perceived risk indicates that it is worth considering the tangible part of the risk as well as the intangible part when designing controls. We propose to decompose the risk sequence into the following step:

1. Threat (a potential risk that might endanger the company, e.g. an inflammable Persian carpet was installed in a customer *salon*)
2. Event (an event related to the threat happens, e.g. cigar ashes fall on the Persian carpet and ignite a fire)
3. Ignorance (or unawareness of the event, e.g. the client and the client advisor have already left the *salon* and are ignoring that a fire has started)
4. Damage (e.g. fire has time to propagate throughout the building, employees just manage to evacuate safely the building)

In Figure 2, we attempt to describe the importance of control to avoid the contagion of major risks. We thus establish a relationship between a threat and its potential resulting damage. If the ICS appears to lack measures of prevention, an undesirable event might happen (e.g. lack of due diligence processes). If detection systems are defective or inexistent, it might propagate within the company (e.g. no accurate MIS to perform the reconciliation of assets). Ultimately, if nobody is aware of it and that no protective measures are in place (e.g. no insurance policy), the "expanding" damage might badly hurt the company, which consequently won't be able to reach its objectives.

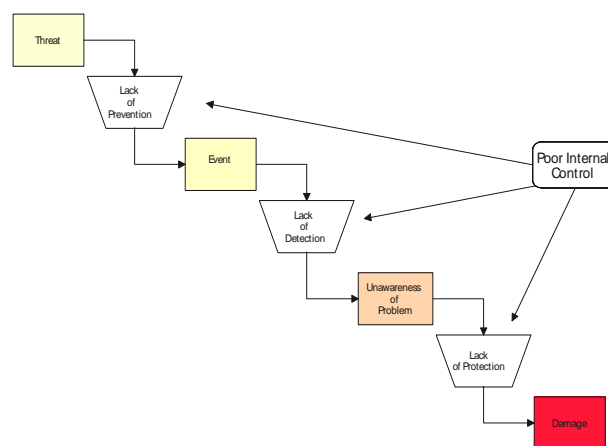


Figure 2. Illustration of a poor ICS

We propose now a simple (fictitious) case study illustrating the implementation of our concept in the banking sector. It is based on the experience of the three authors as internal auditors and portfolio managers. A private bank is analyzing the possible threats that could affect its reputation.

The private bank fears that inappropriate appraisal provided by its investment managers to its wealthy clients could badly endanger its image on the market. The main threat considered corresponds to cases where managers are not able to properly define the risk appetite of their clients. The CEO is aware that just a few cases of this kind could be sufficient to provoke the damage. For instance, a client advisor diagnosed that one of his client displays an aggressive appetite for risk and actually the profile of this investor is rather conservative. There is no objective level of risk. We have to assess and manage the risk as it is perceived by the client (i.e the perceived risk):

1. The management (i.e. in charge of setting up an ICS) will first design a preventive control. Controllers will be in charge of checking that each client advisor has properly conducted a risk appetite diagnosis for each of their clients, that the information is properly consigned according to the policy of the company and finally that this document is regularly updated. At the same time, each client advisor must be trained and instructed to appraise the risk appetite of clients.
2. The management will then design a detective control. Indeed, it might be that nevertheless a portfolio does not match the risk appetite of a given client. Controllers are then in charge of collecting (on a sample basis) feedbacks from clients regarding the performance of their portfolio.
3. The management will finally design a protective (or curative) control. Indeed if the first 2 controls (preventive and detective) are not able to prevent the contagion of events (bad diagnosis of risk appetites), the intention is to add a control that will mitigate the main damage to happen (reputation risk). For instance, the performance of every portfolio associated with a bad performance (i.e. performance can be here different kinds of abstract criteria) will be

checked on a regular basis and compared to those of clients presenting similar characteristics (e.g. age). The bank may also think about ways of “tangibilizing” the service.

This simple case shows the interest of decomposing the risk sequence. Indeed simpler, though very effective, controls can be set up upstream. Our experience tells us that in practice auditors tend unfortunately to focus more on curative controls. In our years in the banking sector, we had the opportunity to recommend and monitor the implementations of such controls (involving a sequence of preventive-detective-curative controls) and we used to formalize them with the help of tools developed by engineers like fault-tree analyses.

VIII. Conclusion

In this paper we propose a new kind of control, which adopts the Risk-Based Auditing (RBA) scheme. RBA is an audit planning approach that uses risk assessment as the main prioritization criterion. This really represents a paradigm shift since classical audit planning techniques tend to use criteria such as frequency of audits performed in the past. So applying RBA will put more emphasis on the design of anticipative controls. This latter kind of controls becomes a necessity to cope with rapid changes in the environment. Our contribution is based on the RBA philosophy except that in our case, risk is not only seen as damage, but rather as a sequence involving the followings steps (or “risk stages”): threat, event, ignorance and damage. Our approach remains qualitative for the time being. Indeed we believe that simple cause-and-effect analyses (e.g. fishbone, fault-tree ...) will be sufficient for experienced auditors to properly prioritize risks and monitor adequate controls for each category of “risk stages”. Additionally, research findings from the discipline of marketing services tell us that threats (upstream treatment of risk) should be handled with the same care as damages (downstream treatment of risk). Allocation of audit resources should be changed and be more oriented towards the identification of threats and the implementation of detective controls to prevent any contagion of risks.

IX. References

- [1] V.W. Mitchell and M. Greatorex, “Risk perception and reduction in the purchase of consumer services”, *The Service Industries Journal*, vol. 13, pp. 179-200, October 1993.
- [2] K. B. Murray and J. L. Schlacter, “The impact of services versus goods on consumers’ assessment of perceived risk”. *Journal of the Academy of Marketing Science*, vol. 18, no. 1, pp. 51-65, 1990.
- [3] A. Finn, “A theory of the consumer evaluation process for new product concepts”, *Research in Consumer Behavior*, vol. 1, pp. 35-65, 1985.
- [4] V.W. Mitchell, “Consumer perceived risk: conceptualizations and models”, *European Journal of Marketing*, vol. 33, no. 1/2, pp. 163-95, 1999.
- [5] D. McNamee, “Risk-based Auditing”, *Internal Auditor*, pp.23-27, August 1997.
- [6] A.C. Filley, R.J. House, and S. Kerr, *Managerial Process and Organizational Behavior*. Glenview, IL: Scott, Foresman, and Co, 1976.
- [7] K.-Y. Low, “The effects of industry specialization on audit risk assessments and audit-planning decisions”, *The Accounting Review*, vol. 79, no. 1, pp. 201-219, 2004.
- [8] W.J. Havelena and W.S. DeSarbo, “On the measurement of perceived consumer risk”, *Decision Sciences*, vol. 22, pp. 927-39, 1990.
- [9] I. Ross, “Perceived risk and consumer behavior: a critical review”, *Conference of the American Marketing Association*, vol. 1, pp. 19-23, 1975.
- [10] J.P. Peter and M.J. Ryan, “An investigation of perceived risk at the brand level”, *Journal of Marketing Research*, vol. 13, pp. 184-88, May 1976.
- [11] J. Jacoby and L. Kaplan, “The components of perceived risk”, in 1972 Proc. 3rd Annual Conference Association for Consumer Research, pp. 382-93.
- [12] T. Roselius, “Consumer rankings of risk reduction methods”, *Journal of Marketing*, vol. 31, no. 1, January, pp.56-61, January 1971.
- [13] M. Laroche, J. Bergeron, and C. Goutaland, “How intangibility affects perceived risk: the moderating role of knowledge and involvement”, *Journal of Services Marketing*, vol. 17, no. 2, pp. 122-140, 2003.
- [14] V.W Mitchell and P. Boustani, “A preliminary investigation into pre- and post-purchase risk perception and reduction”, *European Journal of Marketing*, Vol. 28 No. 1, pp. 56-71, 1994.
- [15] M. Laroche, G.H.G. McDougall, J. Bergeron, and Z. Yang (2004). “Exploring how intangibility affects perceived risk”, *Journal of Service Research*, vol. 6, no. 4, pp. 373-89, May 2004.
- [16] V. W. Mitchell, “A role for consumer risk perceptions in grocery retailing”, *British Food Journal*, vol. 100, no. 4, pp. 171-83, 1998.
- [17] A. Carnino, J.-L. Nicolet and J.-C. Wanner, *Man and Risks: Technological and Human Risk Prevention*, New York, NY: Marcel Dekker Inc, 1990.

Cahiers de recherche du Centre de Recherche Appliquée en Gestion (CRAG) de la Haute Ecole de Gestion - Genève

© 2006

CRAG – Centre de Recherche Appliquée en Gestion

Haute école de gestion - Genève

Campus de Battelle, Bâtiment F

7, route de Drize – 1227 Carouge – Suisse

✉ crag@hesge.ch

www.hesge.ch/heg/crag

☎ +41 22 388 18 18

☎ +41 22 388 17 40

2006

- N° HES-SO/HEG-GE/C--06/1/1--CH
Andrea BARANZINI
Damien ROCHETTE
“La demande de récréation pour un parc naturel. Une application au Bois de Pfyn-Finges, Suisse”
- N° HES-SO/HEG-GE/C--06/2/1--CH
Giovanni FERRO LUZZI
Yves FLÜCKIGER
Sylvain WEBER
“A Cluster Analysis of Multidimensional Poverty in Switzerland”
- N° HES-SO/HEG-GE/C--06/3/1--CH
Giovanni FERRO LUZZI
Sylvain WEBER
“Measuring the Performance of Microfinance Institutions”
- N° HES-SO/HEG-GE/C--06/4/1--CH
Jennifer D’URSO
“L’eau de boisson : Aspects logistiques et attitude du consommateur”
- N° HES-SO/HEG-GE/C--06/5/1--CH
Jennifer D’URSO
“La gestion publique de l’eau en Suisse”
- N° HES-SO/HEG-GE/C--06/6/1--CH
Philippe THALMANN
Andrea BARANZINI
“Gradual Introduction of Coercive Instruments in Climate Policy”

- N° HES-SO/HEG-GE/C--06/7/1--CH
Andrea BARANZINI
Caroline SCHAERER
José RAMIREZ
Philippe THALMANN
"Feel it or Measure it. Perceived vs. Measured Noise in Hedonic Models"
- N° HES-SO/HEG-GE/C--06/8/1--CH
José RAMIREZ
Anatoli VASSILIEV
"An Efficiency Comparison of Regional Employment Offices Operating under Different Exogenous Conditions"
- N° HES-SO/HEG-GE/C--06/9/1--CH
José RAMIREZ
Joseph DEUTSCH
Yves FLÜCKIGER
Jacques SILBER
"Export Activity and Wage Dispersion : The Case of Swiss Firms"
- N° HES-SO/HEG-GE/C--06/10/1--CH
Joëlle DEBELY
Gaëtan DERACHE
Emmanuel FRAGNIERE
Jean TUBEROSA
"Rapport d'enquête : sondage Infobésité"
- N° HES-SO/HEG-GE/C--06/11/1--CH
Andrea BARANZINI
José RAMIREZ
Cristian UGARTE ROMERO
"Les déterminants du choix de (dé)localisation des entreprises en Suisse"
- N° HES-SO/HEG-GE/C--06/12/1--CH
Catherine EQUÉY BALZLI
Jean TUBEROSA
David MARADAN
Marie-Eve ZUFFEREY BERSIER
"Étude du comportement des PME/PMI suisses en matière d'adoption de système de gestion intégré. Entre méconnaissance et satisfaction."
- N° HES-SO/HEG-GE/C--06/13/1--CH
Joëlle DEBELY
Magali DUBOSSON
Emmanuel FRAGNIÈRE
"The pricing of the knowledge-based services : Insight from the environmental sciences"

2007

- N° HES-SO/HEG-GE/C--07/1/1--CH
Andrea BARANZINI
Caroline SCHAERER
“A Sight for Sore Eyes
Assessing the value of view and landscape use on the housing market”
- N° HES-SO/HEG-GE/C--07/2/1--CH
Joëlle DEBELY
Magali DUBOSSON
Emmanuel FRAGNIÈRE
“The Travel Agent: Delivering More Value by Becoming an Operational Risk Manager”
- N° HES-SO/HEG-GE/C--07/3/1--CH
Joëlle DEBELY
Magali DUBOSSON
Emmanuel FRAGNIÈRE
“The Consequences of Information Overload in Knowledge Based Service Economies”
- N° HES-SO/HEG-GE/C--07/4/1--CH
Lucie Bégin
Jacqueline Deschamps
Hélène Madinier
“Une approche interdisciplinaire de l’intelligence économique”
- N° HES-SO/HEG-GE/C--07/5/1--CH
Journée de la recherche HEG 2007
“Recueil des communications”
- N° HES-SO/HEG-GE/C--07/6/1--CH
Sylvain Weber
Andrea Baranzini
Emmanuel Fragnière
“Consumers Choices among Alternative Electricity Programs in Geneva – An Empirical Analysis”

2008

- N° HES-SO/HEG-GE/C--08/1/1--CH
Andrea BARANZINI
José RAMIREZ
Sylvain WEBER
“The Demand for Football in Switzerland : An Empirical Estimation”

- N° HES-SO/HEG-GE/C--08/2/1--CH
Giuseppe CATENAZZO
Gaëtan DERACHE
Emmanuel FRAGNIERE
Patricia HUGENTOBLER
Jean TUBEROSA
“Rapport d’enquête préliminaire : Dessine-moi un service ! Entreprises et administration : comment concevoir et valoriser vos services”
- N° HES-SO/HEG-GE/C--08/3/1--CH
Nguyen VI CAO
Emmanuel FRAGNIERE
Jacques-Antoine GAUTHIER
Marlène SAPIN
Eric WIDMER
“Optimizing the marriage market through the reallocation of partners : An application of the linear assignment model”