Annals of DAAAM for 2012 & Proceedings of the 23rd International DAAAM Symposium, Volume 23, No.1, ISSN 2304-1382
ISBN 978-3-901509-91-9, CDROM version, Ed. B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2012
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2012

INNOVATION IN MANAGING THE IT RISKS OF ENTREPRENEURSHIP RISK MANAGEMENT

JALBA, L[iviu] & ANICAI, O[vidiu]

Abstract: *The three most commonly experienced incidents such as IT risks are in the categories of (a) security and privacy, (b) infrastructure and (c) data. Entrepreneurship Risk Management can de-emphasize control (security / privacy and infrastructure are recognized by entrepreneurs as high risk areas and organizations are planning to spend more to mitigate these risks), procedures, documentation, isolation (the risks around data are not yet very high on the corporate agenda - potential risk of underspending). IT tools (applications and databases) are not immediately a high risk category – eventually companies plan to spend more (with the potential risk of overspending). Our solution follows the next steps: (1) Understand the risk from informatics perspective based-on risk questionnaires and risk surveys (Ex.: a risk questionnaire that includes a series of questions on both internal and external events can also be used effectively to identify risks), (2) Treat IT risk management as a business investment based-on Scenario analysis (Ex.: a number of risks are potentially present within a single event, and the total impact could be very large), (3) Reevaluate risks regularly using technology (Ex.: company's products, services, and overall reputation are vulnerable to Internet-based new media like blogs, message boards, e-mailing lists, etc).*

Keywords: *IT, risk, questionnaire, scenario, analysis, business*

1. INTRODUCTION

Entrepreneurship Risk Management can be influenced by IT risks through a new perspective to interrelationships and requires a higher level of understanding of what risk is in order to get the right balance between control and expansiveness, between process and creativity. The novelty of our solution follows the next steps: (1) Understand the risk from informatics perspective based-on risk questionnaires and risk surveys (BAQ & ITQ), (2) Treat IT risk management as a business investment based-on Scenario analysis (scenario based on BAQ & ITQ risk measures answered by 10 (ten) Romanian SME companies; in this approach we consider a number of possible scenarios, i.e. a number of possible risk-factor mentioned in BAQ &ITQ changes.), (3) Reevaluate risks regularly using technology (examining some of the emerging technologies and trends to identify those that may apply to ERM in the near future).

2. DATA STRUCTURE

There are two questionnaires: one business area questionnaire (BAQ) and other IT Questionnaire (ITQ).
BAQ contains questions such as:

(a) Is IT support for this system adequate?

(b) Does the capacity and functionality of IT system support the company's strategic objectives?

(c) What are the high IT risk conditions in your area?

(d) Please quantify the potential dollar exposure related to misuse or errors connected to operating this system. How many "transactions" are created in your area using this system (please define your answer in the time frame which you judge to be most meaningful, daily, weekly, quarterly, etc.)?

(e) What are the primary controls you use to monitor business processed through this system?

(f) Which of these do you consider to be high risk?

(g) Are the controls effective (i.e., timely accurate, meaningful, etc.)?

(k) How many changes to this system have been implemented this year (both hardware and software)?

(l) How would you rate the potential for financial loss due to any of the following :Human error or fraud (Low, Medium, High), Competitive disadvantage (L,M,H),Incomplete information(L,M,H), Operational disruption(L,M,H); Is the development or administration of this system outsourced?

(m) Are new systems or significant system changes planned for the remainder of this year, or next year?

(n) What would be the best way to improve security or quality for this system?

(o) Do you have risk taking and/or risk management responsibility?

ITQ contains questions such as:

(1) What would be the best way to improve security or quality for this system?

(2) How many years experience does the IT staff have supporting this system?

(3) How many people are qualified to support this system?

(4) System support is outsourced?

(5) How would you rate the systems documentation for this system (L, M, H)? (1) How often was this system changed last year (L, M, H)?

(6) What are the IT controls for assuring the security of this system?

(7) Do they address risks (such as, entering data incorrectly, changing data, deleting data, destroying data, "crashing" systems, holding data hostage, destroying hardware or facilities?

(8) Who is in charge of monitoring the security of this system?

(9) Who is the backup?

(10) What are the IT controls for assuring the systems capacity, and the integrity or quality of this system? To whom are integrity or quality problems reported?

(11) What are the IT controls for assuring the continuity and rapid recovery of this system?

(12) When was the last recovery test for this system?

(13) Is this system described in the recovery test plans, logs, and sign-offs from that test? Are there output samples from this system which were made during that test? Are significant system changes planned for the remainder of this year or in the next year?

(14) What are the most significant threats to this system?

(15) What would be the best way to improve security or quality for this system?

3. DATA MODEL

There is a simple pattern to the consideration of risks as part of business decision-making: determine the risk; analyze it; evaluate it; manage it; ignore it; insure against it; control it; improve the management and business processes that are the basis of the risk.

IT risk management as a business investment based-on Scenario analysis which uses of scenario-based risk analysis are many and varied. The explicit analysis of scenarios may suggest ways of reducing or eliminating exposures through loss control activities. Loss control actions have the effect of shifting where scenarios lie on our risk diagram by reducing probability of loss, amount of loss, or both. The scenario analysis method was used to examine the impact of plausible events on the IT event estimates.

Two approaches were used to aggregate losses generated by the scenarios with the original data: (i) the worst-case IT events defined by a particular scenario; (ii) the average-case IT events given by probability distribute on of the loss defined by a particular scenario. Scenario contains: the first one is based on an unauthorized access, based on an external fraud, based on process management failure loss even types. The aim was to analyze, whether the company would be able to handle particular combinations of IT events defined in the scenarios employed for a particular test combination.

Scenario was based on BAQ & ITQ risk measures answered by 10 (ten) Romanian SME companies; in this approach we consider a number of possible scenarios, i.e. a number of possible risk-factor mentioned in BAQ &ITQ changes. Formally, this approach may be formulated as follows. Fix a number N of possible risk-factor changes

$$[BAQ\ (a) - (o)]\ \&\ [ITQ\ (1) – (15)],\\ Y = \{y1, y2, .yn\} \tag{1}$$

Each scenario is given an impact, w (i) and we write

$$w = (w1;\ \ldots;\ wn) \tag{2}$$

We consider a result with a great impact of business Z[n] (:). The occurrence of the IT risks is then measured as:

$$A\ [Y, w] = max\ \{w1Z[n](y1),\ldots,\ wnZ[n](yn)\} \tag{3}$$

4. RESULTS

Impact of IT Risk management in business area (1-High impact, 3- Medium, 5- Low)

To successfully develop a business, you must identify and focus your attention on middle and high-priority risks – IT risks are among them - otherwise you risk spreading your efforts too thinly, and you'll waste resources on unnecessary risk management.

SME Crt nr.	Scenario			a	b	c	d	e	f	g
	Avg	*BAQ*	*ITQ*	1	2	3	4	5	6	7
1	2,5	*3*	*2*	2	3	3	2	3	1	4
				2	2	3	3	2	1	4
2	2,25	*2,5*	*2*	1	2	3	3	2	2	2
				4	4	1	1	2	2	1
3	2,25	*1,75*	*3,25*	1	2	1	2	2	3	1
				3	2	1	2	2	2	3
4	1,75	*1,75*	*1,75*	1	2	1	1	1	1	1
				2	2	1	2	1	2	2
5	2,6	*2,125*	*3*	1	3	2	1	3	2	2
				3	3	4	2	3	1	1
6	1,75	*1,75*	*1,75*	1	1	2	1	1	2	1
				1	2	1	2	2	1	2
7	2,125	*2,25*	*2*	1	2	1	3	3	3	3
				2	2	3	1	1	1	1
8	1,75	*2*	*1,5*	3	3	3	2	2	2	2
				1	2	2	2	1	1	1
9	2,4	*2,75*	*2*	1	1	2	2	2	2	5
				1	1	2	2	2	2	2
10	2,4	*3*	*1,75*	2	2	3	3	3	4	4
				1	1	1	1	2	1	1

Tab. 1. Impact of IT Risk management for ten (10) Romanian SME

With Likelihood vs Consequences chart, you map out each IT risk – and its position determines its priority. High likely/unlikely are the most critical, and you should put a great deal of effort into managing these. The rare/possible impact risks are next in priority, though you may want to adopt different strategies for each.

Rare impact risks can often be ignored. How dangerous is the IT risks management we've found following BAQ &ITQ

RATING	DESCRIPTION	LIKELIHOOD OF OCCURRENCE
1	--Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	-Unlikely	Not expected, but there's a slight possibility it may occur at some time.
3	Possible	The event might occur at some time as there is a history of casual occurrence
4	+Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence
5	++Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence

Fig.1. Risk Likelihood Descriptors for IT risks management

RATING	DESCRIPTION	BUSINESS INTERRUPTION
1	Insignificant	Negligible; Critical systems unavailable for less than one hour
2	Minor	Inconvenient; Critical systems unavailable for several hours
3	Moderate	Client dissatisfaction; Critical systems unavailable for less than 1 day
4	Major	Critical systems unavailable for 1 day or a series of prolonged outages
5	Catastrophic	Critical systems unavailable for more than a day (at a crucial time)

Fig.2. Risk Consequence Descriptors

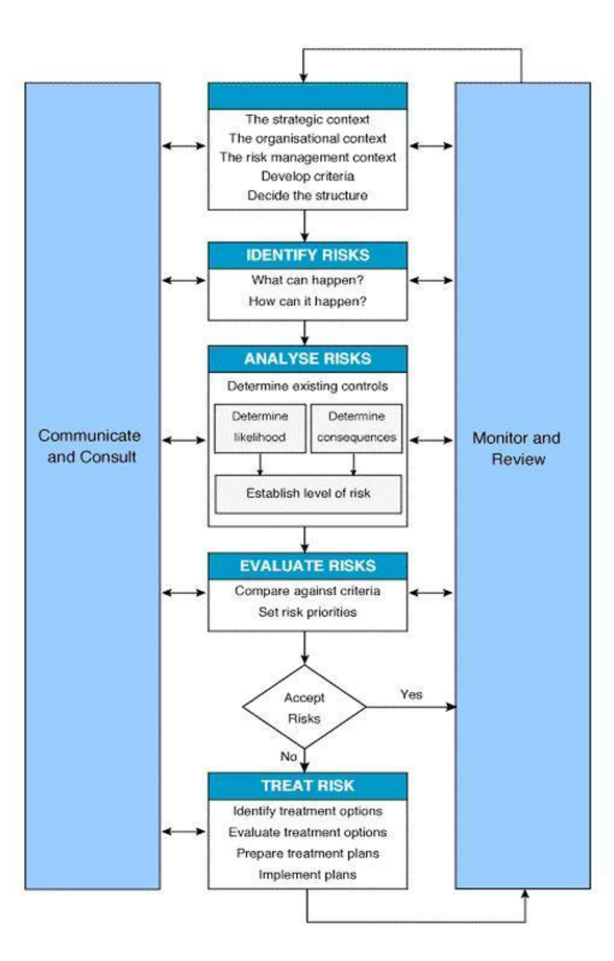

Fig. 1. The IT Risk Management Flow Chart
source: Southern Cross University website

IT risks management such as kind of business includes an adequate business methodology - that provides the possibility to optimize the operational area of a business player - is defined such as:
BPV (business player value) = R (revenues) - C (costs) with R = NR (new revenues) – LR (lost revenues) and C = I (investments) + ATC (additional task cost where includes IT risk management).

The long-term success of the business will be dependent on the pecuniary benefits in addition to the technical merits.

	Likelihood				
Consequenses		+ + **Very Likely** Could happen any time	+ **Likely** Could happen sometime	- **Unlikely** Could happen but very rarely	- - **Very unlikely** Could happen but probably never will
	High damage	2,6	2,5	2,4	-
	Medium damage	2,4	2,25	2,25	-
	Low damage	-	-	2,125	1,75
	Very low damage	-	-	1,75	1,75

Tab. 2. Likelihood vs. Consequences for IT risks management

5. CONCLUSION

In this paper, we have established which the costs and the benefits of corporate IT risk management decisions can be analyzed. The most important conclusion is that IT risk management strategies should be pursued to enhance shareholder value.From the research analysis the authors find that managing the IT Risks of Entrepreneurship Risk Management will start to specialize and it is believed that the next level down is that the industry will have IT Risk Managers specializing in a particular area of risk. IT risk is a subset of business risk, which is a consequence of business decisions. You cannot be in business without taking risks. Whether you accept these risks or not is a function of whether your business thinking is proactive or reactive (see Fig 1.)

The authors conclude that it is necessary to:

(1) Incorporate IT Risks of Entrepreneurship Risk Management tools and techniques into company policies and procedures using different punctual scenario analysis (results for ten SME Romanian companies is in the range (1,75- 2,6);
(2) To have definitions and misconceptions of what Conceptual stage is.
(3) To have a holistic approach to risk means looking at each risk in the context of others (BAQ items and ITQ items).

To involve the whole organization (should be engaged) in the risk management process.

The authors intend this article as a call for action by IT security professionals to react in identifying whether these risks exist at their enterprises. Input should not be trusted from any source unless it is 100 percent certain that the input has not been compromised. All enterprises should employ IT vulnerability tools to identify known IT security weaknesses prior to elevating any software into the production environment. Finally, all non remediated IT vulnerabilities should be signed off on by IT management as matter of recourse for accepting responsibility for the enterprise management.

The present scenario will not provide all the answers, but they help executives ask better questions and prepare for the unexpected. That makes them a very valuable tool indeed. Scenario has some benefits that make them very powerful for understanding risks and opportunities:

(1) Company staff will think more broadly if they develop a range of possible outcomes. By demonstrating how—and why—things could quickly become better or worse, they increase their readiness for the range of possibilities the future may hold.

(2) Having a scenario-based methodology for IT risk management with an IT risk management model, many IT information security functions would be greatly simplified. Instead of requiring the deployment of *ad hoc* IT risk assessment methods and duplicating some risk management functions, security professionals would be able to interact with the risk management framework directly.

(3) IT management will search for predetermined outcomes — particularly unexpected outcomes, which are often the most powerful source of new insight uncovered in the scenario -development process.

(4) Sometime, the hierarchy of an organisation inhibits the free flow of debate. Employees will wait for the most senior executive to state an opinion before venturing their own. Scenario allows the organisation to break out of this trap by providing a political 'safe haven' for contrarian thinking.

(5) Implement personnel IT security controls, background investigations, rotation of duties

(6) Perform periodic system audits.

(7) Conduct ongoing IT risk management to assess and mitigate risk.

(8) Authorize IT systems to address and accept residual risk.

(9) Implement IT assurance techniques to reduce the likelihood of vulnerability's being exercised.

(10) Relate IT risks to business goals.

(11) Keep the business engaged to create support and executive involvement.

(12) IT risks come from multiple sources, change constantly, and require a continuous program of discovery, monitoring, and management. IT risks are managed by the combination of people, process, and technology, balancing risks against business objectives IT Risk Management is a business process that adapts to organizational requirements, guided by best practices

The pace of technology change required more rapid adaptation in technology and process controls than do other forms of operational risk.Many business operations and transactions now took place entirely within IT systems.

6. REFERENCES

[1] Crosbie, P. and Bohn, J. (2001) Modelling Default Risk. K.M.V. Corporation

[2] Crouhy, M., Galai, D. and Mark, R. (2000) A comparative analysis of current risk models, Journal of Banking & Finance 24, 59{117}

[3] Embrechts, P., McNeil, A. and Straumann, D. (2002) Correlation and dependence in risk management: properties and pitfalls. In: Risk manage- ment: value at risk and beyond, edited by Dempster M, published by Cambridge University Press, Cambridge

[4] Embrechts, P., Kluppelberg, C. and Mikosch, T. (1997) Modelling Extremal Events for Insurance and Finance, Springer Verlag, Berlin

[5] Fang, K.-T., Kotz, S. and Ng, K.-W. (1987, Symmetric Multivariate and Related Distributions, Chapman & Hall, London

[6] Gut, A. (1995) An Intermediate Course in Probability, Springer Verlag, New York

[7] McNeil, A., Frey, R., Embrechts, P. (2005) Quantitative Risk Management: Concepts Techniques and Tools, Princeton University Press

[8] Thorp, J., (2003), The Information Paradox: Realizing the Business Benefits of Information Technoloy, McGraw-Hill Ryerson, USA

[9] De Haes, S., Wim Van Grembergen, (2009), An exploratory Study Into IT Governance Implementation and Its impact on Business/IT Alignment,"Information Systems management", vol.26, no.2

[10] http://www.isaca.org, (2008), IT Governance Intitutue (ITGI),Entreprise value:Governance of IT Investments,the ValIT Framework2.0,USA

[11] Ward, S., (2005), Risk management: Organisation and Context, Witherbys

[12] Westerman, G., Hunter, R. ,(2007), IT Risk: Turning Business Threats into Competitive Advantage. (Boston: Harvard Business School Publishing)