Risk Management Framework for IT-Centric Micro and Small Companies

Jasmina Trajkovski[1], Ljupcho Antovski[2]

[1]Trajkovski & Partners Management Consulting
Sveti Kliment Ohridski 24/2/1, 1000 Skopje, Macedonia
jasminat@tpconsulting.com.mk

[2]Faculty of Computer Science and Engineering
University Ss. Cyril and Methodius
Rugjer Boshkovikj 16, 1000 Skopje, Macedonia
ljupcho.antovski@finki.ukim.mk

Abstract. This paper proposes a new risk management framework tailored for IT-centric micro and small companies based on the analysis of the best practices in risk management concepts, specifically the risk management frameworks. The proposed framework for risk management is a synergy of various elements from the existing frameworks, tailored to the specifics of the IT-centric micro and small companies and deals with the identified challenges for the implementation of risk management frameworks. The framework focuses on 4 elements: people, policy, methodology and process, and tools.

Keywords: risk management methodology, risk management framework, ISO31000, ISO27005, enterprise risk management, IT-centric micro and small companies

1 Introduction

In this paper we review the risk management concepts, specifically the risk management frameworks, and based on them we propose a new risk management framework tailored for IT-centric micro and small companies. The proposed framework for risk management is a summary of various elements from the existing frameworks, but adapted to the specifics of the IT-centric companies and deals with the identified challenges for the implementation of risk management frameworks. The research is based on the direct experience of the leading author in the last 5 years with over 20 micro and small companies that are heavily IT-centric in their operations. In each of these companies, there has been a process of application of risk management frameworks, and specifically conducting the risk assessment exercises. The necessity of further work in testing the proposed framework in real-life IT-centric micro and small companies is elaborated toward the end of the paper, and such work will be conducted as part of the PhD research on integrated risk management frameworks and the proposal of a usable model for valuation of risks for the micro and small companies.

This paper is structured in several segments. In Chapter 2, an overview of risk and risk management is provided together with reviews of the risk management frameworks and standards. In the following chapter, the related specifics and challenges for micro and small IT-centric companies are elaborated, while in the Chapter 4, the proposed risk management framework is presented.

2 Overview of Risks and Risk Management Frameworks

The main concepts of risks management in IT-centric micro and small companies are divided into 2 groups: (i) definition of risk, types of risks and risk management, and (ii) risk management frameworks and standards.

Based on the International standard for Risk Management – ISO31000, risk is defined as: “effect of uncertainty on objectives”(ISO, 2009), where the uncertainties include events (which may or not happen) and uncertainties caused by ambiguity or a lack of information, while the objectives can have different aspects (health and safety, financial, IT, environmental) and can apply at different levels (such as strategic, organizational, project, process). It also includes both negative and positive impacts on objectives. The risk is often expresses as a combination of the consequences of an event and the associated likelihood of occurrence. As we discuss risks management frameworks for IT-centric micro and small companies, the main focus are the organizational risks. There are various types of organizational risks such as program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk. (NIST, 2011)

For the needs of the management of the IT-centric micro and small companies, all these risks could not be approached independently, and an integrated approach is necessary. This approach should be focused on the main drivers in the company, like the continual operations thru IT operation and known business processes so that the employees can understand what they should do. The reliance on IT as well puts the information security risks among the top as well. For the purposes of the research questions, we make the assumption that the management of these IT-centric micro and small companies deals with the legal and financial risks intuitively, and that they are not necessary to be included in the integrated risk management framework and approach of the company.

Having said that, for the purposes of the paper, we will look into the IT risk, information security risk and operational risk, which are respectively defined as:

- IT risk—that is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. (ISACA, 2009)
- Information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.(NIST, 2011)

- Operational risk - The most common definition, first published in The Next Frontier and also adopted in recent operational risk documents issued by the Basel Committee, is that "Operational risk is the direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events." (Haubenstock, 2001)

The next concept to be introduced is the risk management. ISO31000(ISO, 2009) defines the risk management very broadly as the coordinated activities to direct and control an organization with regards to risk. Other institutions have a more precise definition, as described for example in NIST special publication SP800-39 (NIST, 2011), where risk management is defined as a comprehensive process that requires organizations to:

- frame risk (i.e. establish the context for risk-based decisions);
- assess risk;
- respond to risk once determined; and
- monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.

Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk based decision making is integrated into every aspect of the organization.

With the development of risk management as an organizational discipline, a more defined concept evolved, named Enterprise Risk Management (ERM). There are many definitions of ERM, but a representative one is from the COSO framework: "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 1992).

After setting the stage with the definition of the concept, lets look at the available risk management frameworks. Nowadays, there are several types of risk management methodologies, some of them issued by national and international organizations such as ISO, NIST, AS/NZS, BSI, others issued by professional organizations such as ISACA or COSO, and the rest presented by research projects. Each of these methods has been developed to meet a particular need so they have a vast scope of application, structure and steps. The common goal of these methods is to enable organizations to conduct risk assessment exercises and then effectively manage the risks by minimizing them to an acceptable level (Saleh & Alfantookh, 2011).

Table 1 provides a comparative overview of the elements of the various frameworks, methodologies and/or standards.

Vorster and Labuschagne in their work(Vorster; & Labuschagne, 2005) go even deeper in the analysis focusing solely on the methodologies for information security risk analysis and define a framework for comparing them. The objective of their framework is to assist the organization in the selection process o the most suitable methodology and/or framework. The elements than they are taking into consideration include:

- Whether risk analysis is done on single assets or groups of assets
- Where in the methodology risk analysis is done
- The people involved in the risk analysis
- The main formulas used
- Whether the results of the methodology are relative or absolute

Some of these criteria are tightly related to the risk management considerations we have identified in the following section for the IT-centric micro and small companies.

Table 1. Overview of elements in risk management frameworks and methodologies

Type of framework	Main elements	Resource
Generic risk management frameworks	• 11 Principles for managing risks • 5 segment framework: mandate and commitment; design framework; implement risk management; monitor and review the framework; continual improvement • 5 step process: establish the context; risk assessment; risk treatment; monitoring and review; communication and consultation	ISO31000:2009 Risk Management Standard(ISO, 2009)
	• It has 4 sub-processes: Risk assessment process; Risk treatment process; Risk communication process; Risk review and monitoring process.	Corpuz and Barnes in their 2010 paper on integration information security policy into corporate risk management (Corpuz & Barnes, 2010)
Information Security Risk Management Frameworks	The tiers are: Organization, Mission / business processes and Information Systems, while the phases are Frame, Assess, Respond and Monitor	NIST SP800-39: Managing Information Security Risk (NIST, 2011).
	6 step process: context establishment; risk assessment; risk treatment; risk acceptance; monitoring and review; risk communication.	ISO27005:2008 Information Security Risk management (ISO, 2008).
	Views: STROPE - strategy, technology, organization, people, and environment Phases: DMAIC - define, measure, analyze, improve, and control cyclic phases.	Information security risk management (ISRM) framework for enterprises using IT (Saleh & Alfantookh, 2011)
IT Risk management frameworks	Domains: Risk governance, Risk evaluation and Risk response	RiskIT framework (ISACA, 2009)

Type of framework	Main elements	Resource
Operational Risk Management Framework	Components: identify, assess, respond to and control risk	COSO Enterprise risk management integrated framework (Aguilar, 2004)
	Elements: 1. leadership, 2. management, 3. risk, and 4. tools.	RMA Operational risk management framework (Taylor, 2006)

3 Risk Management considerations for IT-Centric Micro and Small Companies

As further elaborated in the authors' paper on challenges or implementation of risk management frameworks in IT-centric micro and small companies(Trajkovski J., 2012Trajkovski J., 2012) , there are several specifics and challenges that need to be taken into consideration when designing a suitable integrated framework for such companies. These include:

- Specifics of IT-centric micro and small companies:
  - Exposure to various types of risks
  - Limited resources for risk management
  - Low resilience of the organizations to operations and information security risks
- Challenges related to meeting the following requirements:
  - Need for integrated approach to treat various types of risks
  - Need for comprehensive and usable methodology

These considerations, together with the findings from the analysis of the various existent risk management frameworks, standards and/or methodologies demonstrate the need for development of an integrated risk management framework for IT centric micro and small companies.

The developed framework should be applicable for the identified key risks groups: operational, IT and information security risks, as well as be implementable i.e. doable for an average team for risk management that includes 3-5 people, within 5-10 days annually, and the respective level of effort of 20-25 man/days on annual basis.

Regarding the need for comprehensive and usable methodology, the integrated risk management framework for IT-centric micro and small enterprises should be comprehensive and should present an understandable set of steps and activities, with clear inputs and defined outputs. The elements of the organizational context should be clearly defined and should allow for small or even non-existent organizational hierarchies and procedures. The framework should allow for unclear segregation of duties, and for very high criticality of managers and/or owners, as well as lack of documented knowledge.

The integrated approach should as well include an adjusted valuation model as part of the risk assessment phase that can be used on various types of risks. This model should not be data intensive as experience shows that micro and small companies do not have access to historical data about risks, probabilities and impacts. It as well should not be based on complex calculations, require advanced skills, nor should it require too much time or people to conduct the risk assessment exercise.

4 Proposed Risk Management framework for IT-Centric Micro and Small Companies

As defined in the ISO31000:2009 Risk Management Standard (ISO, 2009), a risk management framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management in the organization.

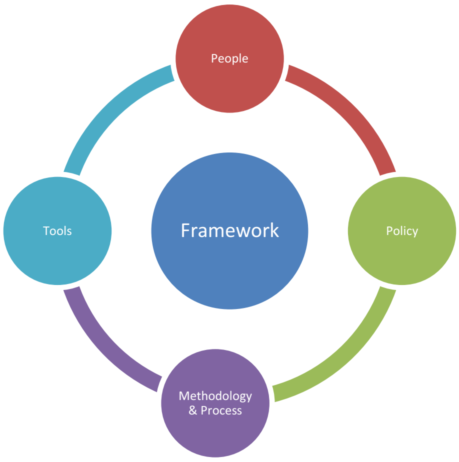


Fig. 1. Risk Management Framework

We presented in the previous section an overview of the various risk management frameworks connected to the identified key risks for an IT-centric micro and small company, showing the main elements of the frameworks. In order to provide a usable framework which covers all the key risks, and which takes into consideration the specifics of the IT-centric micro and small company, we took the common elements of the analyzed frameworks and created a customized framework. This new framework reflects the experiences gained from implementing risk management in over 20 micro and small IT-centric companies in the Balkan region which the authors have.

In future work, the authors will focus on further development of all the elements of the proposed framework and their elaboration in detail. The framework will then be tested on IT-centric micro and small companies. The results will be used to fine-tune the framework to the specific needs of these companies in the Balkan Region.

The customized framework for risk management in IT-centric micro and small companies presented on Figure 1 consists of: people, policy, methodology and process, and tools.

4.1 People

The People component of this framework deals with the Risk management team and the Risk management officer. It is described first, as it reflects the facts that risk management is people intensive process and the people are crucial for the successful implementation and maintenance of risk management in the organization

- Risk management team – to include the representatives from the main processes or units in the company, as well as the management team. Optimal number of representatives is 5 to 7.
- Risk management officer – a responsible person in the company, the owner, and managing director or other person from the management team in the forefront of the activities for risk management.

4.2 Policy

The risk management policy is a simple but straightforward document summarizing the intent and the approach for risk management. As main elements, the policy includes:

- Scope and purpose of the risk management
- Main objectives
- Risk management principles
- The commitment of management to risk management
- Allocated responsibilities for the process and results
- References to the methodology and process to be used
- Level of acceptable risk for the company.

The document is public and circulated to all employees. Its optimal length is 1 to 2 pages, and it should be in line with other management policies, if they exist in the company, such as Quality management policy or Information Security Management policy. The policy should be reviewed at least annually to reflect the changes in the environment of the company in which the risk are identified, assessed and managed, as well as the level of acceptable risk.

4.3 Methodology and Process

The risk management methodology includes comprehensive and implementable guidelines for conducting the risk management process. It enables the company to:

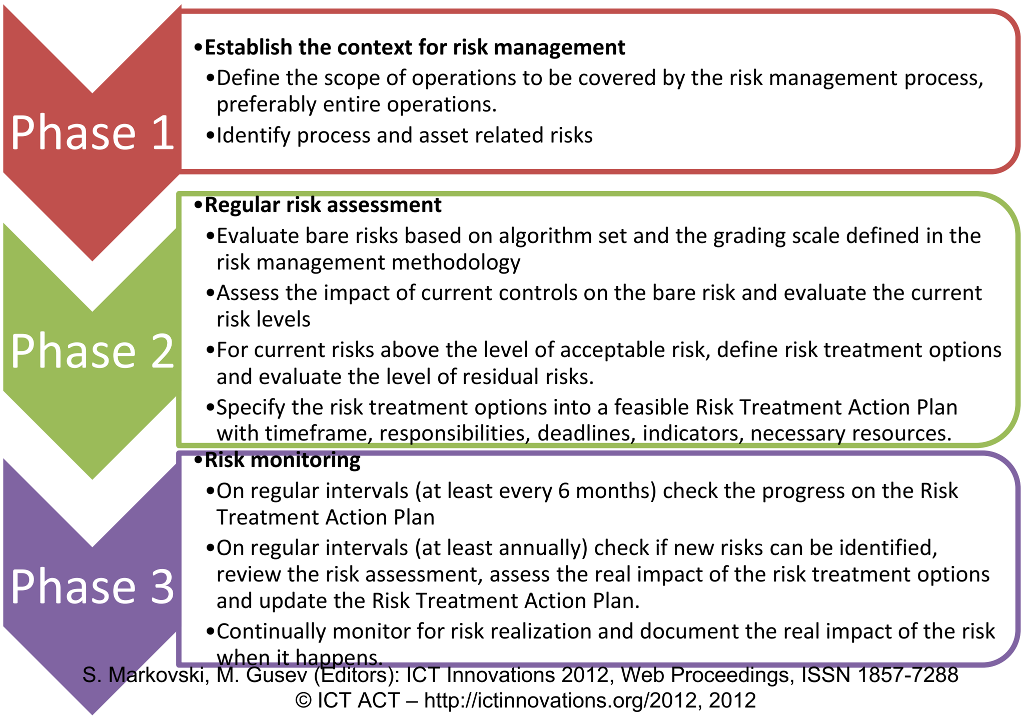
- Identify process and asset related threats and vulnerabilities

- Repeatedly conduct risk assessment with comparable/consistent results taking into account the already implemented mitigation steps
- Get a prioritized list of key risks using a common qualitative scale
- Decide on the level of acceptable risk for the company
- Identify further mitigation action necessary
- Define a realistic Risk Treatment Action Plan with necessary resources, priorities for the actions, responsible person

The methodology enables consistent implementation of the Risk management process and its activities. The Risk Management team should understand the Risk Management methodology and should be trained and competent to implement the Risk Management process.

Risk management process is a series of inter-related activities that enable the company to address risk. It includes the steps grouped in 3 phases as described in the in Figure 2. The main results of the process are:

- the process and/or asset register,
- the risk identification register,
- decision on range of value for probability and impact of risks, and calculation formula;
- the risk assessment register,
- decision on acceptable risk,
- the risk treatment plan,
- the risk treatment action plan,
- the risk measurement/monitoring log.



- **Establish the context for risk management**
  - Define the scope of operations to be covered by the risk management process, preferably entire operations.
  - Identify process and asset related risks
- **Regular risk assessment**
  - Evaluate bare risks based on algorithm set and the grading scale defined in the risk management methodology
  - Assess the impact of current controls on the bare risk and evaluate the current risk levels
  - For current risks above the level of acceptable risk, define risk treatment options and evaluate the level of residual risks.
  - Specify the risk treatment options into a feasible Risk Treatment Action Plan with timeframe, responsibilities, deadlines, indicators, necessary resources.
- **Risk monitoring**
  - On regular intervals (at least every 6 months) check the progress on the Risk Treatment Action Plan
  - On regular intervals (at least annually) check if new risks can be identified, review the risk assessment, assess the real impact of the risk treatment options and update the Risk Treatment Action Plan.
  - Continually monitor for risk realization and document the real impact of the risk when it happens.

Fig. 2. Diagram of the phases in the Risk Management Process

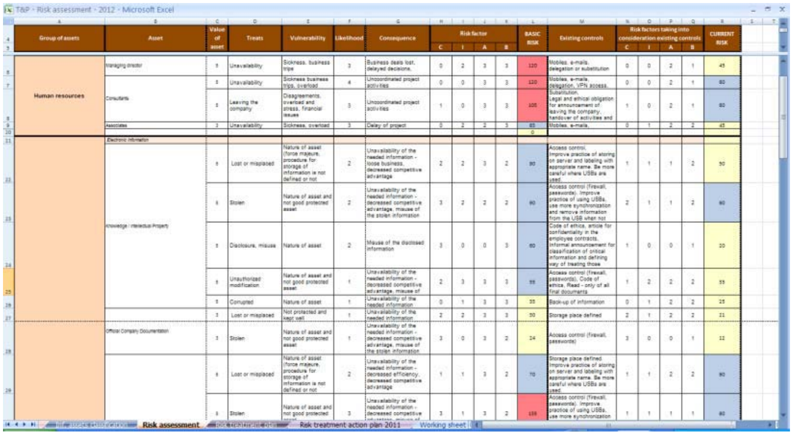
4.4 Tools

Risk management toolkit is a usable software tool (spreadsheet or more advanced software) for gathering, calculating and presenting risk assessment results as well as other related information. It can include:

- the process and/or asset register,
- the risk identification register,
- the risk assessment register,
- the risk treatment plan,
- the risk treatment action plan,
- the risk measurement/monitoring log.

The benefits of using a toolkit is the automation of the calculations required for the risk assessment (Figure 3), as well as possibility for manipulation of the risk management results for better and more understandable presentation which will allow for adequate decision making by the management.

The toolkit should allow a maximal human influence on the results, as the risks identification and their assessment cannot be automated and still provide a usable result for the IT centric micro and small enterprise.


T&P - Risk assessment - 2012 - Microsoft Excel
Risk assessment
Risk treatment action plan 2011
Working sheet

Group of assets	Asset	Value of asset	Treats	Vulnerability	Likelihood	Consequence	Risk factor				BASIC RISK	Existing controls	Risk factors taking into consideration existing controls				CURRENT RISK
							C	I	A	B			C	I	A	B	
Human resources	Managing director	5	Unavailability	Sickness, business trips	3	Business deals lost, delayed decisions.	0	2	3	3	120	Mobiles, e-mails, delegation or substitution	0	0	2	1	45
	Consultants	5	Unavailability	Sickness business trips, overload	4	Uncoordinated project activities	0	0	3	3	120	Mobiles, e-mails, delegation, VPN access,	0	0	2	1	60
		5	Leaving the company	Disagreements, overload and stress, financial issues	3	Uncoordinated project activities	1	0	3	3	105	Substitution, Legal and ethical obligation for announcement of leaving the company, handover of activities and	1	0	2	1	60
	Associates	3	Unavailability	Sickness, overload	3	Delay of project	0	2	2	3	63	Mobiles, e-mails,	0	1	2	2	45
											0						
	Electronic information																
	Knowledge / Intellectual Property	5	Lost or misplaced	Nature of asset (force majeure, procedure for storage of information is not defined or not	2	Unavailability of the needed information - loose business, decreased competitive advantage	2	2	3	2	90	Access control, Improve practice of storing on server and labeling with appropriate name. Be more careful where USBs are used.	1	1	1	2	50
		5	Stolen	Nature of asset and not good protected asset	2	Unavailability of the needed information - decreased competitive advantage, misuse of the stolen information	3	2	2	2	90	Access control (firewall, passwords). Improve practice of using USBs, use more synchronization and remove information from the USB when not	2	1	1	2	60
		5	Disclosure, misuse	Nature of asset	2	Misuse of the disclosed information	3	0	0	3	60	Code of ethics, article for confidentiality in the employee contracts, Informal announcement for classification of critical information and defining way of treating those	1	0	0	1	20
		5	Unauthorized modification	Nature of asset and not good protected asset	1	Unavailability of the needed information - decreased competitive advantage, misuse of	2	3	3	3	55	Access control (firewall, passwords), Code of ethics, Read - only of all final documents	1	2	2	2	35
		5	Corrupted	Nature of asset	1	Unavailability of the needed information	0	1	3	3	35	Back-up of information	0	1	2	2	25
		3	Lost or misplaced	Not protected and kept well	1	Unavailability of the needed information	2	2	3	3	30	Storage place defined	2	1	2	2	21
	Official Company Documentation	3	Stolen	Nature of asset and not good protected asset	1	Unavailability of the needed information - decreased competitive advantage, misuse of the stolen information	3	0	3	2	24	Access control (firewall, passwords)	3	0	0	1	12
		5	Lost or misplaced	Nature of asset (force majeure, procedure for storage of information is not defined or not	2	Unavailability of the needed information - decreased efficiency, decreased competitive advantage	1	1	3	2	70	Storage place defined. Improve practice of storing on server and labeling with appropriate name. Be more careful where USBs are used.	1	1	2	2	60
		5	Stolen	Nature of asset and not good protected asset	3	Unavailability of the needed information - decreased competitive advantage, misuse of	3	1	3	2	135	Access control (firewall, passwords). Improve practice of using USBs, use more synchronization	1	1	1	1	60

Fig. 3. Sample Risk Assessment spreadsheet

5 Conclusion

This paper reviewed the risk management concepts, specifically the risk management frameworks, and discussed a newly proposed risk management framework that is designed to reflect the specifics of the IT-centric micro and small companies. The proposed framework is focused on the 4 main elements in risk management: people, policy, methodology and process, and tools. Due to the simplicity and the generalized approach of the framework, it can be used to deal with various types of risks to which micro and small companies are exposed. Its main benefit is that it addresses the challenge of very limited human resources for risk management in the companies.

The open questions which remain are concerned with the availability of adequate models for risk assessment i.e. valuation of risks so that the management of the micro and small companies can compare the various types of risks to which they are exposed, prioritize them and set appropriate risk mitigation controls.

In future work, the authors will focus on development in detail of all the elements of the proposed framework, elaboration of them in detail and specifically identifying a suitable and scientifically valid risk valuation model. The framework and model will then be validated and tested on IT-centric micro and small companies. The results will be used to fine-tune the framework and model to the specific needs of these companies in the Balkan Region.

6 References

1. Aguilar, M. K. (2004). COSO releases a new risk management framework. Accounting TOday, 18(19), 1.
2. Corpuz, M., & Barnes, P. H. (2010). Integrating information security policy management with corporatre risk management for strategic allignment. Paper presented at the 14th World Multi-conference on Systemics, Cybernetics and Informatics (WMSCI 2010).
3. COSO. (1992). Internal Control-Integrated Framework: Committee of Sponsoring Organizations of the Tread way Commission (COSO), AICPA/COSO.
4. Haubenstock, M. (2001). The Evolving Operational Risk Management Framework. The RMA Journal, 84(4), 5.
5. ISACA. (2009). The RISK IT framework: ISACA.
6. ISO. (2008). ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management: ISO.
7. ISO. (2009). ISO 31000:2009 - Risk Management - Principles and guidelines: ISO.
8. NIST. (2011). Managing Information Security Risk, SP800-39 NIST Special publication.
9. Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics, 9(2), 107-118. doi: 10.1016/j.aci.2011.05.002
10. Taylor, C., ;. (2006). The RMA operational risk management framework. The RMA Journal, 88(5), 3.
11. Trajkovski J., A. L. (2012). Overview of risk management frameworks and challenges for their implemetation in ITcentric micro and small companies. Paper presented at the EuroSPI 2012, Vienna.
12. Vorster;, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. Paper presented at the SAICSIT 2005