ISCTE Business School
Instituto Universitário de Lisboa

The impact of IT within organizations – Risks and Security

Carlos Miguel Morgado Ferreira Felício

Project submitted as partial requirement for the conferral of:

Master of Science in Business Administration

December 2010

Acknowledgements

I would like to thank my parents for giving me the opportunity and encouragement to do this Msc. BA. I would like to thank my girlfriend Rita and my friends for the support given during all the steps of this program.

At last, I would like to thank my master colleagues and INDEG members for the great experience that was this master.

Abstract

This dissertation aims to aware and present a critical perspective about an issue that is becoming a top priority in every type of organizational strategies, the risks related to information technology, where is proposed a framework to struggle these questions.

In the first chapter is made an analysis about the growing use of information technologies, where is pretended to distinguish the benefits generated by the implementation of these kind of technologies in organizational processes and the risks/consequences that they carry with them.

In the second chapter are presented concepts about the risks related to information technology, being them distinguish and subsequently characterized.

The third chapter pretends to give an overview on how the IT risks can be identified, measured and, finally, treated or mitigated. Is also presented the purpose and benefits of putting in practice a framework with guidelines, which aims to treat these risks in the operational processes and manage their impact in strategies of organizations.

In the fourth chapter is discussed the governance structure scope extension or its restructuration within an organization, so it can embrace questions related to risks carried by information technologies and the potential value generated by an effective management of this issue.

In the fifth and last chapter, is presented a framework with guidelines that aims to respond to these kinds of risks. This framework resulted from the research and study done for this dissertation.

Key-words: IT risk, IT framework, IT impact, IT Governance.

Jel Classification System: O33 - Technological Change: Choices and Consequences; Diffusion Processes; O39 – Other.

Abstracto

A presente dissertação tem como objectivo alertar e apresentar uma perspectiva crítica sobre uma problemática que se tem vindo a torna uma prioridade em todo o tipo de estratégias das organizações, os riscos associados as tecnologias de informação, onde é proposto um quadro com linhas orientadoras para fazer face a esta questão.

No primeiro capítulo é feita uma análise sobre o crescente uso de tecnologias de informação, pretendendo-se distinguir os benefícios gerados pela implementação destas tecnologias nos processos organizacionais e os riscos/consequências que estas trazem consigo.

No segundo capítulo são apresentados conceitos sobre os riscos associados as tecnologias de informação, sendo eles distinguidos e subsequentemente caracterizados.

O terceiro capítulo pretende dar uma visão na forma como os riscos de TI podem ser identificados, mensurados e, por último, tratados ou mitigados. É também apresentado o propósito e os benefícios de colocar em prática um quadro com linhas orientadoras, para o tratamento destes riscos nos processos operacionais e, gestão do seu impacto nas estratégias das organizações.

No quarto capítulo discute-se o alargamento de âmbito ou reestruturação da estrutura de governação de uma organização, de modo a abranger questões relacionadas com os riscos que as tecnologias de informação acarretam e o potencial valor gerado por uma eficaz gestão desta problemática.

No quinto e último capítulo, é apresentado um quadro de linhas orientados que visa dar resposta a este tipo de riscos. Este quadro resultou da pesquisa e estudo realizado para esta dissertação.

Palavras-chave: Risco de TI, Quadro de TI, Impacto das TI, Governação de TI.

Jel Classification System: O33 - Technological Change: Choices and Consequences; Diffusion Processes; O39 – Other.

Index

List of Abbreviations

IT	Information Technology
MAR	Modelo de Avaliação de Risco
ITGI	IT Governance Institute
BIA	Business impact analysis
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management

List of Figures

List of Tables

Executive Summary

This dissertation aims to aware and present a critical perspective about an issue that is becoming a top priority in every type of organizational strategies, the risks related to information technology. In the end it is proposed a framework or a way to organize some areas and management aspects of an organization to struggle these questions.

The first chapter starts with an overview about the increase deployment of technologies within organizations over the last decades, which result on businesses dependency on them. With this fast adoption of technologies it is essential for business to understand the benefits provided by them, but also the consequences of not manage them efficiently and effectively. These two sides are analyzed and shown by examples. The end of the chapter focus on the damages cause to an organization that is not aware or doesn't understand the risks implied on the current or future deployment of technologies.

In the second chapter are presented IT risk concepts. Starting with the basic concept of what is an IT risk, it is after shown how they can be classified by their business impact and categorized. There are five categorization where IT risks can be divided, being them availability, access, accuracy, agility and compliance. All the five categorization are described and some case studies are shown to exemplify the damages cause by them.

The third chapter pretends to give notions on how IT risks should be managed. To manage IT risk, organizations must put in place and develop certain activities with objective to make IT risk understandable so they can think with accuracy about the present having in mind the future, extracting the most value possible in every strategy where technology is inserted.

One of the key decisions is the implementation of an effective, systematic and efficient mechanism to address IT risk. During this chapter is described step by step a methodology that aims to identify, quantify and treat technology risks. The objective here is not to go deeply about the methodology, but to give a broad view about the importance of having an IT risk framework that analysis and treat these issues, and how to deal with IT risk.

In the fourth chapter is discussed the governance structure scope extension or its restructuration within an organization, so it can embrace questions related to risks carried by information technologies and the potential value generated by an effective management of this issue. This state can only be achieved when an organization knows deeply about its IT risks and have a well structured mechanism to address wisely investments on IT.

During this chapter are presented concepts about IT governance and its five domains, strategic alignment, performance management, resource management, risk management and value delivery.

At the end is presented a proposal framework with guidelines that aims to respond to these kinds of risks. This framework is composed by three pillars, IT foundation structure, IT risk framework and IT awareness culture. To support and obtain results from these pillars it is proposed a monitoring process that aims to make the bridge between the pillars and the last component of this framework IT governance framework, providing constantly information to management about organizational IT risks and how the organization is responding to them. The objective of having an IT governance framework is to ensure that the information provided is well understand and is considered when decisions must be taken.

IT within organizations

IT overview

Over the last decades, markets and life style trends have been changing constantly, resulting in tough challenges for organizations to follow all these shifts. The life cycle of products had decrease, and answering to customers satisfaction has become a more exigent task. These facts are justified by the globalization that made countries different markets in one very competitive world-wide market. Customers, more than ever, have easier information access which allows them to support their consumption decisions regarding what they are looking for in a more precise way, they become more exigent.

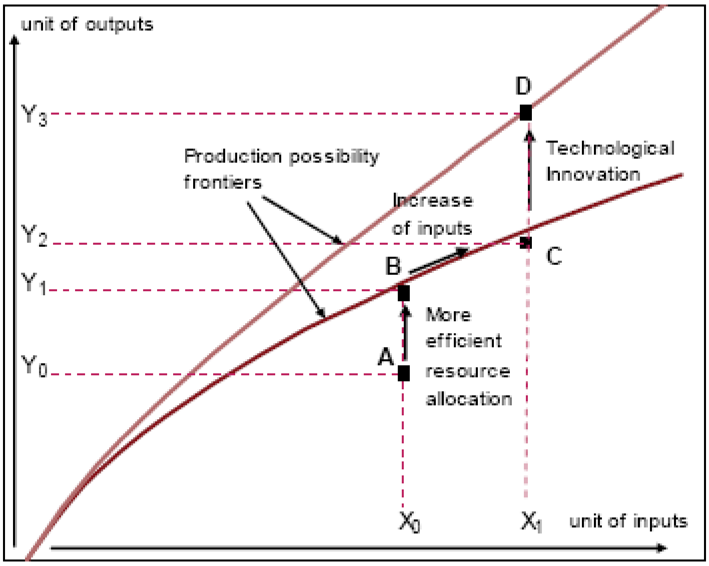
The current environment that markets face, forces companies to seek for at least one competitive advantage, in order to struggle both for its survival and its success. Organizations must be one step ahead comparing to its competitors, this means that they must have a real picture of the present and also the creativity to design the future.

This competitive advantage in the past was easier to find. Geography is one good example. If we go back years ago, when the transports sector was not so developed, an organization that had a good strategic location had a bigger advantage comparing to its competitors. Nowadays, because of technology innovation, the spending in education by countries, the development of some industries, the funds that governments distribute, are all factors that facilitate businesses, but in the other hand, make them difficult to find the competitive advantage, the factor that makes an organization leading a market.

Considering this, information technology (IT) plays an important role in the organizations life nowadays. IT has been started to be viewed as a weapon that can creates the desirable competitive advantage. It has the potential to burst business toward a higher performance and enable new opportunities.

IT benefits and issues

Many companies achieve a good level of success without investing much in IT. But at some point, to continue its successful growth path or to maintain its position, only the use of IT can improve organizations efficiency and performance.



[1]

Figure 1 – IT Investment Benefits

The graphic above shows how a company can achieve a higher production rate with the minimum required resources. We have two curves that represent the correlation between X input units and Y, output units. This means that with the X units we can produce Y units. From point A to D we can follow a low efficient to a high efficient company, the benefits that some investments create with impact on production performance. If a company is currently in point A, to move to point B it must eliminate some production inefficiencies by allocating better its resources. In point B, is possible to produce more output with the same resources of point A. If the company increases the input of capital, there's a shift to point C to a higher output production. Finally, for the maximization of output per input units, the company has to invest in IT, represented by point D. In this point there's a shift to another curve where production reaches the most efficient point.

[1] From: Goldman Sachs Economic Research, http://www2.goldmansachs.com

As we can see, IT plays a big role in organizations performance and far beyond, creates conditions for a sustainable growth - it's the trigger that allows the organizations to maintain or increase their development, in order to reduce the gap that separates them from its competitors.

It is known that IT has a lot of benefits. Many studies in this area concluded that IT brings many advantages, besides the efficiency in production, IT among others:

- Helps organizations to lower costs, by for example the automation of repetitive tasks;
- Increases the levels of innovation within organizations;
- Manages a high-value and sensitive information, and delivers accurate analysis of this information on behalf of users;
- Optimization of processes performance;
- Allows businesses to be closer to customers, partners and suppliers, by synchronization of interactions among them;
- Helps in meeting regulatory and audit requirements. These can be achieved through automated reporting procedures that give feedback regarding organization compliance to regulatory and industry-accepted best practices and policies that cover all IT architecture and structure.

IT delivers substantial value to businesses, but the most important factor is that it facilitates the provision of customer services at an economically viable cost for the organization, as clients demand faster payments and faster response to their requests.

The case study of Maggiore Group demonstrates a good example how IT can affect business, bringing a big set of advantages.

The Maggiore Group is one of the Italy's leading car rental companies, with an 11% market share. It has physical location in 140 regions, with its headquarters in Rome. Maggiore manage 14 branches directly, and has more 126 independent franchises.

The car rental industry has suffered many transformations over the last years. The development of technologies, such as the internet has created opportunities but at the same time many threats to companies which didn't innovated in obtaining or re-adapt tools to take advantage of the opportunities created. It is an industry where became hard to create customer loyalty and where the business requires a lot of efficiency and effectiveness to answer customers demand. One of the challenges for Maggiore was the inter-offices communication. The need for manage all its 13.000 cars fleet and provide employees constant information about customer for faster response, in order to improved service quality, made the company invest in a new telephony platform. With the current analogue telephone system, Maggiore also had other issues. This system was not flexible enough to follow company changes. Typically per year, the company opens and closes 15 to 20 offices. Another issue was the telephone bills that were increasing because of the volume of the inter-office calls that were made over the public telephone network at normal rates.

Regarding all these issues, Maggiore decided to implement this new platform. Focusing also in the future this new system at the same time allowed the company to become prepared for changes in its applications such as videoconference calls, video telephony and implementation of an effective call center making the communication system more unified. As the head of the IT department, Simone Saponaro explained:

“We were encouraged to find alternative solutions to traditional technology by the need to equip the Group with a modern, effective telephone management system”[2]

In January 2006, Maggiore initiated the implementation process of the new system, which was completed after seven months. This quick installation was a great advantage for the company says Saponaro:

“The compressed timeframe for the implementation was a great advantage in business terms”

Later, the company analyzed its investment and showed the results. They were great, the system shown to be extremely efficiency. Due to the internal network, Maggiore telephone bills decrease 40%. Maggiore was managing customer calls more effectively, improving service and customer satisfaction level, by answering calls more quickly and dropping ‘on hold’ amount of time spent. The lost calls were reduced to near zero, ensuring that potential customer do not take their business to competitors.

IT staff at Maggiore particularly value the flexibility and the user friendly interface that the new system provide. These advantages allow them to respond to

[2] From: Cisco Systems customer case study, 2007

changes that might appear in the business, more quickly and cost effectively. They also can manage changes from the headquarters, which also ensures a minimal disruption to the business, boosting productivity and reducing operating costs.

At last, the company is fully integrated with the same system, a fully scalable system. This benefit improved internal communication and reduced the need for re-training when staff moves offices.

Maggiore benefits much due to this new system. The investment brought value to the business. It made company business requirements more effective and controllable. It increased company efficiency, effectiveness, scalability, robustness and adaptability. Maggiore become even more competitive, making it prepared to growth sustainably, by the opportunities that were created.

Nowadays, it is hard to think how companies can do business without the deployment of IT systems. IT plays a more sophisticated role. IT helps organizations to implement their strategies and reach high levels of competition, allowing them to continue to struggle for an increase in their market share, or to grab important opportunities that make the organization stronger.

Consequences

Today we live in a society where technology is present in our daily routine. It is hard to think how we could manage our tasks without the support of technology. It’s not only the tool which allows us to accomplish our jobs, but also a source of pleasure, our well being. The astonishing rate of innovation changes the way we live, the way we think and most important our habits. With all these changes, companies had to follow and adapt to trends of a constant changing society. Therefore, technology changed the way of doing business.

This reality of innovation made organizations dependent and interdependent on IT, and this factor has tendency to increase even more.

Together with all these shifts, the consequences of IT risks have increased as well. From all the benefits that IT carries, it is extremely important that organizations must be aware of the consequences of using IT, to be prepared to answer the question “What happens when it goes wrong?”. A simple IT incident has the potential to produce substantial consequences that touch a wide range of stakeholders, and mainly the continuity of the organization. IT carries risks.

One of the first risks that come to people mind is the security attacks. A simple intrusion into an organization can bring enormous losses which can result into the organization ending or a tough recovery period to walk. A study[3] conducted by Ernst & Young in 2008 shows clearly the impact of information security incidents, from the base to the top of an organization. Figure 2 shows the results.

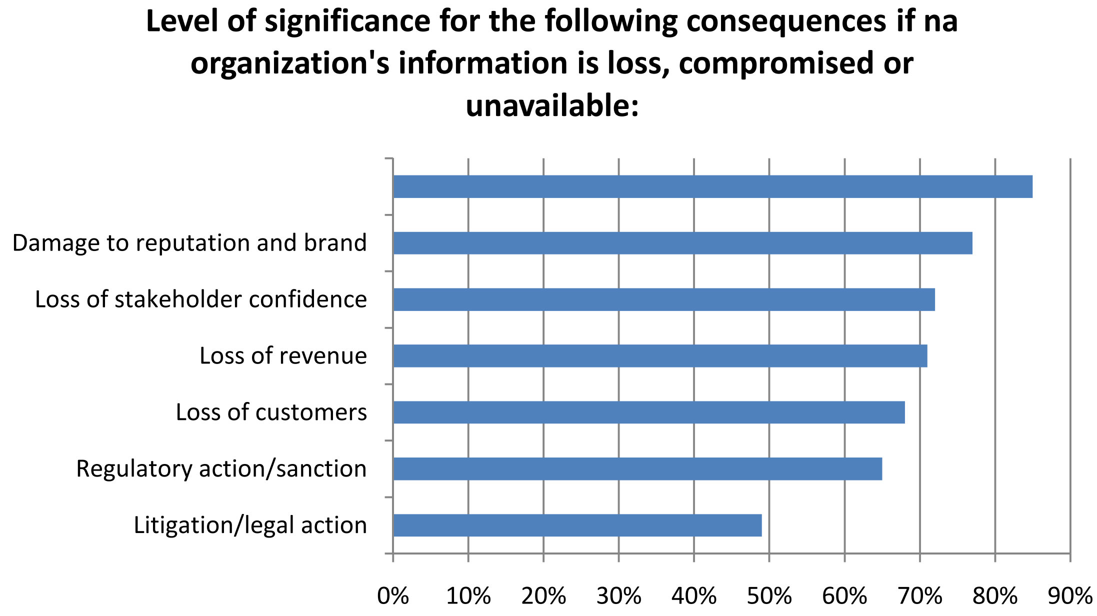


Figure 2 – Consequences of information security incidents

The biggest consequence with 85% is the damage caused to the reputation and brand. With this result we can conclude that companies are extremely vulnerable to this kind of incidents. Reputation and brand recognition can take years to build, but can be severely damaged by a single incident. This factor can be followed by the loss of customers that start not trusting the brand and move to the competitors, and consequently the loss of revenues. We also have to consider the additional money that must be spent to recover company's reputation.

The types of failure that need to be considered became much more complex since the almost business universal adoption of every kind of systems, distributed

[3] http://www.ey.com/PT/en/Issues/Managing-risk/Information-security-and-privacy/Assurance---Advisory---Technology-and-Security-Risk---Global-Information-Security-Survey-2008

systems, direct Business-to-Business and Business-to-Customer transactions, remote and mobile access and portable storage media are just a few examples. They include short or long term applications loss of access, the corruption or destruction of information, the possibility for information fall into the wrong hands, internal fraud, and the failure of vital systems belonging to partners or suppliers.

Whereas IT risk was considered to be a strictly back-office problem, today almost every aspect of a business is exposed to IT risks. IT is present, even some times unseen, in nearly every business process. By this reason IT risks may not only be detected by the IT department but also by the other business units, due to the complex business dependency on it and the business processes it supports. For example, a failure on a server may not cause only damages in the applications it supports, but also cause a cascading effect of further failures in other machines. If the data is rerouted to another server already in use, the increased load volume may cause it a failure as well. Therefore, the applications that are supported by the last server may fail too, and these fails may cause further failures to other systems/applications which rely on these servers. Figure 3 illustrates the interdependencies among the various IT components.

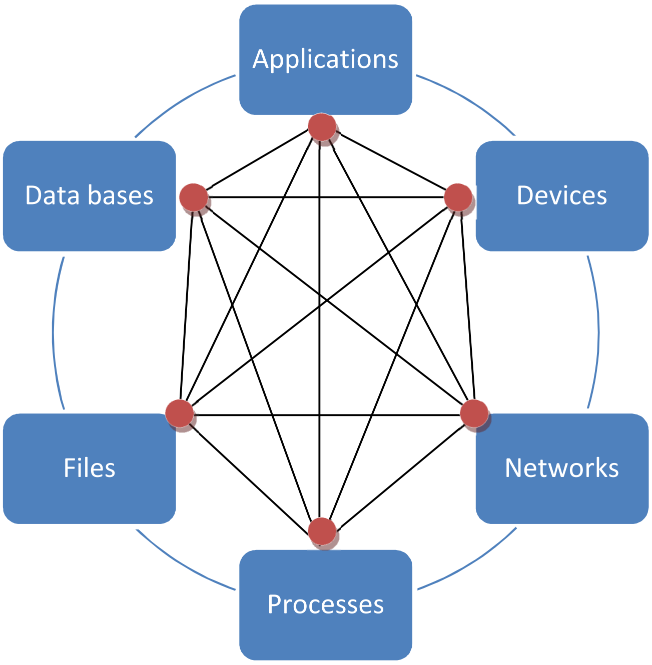


Figure 3 – IT components interdependencies

IT may fail for different causes and in many different ways. Sometimes a failure is immediately detected and the organization can avoid big financial losses by taking measures to solve the problem, or a failure can be subtle, causing cumulative damages that might go unnoticed for a long period, causing huge financial losses.

Every organization at some time already experienced problems with IT systems, as delays, unexpected costs in developing projects, temporary loss of service, incorrect data, processes made unnecessarily complex by the type of applications and their limitations.

The Comair case study[4] exemplifies well how IT risks can affect business, as being big threats to organizations.

Comair is a $780 million subsidiary of Delta Air Lines. In December 2004 it experienced an IT risk incident, when the crew scheduling system failed. This system defines the flights schedules and manages the crew to the correspondent flights. It also ensures that the flights meet the regulations defined by the Federal Aviation Administration. Without its scheduling system, an airline does fly, therefore, it is considered as a critical system.

For several years Comair was delaying the deployment of a new crew scheduling system. This was the oldest system that the company had. Late in 2002, the Comair IT team turns its attention to the crew management system and brought in several vendors. After some demonstrations, Comair got approval from Delta to replace the system. One vendor was chosen to provide and to implement the new system. Implementation was set to begin in 2005. But by then, it would be too late.

Because of the holidays, December is one of the busiest seasons of the year for this type of companies. December 2004 was busier than normal. A severe winter caught Ohio Valley with snows and freezing rains. This situation forced the airline to delay, to cancel and to reschedule many flights, 91 percent of all flights between 22nd and 24th of December. This situation was seriously threatening the airline, since no one at Comair knew that the crew management system could only process a maximum number of changes, 32,000 per month before shutting down. That's exactly what happened on Christmas Eve, when Comair entered one more flight change, exceeding the monthly capability, the system stopped functioning.

[4] CXO Media Inc (2010), Comair's Christmas Disaster: Bound to Fail, http://www.cio.com/article/112103/Comair_s_Christmas_Disaster_Bound_To_Fail

Comair technicians realized soon that the system was not able to be restarted. The only solution was to load the entire system as quick as possible. A Comair team supported by the software vendor specialists started the re-load process late on 25, but was only accomplished on December 29.

As a result, Comair had to cancel all 1,100 of its flights on Christmas Day, affecting thousands of passengers. Throughout the Christmas holiday, reporters from local and national television news followed passengers through airports terminals, broadcasting travelers and Comair distress to the American public.

Two weeks after the system crash, the US Secretary of Transportation announced an investigation on this incident. A week later, the company CEO Randy Rademacher resigned. In addition to the damage to the company's reputation, to its management, and its customers, Comair estimated that their losses were about 20 millions. This means that the damage of a single incident cause almost the same loss comparing to the previous quarter operational profit of 25 millions.

During many years, Comair had planned and delayed a new crew management system several times before it failed. But something more was involved than an unfortunate decision to defer an upgrade. When the system went down, there were no backups that could be loaded immediately to attenuate some losses. The airline lacked a viable plan for the immediate disaster recovery of its critical business processes. Comair executives failed to plan for such a high impact failure.

The Comair case study is a good example how IT risks can impact businesses. Despite its likelihood, a failure can create huge damages, affecting businesses in many ways. A special attention to these issues must be taken by executives, in order to maintain organization up to date regarding both their internal (business capabilities) and external environment (market need). Therefore, the Comair system failure wasn't the only problem, it was Comair's process for understanding and managing the businesses consequences of IT risk that fails.

IT risk an issue

In recent years, we have been assisting a huge proliferation of information technology in businesses. Actually, their objective to support critical processes and operations creates a tough task in managing them. All the different systems are being organized in complex, dispersed and heterogeneous environments.

The Comair disaster is a typical example of failure of what can happen to any kind of organizations. It exemplifies the importance to have in place processes, methodologies that look for IT risks. Comair IT executives should have done the kind of risk management analysis that would alert Delta to the dangers, in this particular case, of not replacing the system. And IT department should have repeatedly brought that analysis to the attention of Delta board until its replacement. But in other hand, Delta executives should have had the responsibility to impose and insist in examining these kinds of issues in its all subsidiaries.

After the incident the former Delta executive said:

"Anything that can damage a parent company's brand or reputation has to be managed in some way. Risk assessment of worst-case scenarios at Comair should have happened at Delta."

Comair's failure is just an example of incidents that happen every week. Over the last twenty years, companies became more dependent on IT systems in order to achieve a higher performance. But many organizations do not adapt their businesses regarding IT and IT risks decisions. For George Westerman and Richard Hunter (2007), the result in these situations is risk incidents that have three factors in common:

- "They involve significant harm to constituencies inside and outside the enterprise that results from failure of IT systems or controls on IT processes."
- "Increasingly, they involve public disclosure, resulting in reputation damage and regulatory scrutiny. Such public disclosure amplifies the consequences of IT risk, with subsequent consequences sometimes far exceeding the initial economic losses."
- "They expose failure to account for potential businesses consequences in managing It risks – in other words, they expose a failure of general management, not just IT management."

Executives who are aware of the potential of IT, and wisely invest on it, simultaneously increase their company's exposure to IT risks. By depending more on IT systems for streamline and optimize their processes, they increase their dependence on the IT availability, which increase as well their vulnerabilities and threats.

Easily arise us the question, are companies aware of these issues and their consequences? Many executives do not yet understand the implications of this shift. Management of IT risk hasn't been following the reality of businesses IT risk. IT risk is still handled as a technical issue, as not being a main concern and many times ignored by business executives.

Considering this issue, the main purposes of this thesis is to enhance the importance of having an IT risk management strategy in practice and to propose a way on how it can be done, in order to avoid these unexpected events that can lead to huge damages and which can take several years to recover. IT risks management must be a top priority in the overall organization's strategy.

IT Risk

Definition of IT risk

> "*1. expose to a chance of loss or damage;*
>
> *2. a source of danger; a possibility of incurring loss or misfortune;*
>
> *3. a venture undertaken without regard to possible loss or injury;*
>
> *4. take a risk in the hope of a favorable outcome;*
>
> *5. the probability of being exposed to an infectious agent*".[5]

As we can observe, risk definition is widespread and covers a lot of issues. It doesn't imply for a single definition, but we all agree than risk is an event that prevents an organization to reach their goals and objectives, making the organization slowing down its aspirations.

Risk to the business might come from many sources, both internal and external to the organization, as: economic, geography, political, social-culture, regulatory, operational, financial, market, technology, people, etc. IT risk is the business risk associated with the use of the information systems, from the adoption of them, to over all their life cycle, including what is need to do to keep them useful to fulfill their objectives. IT risk consists of IT related events that may possibly impact the business. Which risk has its own uncertainty frequency and impact. It creates challenges and barriers in meeting the strategic objectives as well as uncertainty in tracking opportunities.

A risk IT framework design by the IT Governance Institute, categorize IT risk in different ways, regarding the purpose of IT has within organizations:

- IT service delivery risk, linked with the performance and availability of IT services, which can affects negatively the value to the organization;
- IT solutions delivery risk, linked with the benefits that IT can bring to the business solutions.

[5] From: http://www.lookwayup.com

- IT profit realization risk, linked with opportunities to use technology to improved business processes efficiency and effectiveness, or as an enabler to new valuable initiatives.

Thus, having in account the impact that risk can have in each function, process and application, risk assessment can be classified through a scale used by the *Banco de Portugal*, *Modelo de Avaliação de Risco* (MAR):

Risk Classification	Description
Low	The likelihood of negative impacts to the organization by vulnerability is low.
Moderate	The likelihood of negative impacts to the organization by vulnerability is not significant.
Material	The likelihood of negative impacts to the organization by vulnerability is significant.
High	The likelihood of negative impacts to the organization by vulnerability is high.

Table 1 – Risk Level Classification

Whether or not IT risk is detected or recognized by an organization, it always exists.

IT Risk Categorization

To understand how IT risks affect business, any IT risk must be understood in terms of its potential to affect all organization goals and objectives that are enabled by IT. Risk categorization helps in understanding the risks inherent to these objectives.

Risk categorization must be used by organizations**.** Putting in practice this best practice, it allows business and IT staff to discuss IT risk in the same terms and to develop an integrated view of the business threats created by IT risks. These two points create an enormous advantage, it makes communication easier within all organization and also makes simpler the risks addressing.

Based on the 4A Framework designed by George Westerman and Richard Hunter (2007), IT risks are categorized with the association of each concerned requirement that should be considered when analyzing its categorization, in the following way:

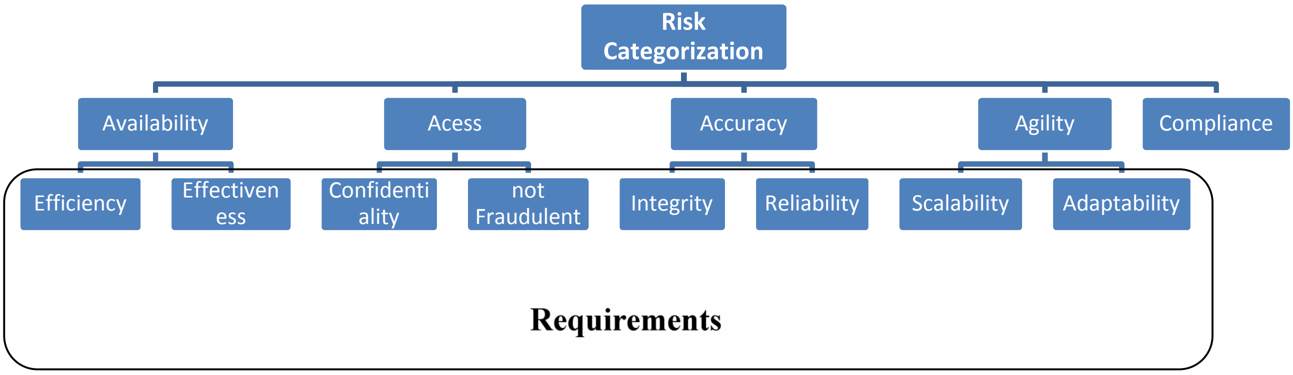


Figure 4 – IT Risk Categorization

Availability

Make the systems running ensuring that requests from business processes are fulfilled, and in case of an interruption occurs, make them recover. This categorization ensures efficiency and effectiveness of the systems.

The Comair's case study described above is a good example on how systems availability is crucial for business.

Access

Guarantee that information and systems access is restricted to the right people. This categorization ensures confidentiality of data and avoids frauds.

Example

Société Générale, one of the largest banks in Europe was in 2007 victim of the biggest trading fraud ever, which resulted to the bank losses of more than 4,9 billion Euros. The biggest loss ever recorded in the financial industry by a single trader.

The trader Jérôme Kerviel, the responsible for the scandal, joined Société Générale in 2000 and worked several years in the bank's French risk management office before being moved to its Delta One trading desk in Paris.

Between 2007 and 2008, Jérôme who benefited from the knowledge in control procedures he acquired while working at risk management office, conducted huge fraudulent actions beyond his limited authority through a scheme of fictitious transactions he elaborated.

The fraud was discovered by an audit conducted by the risk management office team when they checked Jérôme trade books.

This event brought several problems to Société Générale. Despite the financial loss, stakeholders and clients raised many questions about the bank risk control management.

If one single trader could manage a fraud of this scale, it means the organization had big weaknesses and wasn't deploying efforts in risk management. By this reason many institutions saw this case as a lesson applied not only for banks but for all kind of companies in every industry.

Accuracy

Information provided by the systems is correct, timely and complete, meeting the requirements of business. This categorization ensures integrity and reliability of data.

Example

In the late 90's, the Dutch ministries started to reconsider the performance given by their information systems. After an analysis on their current situation and the needs for further changes that the systems were going to suffer, as the introduction of the Euro, resulted on a reform program to accelerate the process of financial accounting. The main goal was to improve the performance and quality of this process.

The solution to achieve this objective was the deployment of an ERP that could link several ministries. A huge project as this one needs a lot of resources and more important experience resources. Each department has their own systems and as a result the data management is completely different from each others. The implementation of an ERP must be done very carefully and detailed, so that full integration must be accomplished successfully to ensure data integrity and reliability.

After the implementation of the ERP, an audit company was contracted to conduct annually audits to the governmental systems.

Over the years the audit team found a number of issues:

- the Ministry of Foreign Affairs (in 2002) and the Ministry of Social Affairs and Employment (in 2006) experienced data conversion problems;
- in 1999 and in 2005 the Ministry of Economic Affairs showed repeated deficiencies on authorization management;
- The Ministry of Defence (in 2004 and 2005), the Ministry of Social Affairs and Employment (in 2005 and 2006) and the Ministry of Foreign Affairs (in 2002) were unable to ensure data reliability.

After all these issues experienced by all kind of ministries, the Netherlands Court of Audit conclude that most ministries made the same mistakes when developing the change for the new system and when they start to implement it. In this example we clearly understand the problems caused to data when occurred the conversion and the migration of it to the new system. When the implementation of the system was completed, they realized that when doing operation in the system the data was not complete and with inconsistencies, and so the information provided from the system was not fully reliable. Easily we understand the results as financial losses, operational incidents and the impact cause to the population generated by the inaccuracy system data problems.

Agility

IT has the capability to change regarding business needs. This categorization ensures scalability and adaptability of the systems.

IT systems complexity

The speed and complexity of doing business is one of the main factors that lead to the deployment of complex IT systems. When businesses start, typical start with a simple system that aims to support the main processes and to give output with important information for analysis. But during the life cycle of businesses many decisions are taken and IT systems are updated and changed. With these changes systems became more complex which increase the number and the likelihood of risks and the cost and effort involved in maintaining them.

These kind of situations easily happen or are amplified by mergers and acquisitions. We just have to think that every organization has a different way of managing IT systems, supported by the broad variety of solutions that the market has to offer, making companies decisions in the one that match better its needs. We also have cases where companies invest in tailor-made software's. Now, when an M&A happens, instantly the company who buys the other company also buys a new IT environment and consequently the challenge to learn how to deal with it.

Many CIO's are aware about what can systems complexity can cause to the organization, and they are conscience that the cost of maintain and operate them is far more expensive than a new newer technologies. That cost and the increased opportunity cost it implies is a constant pain to the IT team, but when executives compare it with the cost and effort of changing the system, it often seems not a trivial decision.

Managing IT is not a simple task, it embrace a lot of issues, most of them with direct impact in business. System complexity is one of them which carry a lot of risks, the operation of critical processes and mostly barriers to CIO's in planning strategies and enabling opportunities to the business.

Compliance

Ensure that information meets legislation demands, as well as, internal and external regulation and contractual obligations that business processes are subject.

The arrival of the new millennium brought a series of coordinated acts of terrorism and a number of massive corporate scandals as for example Enron. These events highlighted the fact that economies can have big repercussions and a long recovering time. The proliferation of new technologies and communication platforms had created enormous opportunities for fraud, money laundering or any other kind of illicit financial activities. By this reason, over the last years many kinds of standards, regulations and best practices were created in order to protect organizations from malicious events. Nowadays, having in mind the events of the last ten years almost regulation entities from countries obliged mainly financial institutions (because of their impact in the country's economy) to implement some of these standards. IT makes part of these standards, some specifications and configurations are recommended as minimum to guarantee that systems are protected, reliable and do not fail. Businesses dependency on IT increased and so, being compliance is today one of the top priorities for organizations, as it is mandatory (for some industries) in one side and in the other it brings advantages as gain suppliers and customers confidence in the organization.

Categorization the IT risks when analyzing them, allows organizations to have a big picture of where their threats and vulnerabilities are. Therefore, they are more capable to allocate investments in such risks that have a higher harmful profile. Without such method, there's also a much danger of overinvestment in treating risks as there is underinvestment.

IT Risk Management

The combination of the increasing types of risk to which IT systems are exposed and the increasing of the business dependence on IT, results in the need for organizations to take a systematic, repeatable and analytical approach to manage IT risk through an IT risk holistic view creation.

When we talk about this kind of approach, we talk about rigid processes, procedures and politics in place. To manage IT risk efficiently, organizations must establish a framework designed according their business needs.

In this chapter, we are going to focus on the most important phases of an IT risk management framework, in order to better understand how works the mechanism for IT risk identification and treatment. Through theses points we will realize its importance and the benefits it can bring to businesses when it is correctly implemented.

Purpose

Every organizational decision taken is accompanied by risk. For this reason management of business risk is a critical and essential area that companies must consider, in order to balance their associated risk and benefit in every decision.

Due to IT's importance to the overall business, IT risk must be treated like other business risk. As we have seen, IT risks are as important as financial risks or operational risks, they create damages that avoid organizations to achieve their strategic objectives. The issue that remains is that many executives and boards aren't aware of IT risks impact to business. While other risk are incorporated into corporate decisions, IT risk is still viewed has a problem that should be solved by technical specialists outside the boardroom. An IT risk management strategy initiative should be viewed as a critical subset of the broader enterprise risk governance process.

The purpose of an IT risk management supported by an IT risk framework focus in explaining the current IT risk that organizations face, this means show up IT related threats. It also enables executives to design and integrate IT risk management strategy that best match the organization needs, enables executives to make well informed decisions about the extent of the risk (for example if the organization supports or not that kind of risk, or how can executives decisions go with a controlled risk – risk adjusted decisions). At least and the most important aspect, an IT risk management framework gives answers how to respond and tackle risk.

In summary, an IT risk management framework provides a holistic view of organizational threats related to its IT systems.

IT Risk Management Framework Benefits

The implementation of an IT risk management framework leads to a big organization efforts. It requires specialized staff with deep knowledge on this area and it requires time to organize and to put in practice the framework. In almost every case organization has to change or create/apply many procedures, processes, technology and people. It takes time but after its well deployment, it brings enormous benefits, creating value to the organization future investments.

Having a reliable approach for IT risk management by the organization, leads, immediately, to confidence results to investors. A survey conducted by Ernst & Young (2007) revealed the following results:

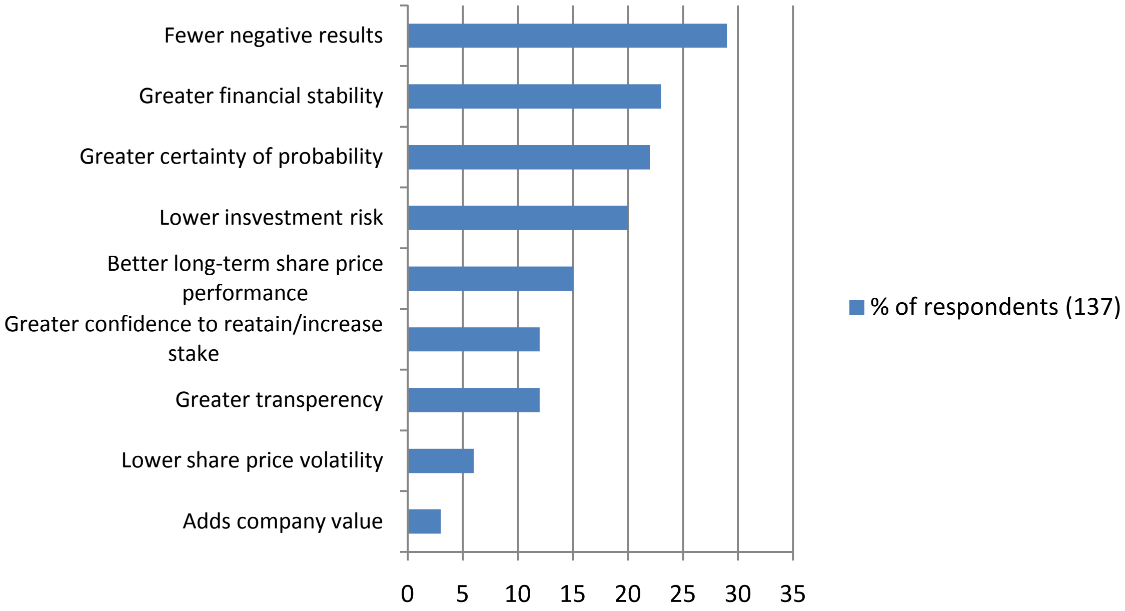


Figure 5 – E&Y Investor Risk Survey Results

From the perspective of the investor we can see above that the results embrace very wide aspects that affect not only IT issues but the overall business.

However, the results from figure five came from lower results, the ones directly connected from the implementations of the risk management framework. These results are what we name as the benefits of having in practice a framework:

- IT risk holist view;
- how to manage IT risk, beyond merely technical aspects;
- how to direct the investment on the current IT risk internal controls;
- ensure that risk assessment covers all IT risk within organization;
- a common language which helps to manage the relationships among the different organization levels;
- better understanding of risks profiles that allows the organization to organize better its resources.
- IT risk responsibility promotion;

A well established IT risk management framework guided on a set of approved standards that ensure the requirements (being systematic, repeatable and analytical) raises the confidence level among the individuals of the organization and outside organization. A risk management framework creates a picture of the overall current threats and vulnerabilities within organization and therefore the picture of the corporate tolerance to IT risk. For this reason it should be a top priority strategy, which helps to protect the present and secure the future of business.

IT Risk Assessment

Risk emerges from many factors as changes (people, processes, systems, and technology), external influences (regulatory, legal, economic, competition), complexity of processes, and volume of process activity. By the dependence of business on IT, every of these factors emerge IT risks.

The IT risk assessment is a complex process which needs collaboration from all individuals of the organization levels. The objective of this process is to identify, assess and prioritize business IT key risks across the organization, this means that risk assessment provides an insight point of view on significant inherent risks from an industry perspective, and links them to the organization objectives, strategies and business processes. It also helps management to validate and prioritize key risks to monitor or test, and defines opportunities for controls improvement and management activities.

As we can see on figure 6, the risk assessment is composed by several phases where each of them depends on the previous one. This process is based on the Risk Management Guide for Information Technology Systems (2002) design by the National Institute of Standards and Technology.

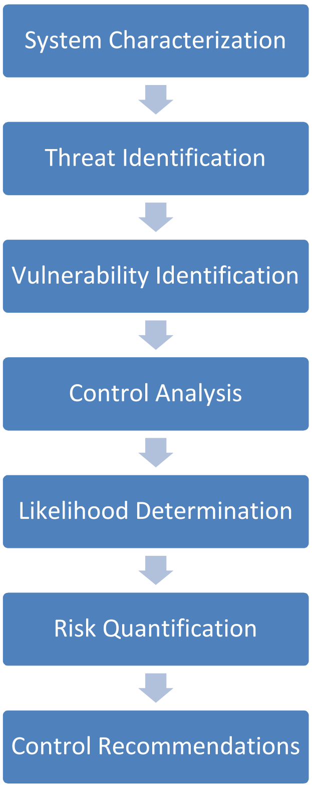


Figure 6 – Risk Assessment Process

To have a well structured risk assessment an organization has to ensure that each of these steps are being well managed and well guided. In the next topics we are going deep on each of these steps to better understand all the mechanism and also the effort they need in terms of resources and time.

Step 1: System Characterization

The first step of the IT risk assessment is to define the scope of the analysis. Usually the scope is defined by a board meeting, where they define the boundaries of the IT system and most critical aspects to analyze.

With the scope defined, the next step is to gather information about the systems environment and what support them within the scope:

- Hardware;
- Software;
- Data bases;
- Staff which support the system;
- Information and data of the system.

The information and data of the system is related with the operational environment of the IT system in analyze and include:

- Politics and procedures;
- System administrators and users;
- Users privileges;
- Related processes with the system;
- Changes occurred;
- System architecture;
- System configuration;
- Incidents management process;
- Controls applied within the system
- Physical security

All the information collected must be from the IT systems production environment or at least a copy of what is in the production environment. There are several methods to gather this kind of information as interviews and questionnaires. What must be ensured is that the people who provide the information are the ones who have the best knowledge on the areas requested.

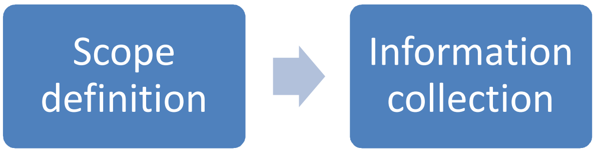


Figure 7 – System Characterization

On figure seven we have the process resume of this step, which starts with the definition of the scope and then with the information collection regarding the scope defined.

Step 2: Threats Identification

With the systems characterized the next step is the identification of threats. Threats are events created by IT external sources which create vulnerabilities on it, this means that a potential threat arises vulnerabilities to the system. Vulnerabilities are system weaknesses that can't respond to a certain threat.

In this step, the main objective is to identify all the potential threat sources that can have impact on the system under evaluation. There are three types of threat sources:

- Human threats, events that are enabled by humans such as hacking and frauds;
- Natural threats, events such as earthquakes, floods and storms;
- Environmental threats, such as power failures.

Human threats are the most critical thread source. This one implies a bigger likelihood of these kinds of events. The table 2 shows the different threats caused by humans and their possible motivation to conduct such acts.

Threats Source	Motivation	Threat Actions
Hacker, craker	-Challenge -Ego -Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	-Destruction of information -Illegal information	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay,

	disclosure -Monetary gain -Unauthorized data alteration	impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	-Blackmail -Destruction -Exploitation -Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	-Competitive advantage -Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	-Curiosity -Ego -Intelligence -Monetary gain -Revenge -Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Table 2 – Human Threats[6]

An estimation of the motivation, resources and skills that is needed to conduct a successful attack should be taken after the threat is detected. This analysis will help to determine the likelihood of the attack and to check the system robustness.

In figure eight we have the resume of this step process, composed by the two phases.

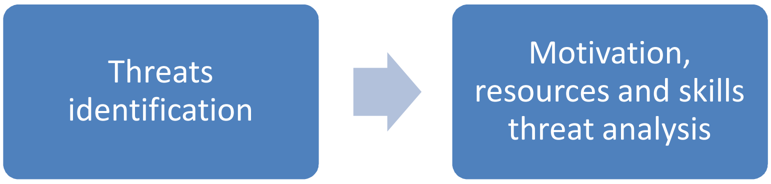


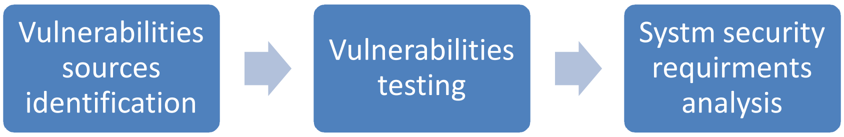
Figure 8 – Threats Identification

Step 3: Vulnerabilities Identification

The goal of this step is to develop a list of the system vulnerabilities that could be exploited by the potential threats sources from the previous step.

The first phase is to identify the vulnerabilities sources. This requires data collection from many sources as previous risk assessments, industry sources, audit reports, vendor recommendations, among others. With the conclusion of this phase we proceed to the system security tests. These tests will help to understand what kind of vulnerabilities exists and its critically level.

After all this process of assessing the vulnerabilities, the final phase is to determine if the system security requirements defined are being met.


Vulnerabilities sources identification
Vulnerabilities testing
Systm security requirments analysis

[6] National Institute of Standards and Technology (2002), Gary Stoneburner, Alice Goguen and Alexis Feringa, Risk Management Guide for Information Technology Systems.

Figure 9 – Vulnerabilities Identification

In figure nine we can visualize the process resume of this step that result in a list of the system vulnerabilities that could be exploited by the potential threats.

Step 4: Control Analysis

The objective of this step is to analyze the current controls already implemented by the organization to minimize past system threats. This phrase is crucial to determine the overall likelihood rating that indicates the probability of certain vulnerability may exercise in the system. For example, the likelihood of vulnerability is strongly correlated with the associated threat likelihood and with the effectiveness of the controls already implemented.

The output of this step is a list of the current or planned controls used for the IT system to mitigate the likelihood of vulnerability's being exercised and reduce the impact of such an adverse event.

Step 5: Likelihood Determination

In this step the likelihood of the potential vulnerabilities are determined. The accuracy of these determinations is only possibly with the success of the previous steps:

- Threat source motivation and capability;
- Vulnerabilities identification;
- Existence and effectiveness of the current controls in place.

The likelihood of a potential vulnerability can be measure in the following way:

Likelihood Level	Likelihood Definition
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat source is motivated and capable, and controls to prevent may impede successful exercise of the vulnerability.
Low	The threat source lacks motivated and capability or controls in place prevent the vulnerabilities from being exercised.

Table 3 – Likelihood Determination

The output of this step is a list with the likelihood rating for every vulnerability.

Step 6: Risk Quantification

In this step, the objective is to assess the level of risk through the prioritization according their quantification by likelihood and impact. To go further the organization must do a big effort to collect all the information need to support this step.

In all this information required is included the BIA (business impact analysis). The BIA prioritizes the impact levels associated with the compromise of an organization's information assets based in assessing the sensibility and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (software, networks, hardware, services, and related technology assets) that support the organization's critical strategies. In case the organization doesn't have this information, it must do this assessment or evaluate the protection required to maintain the systems and data's availability, integrity and confidentiality.

The analysis of all information gathered generate a matrix where the vulnerabilities impact is quantitative and qualitative assessed.

At this point the final quantification is performed by multiplying the ratings assigned for threat likelihood and treats impact. The matrix in Table 4 shows the overall risk levels of High, Medium, and Low are derived. Although, the quantification presented may be subjective, being possible to do it in different ways, always with an explained rationale behind. In the following example the rationale is explained by the probability assigned for each threat likelihood level and a value assigned for each impact level:

Threat Likelihood	**Impact**		
	Low (10)	**Medium (50)**	**High(100)**
High (1.0)	Low 10x1.0 = 10	Medium 50x1.0 = 50	High 100x1.0 = 100
Medium (0.5)	Low 10x0.5 = 5	Medium 50x0.5 = 25	Medium 100x0.5 = 50

Low (0.1)	Low 10x0.1 = 1	Low 50x0.1 = 5	Low 100x0.1 = 10

Table 4 – Risk Levels Matrix[7]

With all risks quantified, the organization has now a clear view of the most critical risks. With this information is now possible to prioritize and direct efforts in an efficient way to implement changes in order to reduce the organization exposure to these risks.

Step 7: Control Recommendations

This is the final step of risk assessment. When reaching this point, we have clearly identified the harmful risks to the IT system and the controls that could mitigate or eliminate the identified risks.

When recommending controls, organizations must consider several factors such as: effectiveness of the recommended options (for example the system compatibility), operational impact, safety, reliability and if the recommendations are compliance with the organization policies and external legislation. It should be noted that is extremely expensive and it requires a lot of effort to implement all the recommendation. For this reason, to determine which ones are required and appropriate for a specific organization, a cost-benefit analysis should be conducted, to demonstrate that the cost of implementing the controls can be justified by the reduction of risk level.

The control recommendations are the result of the risk assessment process and also are the trigger for the risk mitigation process.

IT Risk Mitigation

Risk mitigation phase is the second major process of risk management. The output of the risk assessment phase results the input of this phase. Therefore, the list of IT risks that can exercise damages to the system are going to be prioritized, evaluated in order to understand the appropriated implementation of the recommended risk reduction controls.

[7] National Institute of Standards and Technology (2002), Gary Stoneburner, Alice Goguen and Alexis Feringa, Risk Management Guide for Information Technology Systems.

Before proceeding to the mitigation process it is important to understand one of basic concepts of risk management. The implementation of all recommended controls will never eliminate all the existence risk, at least still remains the residual risk. For this reason it is extremely important to identify the most harmful points in the business processes in the scope, so that this process results in the appropriated controls implementation used by the least-cost approach to decrease the risk to acceptable levels with minimal adverse impact on the organization.

Deal with IT Risk

In order to understand how to mitigate a risk, it is essential first to comprehend the best approach to respond to it. The purpose of defining a risk response is to bring the residual risk in line with the defined risk tolerance for the organization.

For each risk detected it should be selected one of the following mitigation options:

- Risk acceptance. This means that no action is taken to a particular risk. Therefore, any loss occurred is accepted. Choosing this option doesn't mean that the organization is ignorant about this risk, but that the organization knows about it and assumes any damage cause by it;
- Risk mitigation. This means that an action is taken to reduce the frequency and impact on business of a particular risk. This option ensures the implementation of recommended controls resulted by the risk assessment process;
- Risk avoidance. This option is applied when no other risk option produce the desirable effect, this means that no other option succeeds in reducing the frequency and impact to below the defined thresholds for risk appetite. One good example is the re-location of data centers to regions with low significant catastrophes likelihood;
- Risk transfer. This means that is possible to reduce the frequency of a particular risk by transferring or sharing a part of it. The most common techniques are the outsourcing and insurance contracts.

When an organization review all its risks and aggregate the cost and effort needed to respond to them, most of the times they face a situation where the total effort exceeds the available resources. For this reason an organization must select and prioritize risk responses using some criteria:

- Cost to implement the response to the risk;
- Importance of the risk addressed to the business;
- Benefits of the response;
- The organization capability to implement the response

Controls

As we have seen controls are actions used to mitigate the existing risk and to increase the probability that the business and process will achieve its goals and objectives. Depending on the type and the possible effects of the risk, specific controls are implemented. There are two types of controls to consider:

- Technical controls, are the controls embedded in the software's, hardware's or firmware's that support business processes;
- Nontechnical controls, are the controls created by management decision, are embedded in business processes, such as politics, procedures and physical security.

When actions are going to be taken, it is fundamental to consider both of these two groups. Technical controls must be considered when the organization acquires new software or a new application. Since the acquisition of it, a modification or an upgrade is expensive, for this reason these kinds of decisions must be taken after a careful analysis on what the organization is expecting to achieve and what the application offers. The second group incorporates controls that can be implemented when needed or by strategic decisions in order to improve business compliance and monitoring.

When implemented, which control has its specific role. Besides the output it provides we differentiate the controls in two major categories according to its implementation purpose:

- Preventive. Controls that focus on preventing non authorized events from occurring, such as authentication, authorization, access control enforcement, protected communications and transaction privacy.

- Detective. Controls that focus on detecting certain type of events, such as audits and specific reports.

Manage Change

Manage change is one of the most critical IT processes, it ensures that all changes to applications, data bases, operating systems follow a strict flow, this means that they are properly authorized, tested and approved prior its implementation.

So as we can understand, this process carries with it lots of risk. Every time a change is done for example to an application, certain actions - controls - must be sure that they are follow. First must be signed an authorization for the change. In case the change is developed in-house it must be done in the development environment. After must be done the transition to test environment for the change testing, and finally if tested with success the transition to production environment with the correspondent authorization is the end of the process.

As we can see, this process has several phases and incorporates many people. Let imagine that along the process there are people who can perform both the development and the tests of the change, or can perform the testes and has authorization to pass the change to production environment. These cases are just a few examples of the risks that are inherent to this process, the damage that one change can cause to the organization for not being properly authorized, tested, developed and pass to production. A change that could be seen as a simple, not critic to the application, can have unexpected results, because a simple change in an application can have cascade consequences to the application. Sometimes a problem is not visualized in the beginning, only after it goes to production and used by several people or by data analysis these problems are detected.

As business depend on the consistency of IT, any consequence or malfunction on it will have immediately impact on business.

Logical Access

Logical access is another critical IT process that deserves special attention too. This process has as concern the creation, change and removal of accesses to various levels inside the organization. Therefore, it ensures that only authorized persons have access to data and application (including programs, information and related resources) and that they can perform only specifically authorized functions, this means that they only have privileges to access functions and to perform transactions needed to complete their roles.

An organization that don’t have this process well establish, is running many types of risks for example as fraud and as information stealing. Let’s assume that one employee change department and role in an organization. When this collaborator entered the company was assigned to him certain type of permission and privileges according the role he was going to perform. After some years he changed his function and to perform his new task he need another type of permissions and access to different areas, resources or information. It is very common in this kind of situation that the company assigns the new privileges but don’t remove the ones that it is not going to need for his new position. In this case we assist to privileges accumulation. This can lead to critical scenarios where collaborators can perform conflict tasks, for example make payments and issue invoices. For this reason it is fundamental to have a deep look on how this process is implemented and if it is being accomplished.

More than ever, information security is a main concern that organizations have to care about. For this reason the logical access process must be a top management concern, it is the first step to mitigate risks related to information security.

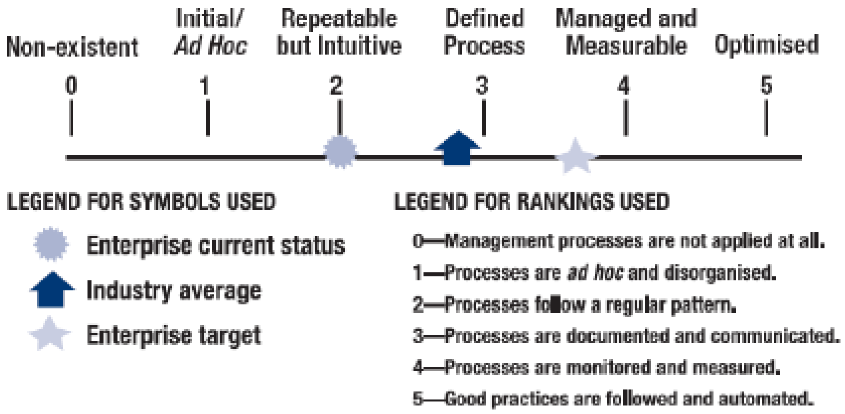
Maturity Models

Boards and executive management periodically need to consider how effective their business is running and more deeply, how their enterprise IT structure is managing risk and how the process are responding to the organizational needs. For this reason, to measure it understanding it should be able to answer some questions:

- What are our peers doing to manage IT risk, and how are we placed in relation to them?
- Are established good practices for managing IT risk?
- Based on these comparisons, is the organization doing enough to respond to their risks?
- How can the organization identify what they need to reach the level of maturity the market is asking for?

It is not easy to answer to these questions. Organizations are constantly looking for benchmarking and self-assessment tools in order to reach the needs that the marking is searching for. One of the tolls is the maturity model, which can give the picture of the current situation where the organization processes are positioned and rate them according to its maturity level, this means from a non-existent or unstructured processes to having adopted and optimized processes through the use of good practices.

The following maturity model showed in figure 10 has been developed by the IT Governance Institute:



0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Figure 10 – Maturity Model

The risk IT maturity stages are designed as profiles in which an organization can identify them self by descriptions of its current and possible future state. After an analysis of their processes according to the maturity model, an organization will recognize that their processes are situated in different stages. Therefore, the maturity model enable management to identify and focus on key areas that need some special attention and where the most critical issues are located, instead of trying to push all them up to the same level. This can lead to excused time and resources consuming, because there are processes that having a high maturity level don’t add value to the business.

The use of IT risk maturity models leads to the identification of the current situation of the organization performance and more important the identification of the organization target for improvement, this means where the organization have to be to reach the desirable maturity state.

For this reason it is important to have in practice a maturity model, it enables the benchmarking of the current state of IT business processes, checks if the year improvements made on them really sorted effect, and also if the most problematic risks were mitigated by the strategies adopted. Nowadays, it is starting being crucial to have certain processes with a high maturity level, because these types of requirements are being more a concern required for partnerships, suppliers and clients contracts, due to the growth level of security in terms of confidence and compliance needed nowadays.

Risk and Opportunity

IT has more than ever a bigger role in the success of any kind of organization. We have been assisting a scenario where typically every day are deployed many kind of IT activities into various areas of an organization, as the need for new applications, software problems that must be solved, networks that fail, important technologies decisions. Each of these activities carries both risk and opportunity that must be considered and analyzed.

As we have seen the risk level is reflected by the combination of the impact and frequency of a certain event occurrence. But risk shouldn't only be seen as threats to achieve success but also as containing opportunities for benefit. Risk and opportunity go together, indeed, to provide value to stakeholders, organizations must be committed in several initiatives (opportunities). However, all of these activities carry different degrees of uncertainty and, therefore, risk. Managing risk and opportunity is a taught task, but is a key strategic activity for organization success.

Hereupon, an IT risk framework designed by the IT Governance Institute defines IT as a key variable in the equation for managing risk-opportunity, it is the driver that supports almost every activity within an organization, and it plays several roles (figure 11):

- Value enabler. The biggest percentage of business projects depend on some investment in IT. Therefore, enabling successful IT projects that support this kind of initiatives and also applying innovative techniques and methods or new technologies, both of these cases enable new opportunities and bring value to the organization. This value can be translated for example as the growth of operational performance which can enable the organization to grow faster and to be more competitive.

- Value inhibitor. As the previous example, IT projects can also fail which can bring serious problems. The failure of identification and capture of new opportunities lead to the fail of value creation. This kind of failure can be translated in many kinds of issues, as for example systems outages for a long time of period, data loss or corruption.

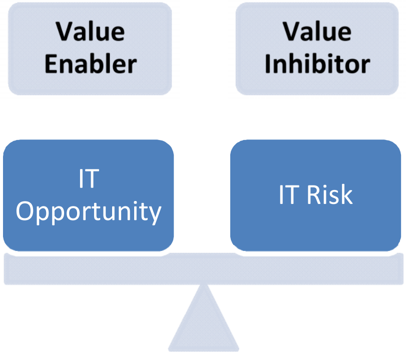


Figure 11 – Opportunity and Risk

It is not easy to deal with this in practice, how can an organization do it? The best way is to embed both risk-aware and opportunity-aware view in the evaluation and monitoring the activities that involve IT. When a complex and expensive investment is proposed, there are many factors that must be considered before any is decision made, as benefits in risk reduction of this investment, risks that this investment carries and business value creation through benefits from the result of the new IT infrastructure and opportunities. During this process of adopting new technology, an organization should assess the expected results through the answer of questions as theses ones: what is the risk of adopting this technology? What could be the consequences of not adopting the new technology? What are the business benefits of the new technology and which opportunities are enabled?

After the organization completes its initial assessment of the risk-opportunity value, it needs to determine how to deal with it. To do this there are many practices that can be applied to enable informed decisions making as risk management or value management practices. To implement these practices support activities is not simple and it requires time and resources. However, it should be noted that going forward with more risk based activities, e g., not having an Business Continuity Plan, may save money in the short term, but it may also block organization growth at a later stage. Therefore, to achieve a successful operational function of all business activities related to IT, it is important to have in mind the importance of low-level activities that supports the success of the organization main strategies.

IT Governance

Years ago, many organizations could succeed despite the weak strategic thinking on how IT could bring benefits. Over the last years, information and consequently IT increase its importance within organizations and became a crucial factor for organizational products and services and for the foundation of organizational wide processes. The jump from the mentality that IT is just a support for businesses to the tight linkage between IT and organization processes result in the mentality that IT must viewed as an important element for organization success that enables new opportunities through the extent to new areas that make organizations more solid and competitive.

A research conducted by Peter Weil and Marianne Broadbent shows that top-performing organizations generate returns on their IT investments up to forty percent greater than their competitors. These cases of success understood the potential of IT and proactively seek value from it in several ways:

- They define clear business strategies align with the role of IT in achieving them;
- They measure and manage budgets spent on with the value created from IT;
- They view the benefits and opportunities from new IT capabilities as one of the drivers for business improvement;
- They learn from each activity that involves IT, which improves business changes more effective and efficient.

Top-performing organizations succeed where others fail by implementing effective IT governance to support their strategies, this means, that an organization with good IT governance practices following specific strategies will have better results, also in profits than one organization with poor IT governance practices. Peter Weill and Jeanne W. Ross define IT governance as:

"...specifying the decision rights and accountability framework to encourage desirable behavior in using IT."[8]

The purpose of IT governance is to determine who systematically makes and contributes to IT decisions making. IT governance is part of the overall corporate governance and principles and focus on the management and use of IT to achieve corporate performance goals. Effective IT governance encourages and leverages a mentality of individual awareness to the overall resources in using IT and ensures compliance with the organization's overall vision and values.

The evaluation of an organization is not restricted to the traditional financial evaluation but also the evaluation of customer satisfaction, the integrity of its internal processes and its ability to innovate and take advantage of opportunities. All of these aspects ensure financial results and drive the organization toward strategic goals having in mind always the balance between them. By this reason every strategic decision and the definition of goals to the organization by top management is also defining the IT goals and IT strategy within the organization. As stated by Dr. Wim Van Gremberger:

"*IT governance is part of the corporate governance and has to provide the organizational structures to enable the creation of business value through IT, the assurance that there are no IT investments in bad projects and that there are adequate IT control mechanisms."*[9]

Value in IT Governance

The IT Governance Institute (ITGI) considers that IT governance is composed by five domains (figure 12), which are strategic alignment, performance management, resource management, risk management and value delivery. Indeed, this last domain only can be reached by the success of the other four domains.

[8] Peter Weill and Jeanne W. Ross (2004), IT Governance: How Top Performers Manage IT Decision Rights for Superior Results

[9] Wim Van Grembergen, The Balanced Scorecard and IT Governance

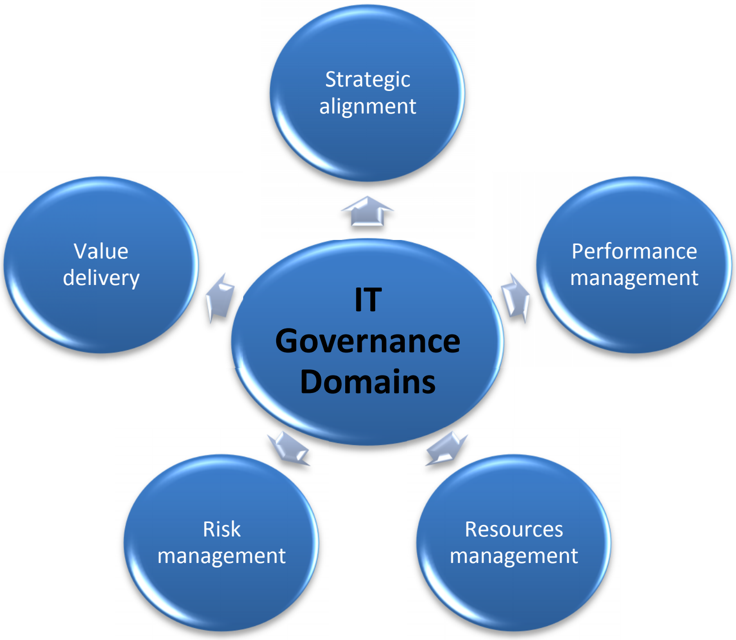


Figure 12 – IT Governance Domains

Each of the components of IT governance has its own function but they are all linked, this means that the improvement of the overall IT Governance depends on the successful implementation of each component. For example, it is impossible to have a successful performance measurement if there is no strategy to create conditions on business processes to do that. It is impossible to have a good risk management if resources and knowledge are not well allocated. The ITGI says that the essential components of IT governance can be expressed as follows:

1. "*IT governance overall is about delivering value and managing risk.*";
2. "*Value delivery, which embodies the concept of risk-related returns, is perhaps the most important.*";
3. "*Value delivery is not possible without strategic alignment and resource management.*";
4. "*It is impossible to provide transparency of success or failure without performance measurement.*"[10]

As we can see, value delivery is in the center of the five domains. It is only achievable by achieving the others. ITGI defines value delivery as:

[10] IT Governance Institute (2005), Optimizing Value Creation From IT Investments

"*Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.*"[11]

Hereupon, in every organization top management has the responsibility to ensure through their decisions that any kind on investment brings benefits to the organization and creates value to stakeholders. Successful acquisition and deployment of information systems require a careful analysis and a large allocation of resources. Consequently, this type of investment as any other should be subject to the same initial detail examination during all the stages of its life cycle including before it is deployed and during its implementation. Any kind of investment should be undertaken without the full knowledge of its impact in all organizational levels, as the expected cost and the return that is also expected, correlated to risk. High risk project have a higher likelihood of failure, so for this kind of investments it is expected a higher return expectation. The same principles and criteria's applied to measure any kind of investment must also be also applied in IT investments.

IT related investments have potential to deliver far greater returns than almost any other conventional investment, says a study conducted by the Group ING in 2004, where a comparison with traditional investments such as, real estate, bond issue and IT related business investments were made. However, despite this fact there are a lot of cases where this goal is not achieved, highlighting the awareness needed to the five domains of IT governance in balancing the attention among them. To reach this balance and implement a structure which ensures the effective function of each domain is a task required that results from a deep analysis of the current state of the organization. There are certain types of issues that must be solve, issues that block value obtain from IT, as the lack of understanding of how well IT is performing, operational failures, staff problems, disconnection between IT and corporate strategy, lack of knowledge in critical systems, among others.

Success in understanding cost and measuring value can be achieved only with the collaboration between IT and business. Martin Curley, director of innovation at Intel states:

[11] IT Governance Institute (2003), Board Briefing on IT Governance, 2º Edition

"*A strategic alignment between IT and the business is a crucial factor in business value generation. Good strategic alignment implies a virtuous circle, that is, a positive bi-directional relationship between IT and business strategy. Within this context IT and business alignment should be measured not only by extent to which IT supports the business, but also by the extent to which business strategy capitalizes on IT capabilities.*"[12]

In his book, he defines four strategies on how can be generated and how to measure value from IT investments:

- Manage for IT business value to maximize benefits such as corporate profitability and growth with existing and future IT investments.;
- Manage the IT budget to enable continuous cost reduction and the flexibility to shift budgets funds from low-yield investments to investments that will deliver competitive advantage.;
- Manage the IT capability to enable sustainable competitive advantage to be delivered from IT.;
- Manage IT like business so that winning business practices enable IT organizations to succeed in their missions.

Ensuring that value is obtained from investments in IT is a big issue and an essential component of IT governance. It involves a wisely selection of investments and the way they are managed through its life cycle. As any facet of governance, without commitment, support from the top and leadership, the success that was planned to be achieved is less probable to happen.A strict discipline must be applied to IT investments assessment in order to ensure that the correct investment is being chosen and value will be delivered.

[12] Martin Curley (2004), Managing Information Technology for business Value, Intel Press

Proposal IT Risk Awareness Framework

Over the last two decades, organizations growth rapidly through entrepreneurial strategies and acquisitions. Today, the growth is slowly due to the change on customer demand, the worldwide competitiveness, tight regulation and laws, which impact and force the corporate environment for many changes. Organizations had to organize them self's to reach competitiveness to at final keep opportunities enable. Facing this fact, never had IT played such a bigger role than now, since all strategic issues are linked closely to IT, its capacity and flexibility. IT left the narrow view of the business support function and adopted a key role for business success.

Since business relies on IT, the awareness for its accuracy, availability and agility become a strong issue that organizations have to manage. IT risks incorporate now the top corporative risks, making IT risk management a serious discipline for consideration and analysis to top executives.

My research on this subject lead me to a proposal on how organizations should organized themselves to manage IT risks and how to gain value from them, making IT structure organized, ready to provide conditions to enable organizations to go forward on important strategies that makes them stronger to face adversities and with bigger sustainable growth. This proposal is based on three pillars, which are: a well IT structured foundation, a well design and implemented IT risk framework and an IT risk awareness culture. As these pillars are continuous operating cycles, they are assessed and supported by a systematic monitoring mechanism assumed by the internal control of the organization. At last, in order to create value from this structure and investment on IT, is important to establish defined and rigorous governance processes to ensure that the best decisions are taken to the benefit of the organization.

The picture below demonstrates the proposal resume on how IT department must be organized to manage IT risks and how should the different parts on this structure interact among them:

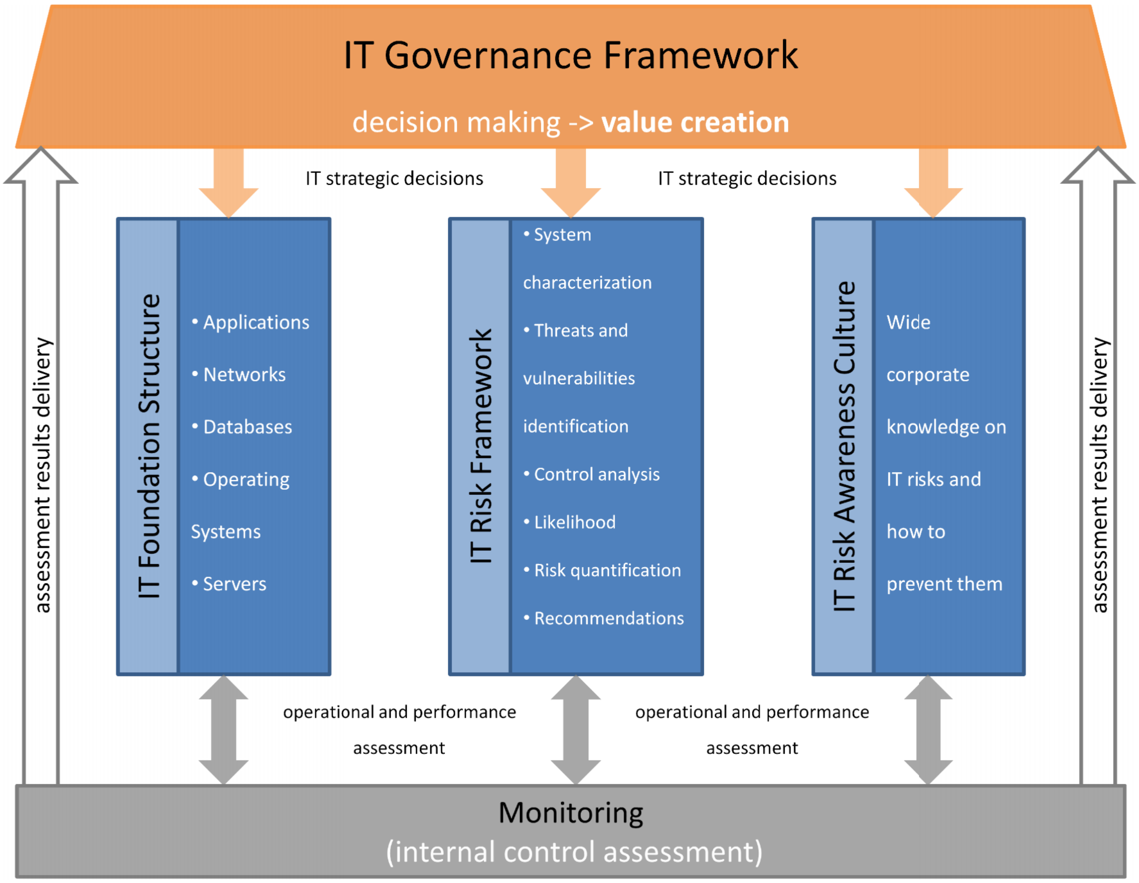

IT Governance Framework
decision making -> value creation
IT strategic decisions
IT strategic decisions
assessment results delivery
assessment results delivery
IT Foundation Structure
• Applications
• Networks
• Databases
• Operating Systems
• Servers
IT Risk Framework
• System characterization
• Threats and vulnerabilities identification
• Control analysis
• Likelihood
• Risk quantification
• Recommendations
IT Risk Awareness Culture
Wide corporate knowledge on IT risks and how to prevent them
operational and performance assessment
operational and performance assessment
Monitoring
(internal control assessment)

Figure 13 – Proposal Structure

As we can see on figure 11, the proposal structure is supported by three pillars, which are the IT Foundation Structure (technologies structure, supporting personnel and procedures are well implemented and understood), the IT Risk Framework (a clear IT risk framework is in practice according to business needs) and the IT Risk Awareness Culture (ensures that everyone in the organization has the appropriate knowledge of IT risk, their costs and how to prevent them). These pillars are the base implementation for the creation of an effective mitigation of IT risk. To guarantee that the pillars work efficiently and produce the expected results, a continuously and systematic assessment process must be implemented, shown in the figure by the Monitoring. Finally, but not less important, is the implementation of an IT Governance Framework, which prime objective is to provide an organizational level view of all IT risks, so that executives can prioritize and invest properly in risk management to bring value to the organization.

An organization that wants to make the most effective use of its resources in managing IT must be competent in all these five aspects. Implementing this structure does more than help the organization to manage IT risks better, it gives executives confidence. You gain confidence since you know what your most important risk are and that you have an effective process to manage them. These can be translated by the ability to take more risk in new strategic decisions, since there is a higher level of knowledge about the organizational current state and how it can respond to certain scenarios.

The next topics detail each of the five aspects of the proposal structure.

IT Foundation Structure

This component of the proposal structure has as main objective the strengthening and the complexity reduction of the technological foundation of the organization, consisting in rethinking about IT assets, procedures and people that support the previous two aspects. This includes:

- IT infrastructure that supports business, information management, networks, middleware, communication between the IT structures, databases. The point here is to check if the current IT structure is well organized and robust enough to respond to business needs. The IT structure is the platform that enables business applications to run reliably.
- Applications that support all business tasks and processes, such as stock management systems, accounting systems, payroll system, ERP's and CRM's. All application deployed must have the specifications needed to business and most important if they are compatible with each others.
- People with the right skills to manage the IT structure and applications. Support staff that knows very well each application and the technological structure and how each technology supports business, their role and purpose.
- Processes and procedure that ensure and guarantee that the IT structure are controlled, monitored and maintained, so that IT assets run safety and secured.

An organization has to guarantee that its IT structure is well understood, and even more important that is no more complex than the absolutely necessary. Ensuring this philosophy, the organization is implicitly ensuring that problems are less likely to happen (intermittent and hidden bugs that are so common in complex systems are much less likely to happen), in case of failures it is much easier to repair through technical staff and solid management processes (in complex systems it can be hard to find the source of the problem), it is easier to address and assess risks (complex systems carry more risks and make their assessment more difficult), it is easier to maintain (in complex systems you take more time to maintain systems and likely you need more resources to do that) and it is easier to change, which makes the IT structure more flexible and scalable (in case business is growing fast and needs, in a short term, to increase their IT resources, in complex systems this can be a tough task, to make any change in the system you need much more time, more resources and in the most of the cases you cannot do this upgrade in the time you want).

Therefore, we can see that complex systems have direct impact on every kind of risks:

- Availability risk increases, because having many types of technologies makes harder to maintain them and to integrate them perfectly.
- Access risk increases, because it is difficult to manage the accesses in every technological component of the IT structure.
- Compliance risk increases, because it is difficult to supervise if every platform is respecting certain type of rules and best practices that a company is obliged to.
- Agility risk increases, because it is difficult to assess the impact of one change in one system in all the structure.
- Accuracy risk increases, because it is difficult to ensure that the information flow within systems remain correct, since every system use different methods on how they treat data.

The IT structure analysis and its restructuration processes take time and require resources and some investment. But when compared with the cost of having a complex system it is far more beneficial in terms of cost and benefits to the organization in medium and long term. If we think in terms of budget, simplifying the foundation will automatically reduce the investment needed every year for foundation purpose tasks, making more budget available for other activities.

Transformation of the IT structure can be done in one of two ways:

- Rapid transformation. This way is faster but also carries more risks with it. To do this, an organization has to ensure that all business units, all management levels are aligned and that this change follows a rigid process already designed by the different levels of skilled people that are responsible for technology.
- Incremental transformation. This way is slower but surer. The organization has more time to think and take care of unexpected issues that might come.

Therefore fixing the IT structure is the first step to consider when applying this proposal. Turning the foundation simpler is a key process for the success of IT risk management. As this process begins until the end, immediate weaknesses are found and corrected, providing time in the future for further improvements. It also makes risk management more cost-effective since risks decrease and are easier to treat, making all the others components of this proposal easier to manage.

IT Risk Framework

In today's business environment, conditions remain challenging for many, and so risk management must take its position high on organization's agenda. Businesses themselves are changing, which brings new risk horizons and, at the same time, they must understand and grapple the changes also brought by downturn economy situations. The ability to anticipate threats, respond and continually adapt is as critical part of the risk management process as it ever has been.

An IT risk management framework well designed and deployed, create big advantages to organizations in managing all the issues related to IT risks. It is a mechanism that enables organizations to have a holistic view on their current situation and, from this point allows the creation of strategies and priority plan on how to treat risk problems in the present and to think further according the business goals.

In the chapter "IT Risk Management" of this thesis we can see the importance of having an IT risk management framework, its purpose, how it works and how it should work. Despite it requires much skilled resources allocation and a big effort in terms of communication across all the organization, the final result brings a lot of benefits, expressed in many organizational aspects, such as operational, performance, strategic and financial.

By all these reasons, the deployment of an IT risk framework is one of the pillars of this proposal fundamental in mitigating IT risk, a pillar that must be looked and treat with special attention so it can bring the desired results.

IT Risk Awareness Culture

Businesses today are converting the way they operate and the way they approach customers using technology. More than ever security started to be a main concern. Since businesses depend on technology and IT risks increase, it is far more difficult now to control people behavior in-house on how to handle information and how to proceed in some type of technological situations. For these reasons it is extremely important to deploy a risk awareness culture in all levels of an organization as a control to give people confidence to struggle risks.

The lack of risk awareness open leaks in the IT structure and puts into question the effectiveness of the risk governance process. Without awareness organization can't avoid risks. As defended by George Westerman and Richard Hunter (2007), an aware risk culture is not only a culture that provides people knowledge about risks and solutions to mitigate them. It goes further, it creates an environment of freedom to discuss issues without the fear of retribution. By them:

"When a culture is risk aware, people know their risks, are comfortable with discussing their risks with others, and are willing to help others resolve risks. People in such a culture have the ability to face and learn from managed failures, which improves performance over time, and to share risks and deal with them as a team."[13]

A risk averse culture is one where people in an organization don't feel comfortable to talk about risks, they are afraid not just of risk but others disapproval or censure where risk is concerned. Usually this happens when people are punished for failure and risky behavior is severally punished on rewards and serves as example to others. Whether it's acknowledged or not, risk is always present, thus a risk adverse culture blocks the organization to understand and to improve their risk status, it avoid

[13] George Westerman and Richard Hunter (2007), IT Risk, turning business threats into competitive advantage

discussions of risks, avoid responsibility for risks, people don't learn from mistakes, in some cases makes budgeting not realistic, failures are not analyzed and in an aggregate level makes an organization weaker.

For these reasons, it is a top priority to implement a risk aware culture. An organization don't change its culture easy, therefore, the best way to start is from the top, this means that are top managers that should encourage their staff to have a proactive communication behavior concerning risk. To do this, it is fundamental to give IT staff the tools and knowledge on how they should respond to this issue, for example:

- Information concerning IT risks management policies.
- Identify organizational practices, such as sources where is possible to find information about established procedures.
- Recognize risk behavior on them and in their colleagues.
- Participate on IT risks assessments and analysis.
- Provide information to address IT risks in their business unit.

Considering this, it's not fear that an organization needs, it's openness. That openness combined with the other aspects of this proposal will allow an organization to improve their awareness and their performance in assessing risk, in treating risk and finally enable an organization to take more on more risk (and the return that comes from it) without becoming more risky.

IT Governance Framework

An issue shared over all organization is that people who can best prioritize risk management across the organization is not the one who are able to address and identify the risks. Top executives can very effectively make business trade-offs among risks, assign funding and responsibilities to address risks but, they don't have the knowledge, skills or time to identify each business units risks.

By these reasons, organizations need a way to link every fragmented views of IT risk, in order to develop and accurate, comprehensive, shared, and action-oriented picture of all IT risks. Beyond these issues, organizations also need a way to put into operation responsibilities to resolve disagreements about impact and likelihood of each risk in the diverse business units.

Getting a comprehensive, consistent and the holistic picture of risks, keeping them updated, and then acting on them appropriately is a tough task in organization reality. Thus, the implementation of an IT Governance Framework, one of the pillars in the proposal, aims to clarify and deploy a mechanism to manage governance in organizations IT processes. With an effective IT Governance Framework allow executives and middle management to have the information they need to make and implement smart, confident business decisions on how to manage IT risk. Without IT risk governance process, organizations cannot understand the real degree and nature of risks they are facing, which leaves them vulnerable to undesirable surprises.

To achieve the expected results an IT Governance Framework should respond to certain types of questions. Peter Weill and Jeanne W. Ross[14] defined three sets of questions that must be answered:

- What decisions must be made?
    - IT principles decisions, high level statements, politics and procedures on how IT is used with organization;
    - IT architecture decisions, how to organize IT foundation to achieve desired business and technical standardization and integration;
    - IT infrastructure decisions, align IT services that provide foundation for the enterprise's IT capabilities;
    - Business applications needs, define business needs and purchase or self development strategies;
    - IT investment and prioritization decisions, define IT budget and the areas of investment.
- Who should make these decisions?
    - Define and allocate human resources for each IT function in all levels of management. When making these decisions it is important to have in mind the skills needed for each task in order to position the right people in the right place to guarantee the alignment of superior business strategies with the desirable results.

[14] Peter Weill and Jeanne W. Ross (2004), IT Governance, How Top Performers Manage IT Decisions Rights for Superior Results

- How to make and monitor these decisions?
    - Define processes and frameworks so that results from all decisions above can be analyzed and assessed, in order to match the obtained results from them to specific area or function. This enables the possibility to correct previously decisions mistakes taken.

A well designed IT Governance Framework enables the technical resources to identify and address risks, providing the management layers information and feedback to manage the risks and allocate the resources in the most convenient way to the most important risks for the organization, this approach brings advantages:

- It distributes resources at all levels of the organization to work in the most effective way, this means, increase the resources performance on the areas that are critical for the organization.
- It allows managers to take decisions based on the current situation of the organization, making possible the take the correct high level decisions.
- It provides a way to escalate disputes, since it is possible to assess disagreements and to identify the authority level to solve them.
- It increases the awareness for responsibilities on management levels.

Good IT governance harmonizes decisions about the management and use of IT with desirable behaviors to the business objectives. Thus, without a carefully designed and implemented governance structures, organizations leave this harmony to chance. Through this thesis we understood why governance should not be left to chance and that’s why it is consider one of the pillars in the proposed framework. An IT Governance Framework act as the mechanism that enables the proper functioning of the entire IT structure (people, processes and technology) and the value extraction from it.

Monitoring

Managing business requires a lot of efforts from all organization levels. Despite the variety of tasks and the responsibility each one carries, it is the aggregation of all tasks success that makes business succeeds as well. To reach this point, it is needed to provide each people the right tools and conditions so they can perform their task efficiently. So, to provide this environment, business resources require effective governance, adequate controls to protect them, and a monitoring process that alerts management to changes in the business and control processes in a timely manner. All these issues are the reasons to have a monitoring process in the proposed framework.

On daily basis, breakdowns occur and deficiencies in processes and controls are found and procedures and policies are not followed. All these failures fail to keep up with the business and their alignment with the strategic objectives established. The aim of the monitoring process is to fill the gaps found during business operations, this means, detect failures in the most critical processes, ensure that standards and procedures are followed, identify business risks, design and implement controls to mitigate current and future critical risks, review controls effectiveness and at the end communicate all findings and respective improvements recommendations to the right levels of management.

In summary, the monitoring process gives the current accurate view on how well business operations are performing and the current business risks that business is facing and the ones it probably will be facing. Its result provides management the holistic view of the organization deficiencies and effectiveness, allowing them to formulate and clarify strategies and decisions in the short, medium and long term.

The purpose of having a monitoring process in the framework proposed is the one shown above. Considering that to success in the implementation of the framework, the three central pillars must be well deployed. To achieve it, must be ensured that their implementation, its processes, and its internal structure are working properly and will be working properly continuously. The main goal of the monitoring process, as we can see in figure 11, is to provide and communicate the findings found during monitoring activities (quality data) to management levels, this means, deficiencies, efficiency and effectiveness of organization risk management activities and improvements to be made in each pillar. With this information, management team is enabled to make local decisions and define at high level business strategies.

The IT monitoring activities within organizations are performed in general by the internal audit department. A common issue shared by organizations regarding their internal audit team, is that most of the times the results delivered don't meet the expectations. Thus the value that was supposed to be delivered and generated from it is little. Usually this happens because the people who are performing these activities don't have the right skills and tools and by this way it is difficult to reach a good maturity level of the monitoring processes and get results from it. Considering this, internal audit department should be provided with people with the right skills and tools so they can improve their work, since it makes the monitoring processes more effective and adding the fact that many of the existing controls within organizations are IT dependent or even monitored in their own right (automatic control).

The continuous monitoring of IT offers substantial benefits:

- Early identification and timely corrective action in processes and controls deficiencies;
- Leveraging of processes to monitor controls and business performance;
- Provision of more accurate, decision-relevant information through reliable financial and operational reporting;
- Better access to data, increasing by extension the speed and quality of management decision making;
- Increase management confidence when making decisions, since their confidence in the information generated by the business process increase as well;
- Ensure compliance with standards, policies, procedures, laws and regulations;
- Provide information on the effectiveness of the framework of internal controls;
- Better detection and prevention of fraud and reduction of impact in the business in case this events occur;
- Cost reduction, due to processes become more efficient;

The monitoring process in the proposed framework plays an important role as we have seen. It acts as the mechanism that calibrates the entire framework, making it more and more efficient, providing constantly to management accurate business information so that they can define the direction which the organization should go. For all these reasons, the monitoring process was included in the bottom of the proposed framework, it is presented in all pillars.

Conclusion

This work is direct to medium and big organizations and aims to create awareness in them on IT risks and their widely impact within them. After an intensive study about the inherent issues to this subject, I present a proposal that I believe that its implementation is very effective in struggling IT risks because a part from the direct effects in mitigate the risks it also obliges indirectly the organization and modernization of the IT departments and a new mentality and critical sense of the surrounding environment.

The objective was not to explore deeply each of the aspects that integrate the proposed framework, but to explain them and demonstrate how them working together can bring benefits in risk reduction and generate value for a variety of organizational areas.

In this work I focused more in one of the components of the proposed framework, the IT Risk Framework, because I wanted to enhance the process on how IT risks are identified and treated, showing the benefits generated by the results of it. I also believe, by this way it is easier to understand the other components, their role and importance in the proposal.

It is important for organization to become competitive as quickly as possible. This proposal framework can help them to achieve this state, but for that an organization must become competent in all the components of the framework: IT foundation structure, IT risk framework, IT risk awareness culture, monitoring process and IT governance framework.

However, should be highlighted that every organization is different and so each one can implement it in a different way regarding their resources, characteristics and specific needs, as some of them could have already in place some of the components proposed. No organization has never-ending attention or capabilities, so a central focal point can help to start. This focal point builds attention and comfort with risk management through the organization, installing it into the way the organization does business and helping the organization to organize and to improve the other framework components. This not means that organization should focus in only one component, since all of them are necessary to address all risks effectively.

Considering this, organizations must understand how they should start. Thus, a deep analysis of them should be made having in mind their culture, their circumstances and their available resources and skills. The goal is to make it comfortable as possible for the organization as a whole to adopt risk management so that it can become competent in the rest of the components as soon as possible.

As no organization or its environment is ever static, no risk management strategy can be the same forever. Because of current competitive and uncertainty environment, most organizations adopt in ongoing strategic change, and thus their IT risk management strategies must be examined regularly for the implications of those changes. Defining their strategic paths, means discovering ways in which organization plans to engage with its customers, suppliers, partners, competitors and environment. Understanding the changes implied by those changes and decisions to existing IT risks is crucial to make sure that the organization follows up to reduce exposure to risky situations and to avoid the consequences of unexpected dangerous surprises.

Bibliography:

Books:

- George Westerman and Richard Hunter (2007), IT Risk, Turning Business Threats into Competitive Advantage, Harvard Business School Press, Boston, Massachusetts.

- Peter Weill and Jeanne W. Ross (2004), IT Governance, How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press.

- Peter Weil and Marianne Broadbent (1998), Leveraging the New Infrastructure: How Market Leaders Capitalize on IT, Boston: Harvard Business School Press.

References from the internet:

- Cisco Systems (2007), customer case study, Printed in the UK 31603/ecoutez/0507, http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps556/prod_case_study_Maggiore.pdf.

- Goldman Sachs (2007), BRICs and Beyond http://www2.goldmansachs.com/ideas/brics/book/BRIC-Full.pdf.

- IT Governance Institute (2009), Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft, V0.1 revised 3Feb09, www.isaca.org.

- ISACA (2010), Monitoring of Internal Controls and IT, A Primer for Business Executives, Managers and Auditors on How to Advance Best Practices – Exposure Draft, www.isaca.org.

- IT Governance Institute (2005), Optimizing Value Creation From IT Investments, www.isaca.org.

- Matthijs Kerkvliet and Thomas Wijsrnan (2008), Dutch experiences with ERP systems, http://www.intosaiitaudit.org/intoit_articles/28_p14top17.pdf.

- Ernst & Young (2008), Moving beyond compliance, Ernst & Young 2008 Global Information Security Survey, http://www.eycom.ch/publications/items/giss_2008/2008_EY_GISS.pdf.

- Ernst & Young (2010), The top 10 risks for business, a sector-wide view of the risks facing businesses across the globe, http://www.ey.com/Publication/vwLUAssets/Business_risk_report_2010/$FILE/EY_Business_risk_report_2010.pdf.

- Ernst & Young (2010), Escalating the role of internal audit, http://www.ey.com/UK/en/Issues/Managing-finance/Internal-Audit/Advisory_Escalating-the-role-of-internal-audit.

- Hewlett-Packard (2008), Getting smarter about IT risks, http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1104465

- Eric Cope, (2007), To compliance and beyond: Adding value to your enterprise through operational and IT risk Management, IBM Zurich Research Lab, ftp://public.dhe.ibm.com/common/ssi/ecm/en/fmw00292usen/FMW00292USEN.pdf.

- Gary Stoneburner, Alice Goguen and Alexis Feringa (2002), Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

- Wim Van Grembergen (2010), The Balanced Scorecard and IT Governance, http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/The-Balanced-Scorecard-and-IT-Governance.pdf.

References from the press:

- Nicola Clark and David Jolly (2008), Société Générale loses $7 billion in trading fraud, 24 de Janeiro.