Environment. Technology. Resources, Rezekne, Latvia
Proceedings of the 11th International Scientific and Practical Conference. Volume II, 124-127

IT Risk Identification and Assessment Methodology

Oskars Podziņš, Andrejs Romānovs
Riga Technical University, Institute of Information Technology Address: Riga, Latvia.

Abstract. There are numerous methods for risk identification and risk assessment phases. Which for risk identification includes historical and systematic approach and inductive or theoretical analysis. One of the main reasons why risk identification is very helpful is that it provides justification in many cases for any large IT investment and other large undertakings. Without it organization probably wouldn't be able to come to conclusion. Also in this phase business recognize the threats, vulnerabilities, and assets associated with its IT systems. Together with risk assessment phase risk management specialist is responsible for determining asset value, what's the value of the asset business is protecting, and risk acceptance level.

Risk assessment on the other hand examines impact or consequence, as well as examines and evaluates the likelihood or probability of that adverse event happening. Risk assessment includes methods like Bayesian analysis, Bow Tie Analysis, brainstorming or structured interviews, business impact analysis, cause and consequence, cause-and-effect analysis, Delphi method, event tree analysis, fault tree analysis, hazard analysis, hazard and operational studies, and finally structured what if technique or SWIFT process. Risk assessment has two distinctive assessment types- quantitative and qualitative assessment. Quantitative assessment tries to put a monetary value on all risks. Qualitative assessment on the other hand rather look at it from a range of values like low, medium, high. The results of these phases are going to be documented in the risk assessment report and reported to senior management.

Keywords: IT risk, risk identification methodology, risk assessment methodology, risk practitioner, qualitative risk, quantitative risk.

I. INTRODUCTION

Nowadays every business who wants to be innovative and be competitive in the global market must utilize at least some form of risk assessment. On a daily basis business has to evaluated short to long term strategic development plan. And the further in the future anyone tries to plan, the greater the risk of unexpected outcome which for business can be devastating. Including financial loss, reputation loss or even bankruptcy. In order to avoid this, it is necessary to know what kind of risks business is facing. And what are possible solutions to greatest risks. To find this out risk management specialist must identify, assess business risks and provide cost effective mitigation solution. After which business management can continue to monitor those high priority risks to be able to react if situation changes to the worst.

To gain knowledge and experience in this field it is necessary to know the procedures and methodologies to accomplish necessary goals on achieving desirable risk level. This article will help you do that. There are many methods and techniques, and it is not possible to cover them all in this article, but author thinks this article has managed to capture most relevant methods.

II. METHODS

IT risk identification methodologies

There are a number of different ways to identify risk. Probably the most common is historical[1]. This is what the insurance companies tend do. They can look at, what is the risk, based on the empirical data they already have many years of what's happened previously. During risk identification and assessment RMS (risk management specialists) should always use historical data when possible [5]. What's happened in the past can greatly help RMS to make sure the same problem doesn't repeat in the future that was not anticipated. But for everyone in the IT that doesn't always work[2].

Sometimes RMS is going to have to use a systematic approach[3]. Process involves bringing in the people that are the subject matter experts, the people that really have an understanding of technology, have an understanding of the threat environment and can offer an expert opinion on what some of the problems could be based on the technologies subject currently have. Even in some cases forecasting events that have not yet happened. This is where it is necessary to look at not only single points of failure, but sometimes even aggregated risk where the risk comes from several different things that work together to form a risk event.

ISSN 1691-5402

http://dx.doi.org/ 10.17770/etr2017vol2.2539

The third type is what RMS calls them inductive or theoretical analysis[4]. Similar to building upon systematic approach, but inductive tries to find what is needed to be done, especially when looking at something where no one in yet an expert. Like when there is a new technology and a new business process. Because of this it's not possible to always know what types of threats will occur. But using that expert opinion systematic approach, imagination and the ability of people to see what things are going to look like, it is possible to perform successful inductive analysis [127]. New ideas can be induced and in some cases, be able to deduce the types of events that could lead up to a risk event in the future. Then what is the objective of doing IT Risk Identification? First of all, RMS helps providing justification in many cases whether or not an organization should make that IT investment. An IT investment is very often a very large capital investment. It's also a very large operational expense. Either way by looking at current risks business management should be able to determine if that new system, is worthwhile investment? Its necessary to understand that as business relies more and more on its IT investment there is a whole new area of security that is important too.

Business have the problem that a person may gain unauthorized access to its sensitive data. Sensitive data theft of course could lead to very severe financial penalties as well as reputational damage. Clients also have to understand what are the risks related to integrity. Is there a chance, for example, that the data employee has in his system would be inaccurate?

So these are all these sorts of things that have to be looked at in risk identification phase. What's the risk of making a poor investment? What's the risk related to improper access and lack of security? What are the risks related to a loss of integrity? Business also have to ensure that its systems provide timely information. Some information can be incredibly time sensitive.

During the risk identification phase, business recognize the threats, vulnerabilities, and assets associated with its IT systems. Risk identification together with risk assessment is responsible for determining asset value, what's the value of the asset business is protecting, and risk acceptance level.

Risk Assessment

What would risk assessment do to the organization? This means RMS have to examine impact or consequence, as well as examining and evaluating the likelihood or probability of that adverse event happening. RMS will now be able to document and determine what our critical business operations are.

As most people know, IT risk is all about supporting business, and RMS want to know which of business IT systems are most critical in the dependency for the business to operate correctly. There are a number of different risk assessment techniques, but author will cover some of the ones that are commonly used.

RMS performs Bayesian analysis, Bow Tie Analysis, and process like brainstorming or structured interviews. RMS borrow from the area of business continuity and disaster recovery, and do a business impact analysis. RMS also can look at cause and consequence, and when that is done RMS will understand what might lead to an event, and what that impact would be. That is very similar to the next one, which is cause-and-effect analysis. In this case, RMS understand the root causes, and how that causes could affect systems. It is preferred to asset risks by simple checklists.

RMS could call on the expertise of the many people within organization who understand the impact on the business, and this is often done through a Delphi method, a Delphi method is where the input from all of the various stakeholders is sought, sometimes even anonymously to allow everyone to contribute to the data collection and analysis process. Many times, when something happens, it's because of a sequence of different events, and this is where event tree analysis can help RMS to determine what are the things that come together to lead to a risk event. Very similar to that is fault tree analysis method.

What are the things that could lead up to an unhealthy environment in which a risk might happen? RMS also could look at hazard analysis and critical control points, where high-level risk is identified within areas within the organization that could lead to a very serious adverse impact, often based on single points of failure. Continuing, some other risk assessment techniques its worth mentioning hazard and operational studies. RMS can look at people within business because many of our risks are related to our employees, and through human reliability analysis.

One of the things that is often done to allow RMS to truly assess risk effectively is to look at the impact of maintenance on the reliability of systems and products. Do business have a skilled staff that is looking after the systems on a regular basis, or are things beginning to deteriorate already?

Most people do not really understand risk assessment, but they do understand a scenario, or a story, or an example, and RMS can use those as a way to gather more accurate information where people now understand what the impact of various types of events could be. Final one is structured what if technique. So what if this happened, then what, what if this happened, and that is sometimes called SWIFT process. When RMS looks at risk assessment, often results are inaccurate. In many cases, that can lead to wrong decisions later on in risk response, so why is that? This is because in many cases, risk is unpredictable. A same event might happen 15 times,

and all 15 times could have a completely different level of impact. In fact even worse, the same event could happen 15 times, 14 times had exactly the same impact, and once it had a completely different result. So it's very difficult for RMS to examine a risk event in isolation. Risk assessment works on a larger population, but not on an individual case.

Because of this RMS should learn from every risk event what has happened in the past.

Risk Assessment Methodologies

So how do RMS perform risk assessment? There's two main ways, quantitative and qualitative. The idea of a quantitative risk assessment is that RMS try to put a monetary value on all risk. If this system went down, what would it cost to business, and there RMS would look at of course not only the impact on IT, of what it would cost business to recover our IT services, but RMS would also cover what would be the monetary impact on the business if business itself would be unable to support a certain business process, product, or service. Dealing with quantitative risk has the problem in that many things are not truly quantitative, things like customer confidence and employee moral are not really quantitative values [5]. It's hard to put a dollar figure on those. So quite often RMS will look at risk from a qualitative perspective.

A qualitative risk is where RMS looks at a scenario. If this system went down, how would that affect other departments. For example, let's look at it from the perspective of very low impact, moderate, high, or very high impact. Instead of putting a monetary value on it, RMS rather look at it from a range of values, and RMS talk to many departments, in order to find out how this scenario would affect not just one department, but might affect other departments within the organization as well. When RMS looks and compare those range of risk levels from the different areas, RMS can now set out priorities according to our risk, in result we're looking at it now from the perspective instead of just money, but we're looking at it in many cases from those non-quantitative values. Quite often RMS will use a range of 5 values, same goes for both the ISO 27005[6], and NIST Special Publications 800-30 revision 1[7] to try to determine what is the range of risk. RMS will use those to compare likelihood, impact, and asset value. Quantitative risk is calculated first of all by saying how much would any one single event cost business. Quite often we hear this written as SLE or single loss expectancy.

Qualitative risk looks at the non-monetary elements of risk quite often by looking at different types of scenarios, and in that scenario RMS can consider things that are outside monetary values such as moral, reputation, customer confidence. RMS calculate risk by looking at those factors of how likely or how probable is a risk event compared to of course the level of impact and if this risk actually happens. How much damage or what would be the consequence, and in order to truly determine a risk level, RMS needs to look at both of those factors, the likelihood of it happening compared with the impact and if it does indeed happen.

Author has reviewed both quantitative and qualitative risk assessment, they both have advantages, but they also both have disadvantages. That quantitative did not bring in some of those non-monetary elements, whereas a qualitative risk did not give us the dollar figures needed to justify the cost of controls. So what do organizations often do? They bring the two together into a hybrid, where RMS will now do a semi-quantitative risk assessment. RMS will compare both quantitative and qualitative, to get a more complete picture of risk, and the assessment provided to management hopefully will be more meaningful and actionable for them.

There is a direct relationship quite often between a technology-related problem and the organization's ability to deliver on its products and services. This helps business to put together a strategic plan, so RMS can say how to ensure that technology is built in a stable, reliable manner in order to support the organizational mission and goals?

Risk Areas to Consider

This phase of risk assessment is extremely important. The results of this phase will guide further the risk response in the next phase of the risk management framework like risk mitigation or risk respond and risk monitoring. For full risk management process please refer to (

Fig. 1). Rest of the phases will be reviewed in the future research.

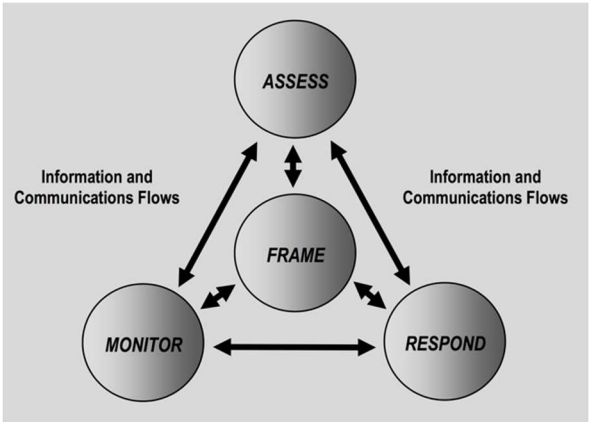

Fig. 1 Risk Assessment Within The Risk Management Process

There are many areas that needs to consider the risk in order to ensure that the risk assessment RMS perform is complete, accurate, and thorough. RMS must look at the risks related to the IT management, the management including the procurement, maintenance, and support of hardware, choice of software, including of course operating systems, as

well as keeping utilities and drivers up to date and patched, making sure that application program interfaces, our APIs are set up correctly. Current security standards built into them. RMS need to ensure that our applications are also secure, that they're robust and able to withstand an attack. Databases are correctly managed so that business have efficiency of the actual extraction of the data, as well as of course the security necessary to ensure the retention of business data, but also protection against unauthorized access. RMS also have to look at the risks related to our networks and network architecture, for example, does business have single points of failure, network architecture has a lack of adequate security to ensure that we are going to prevent unauthorized access to business network communications?

RMS should also examine the process of software development. This is often, of course, done through an SDLC, or Software Development Lifecycle. The SDLC is there to try to ensure better results of software development projects, software development projects hopefully that will meet the business needs more effectively.

III. RESULTS AND DISCUSSION

Final report and risk register

The results of this phase are going to be documented in the risk assessment report. The risk assessment report is the final results of the scoping, the identification, and assessment of risk. It is to provide management with an accurate report, documents what risks business face, and the prioritization or importance of those risks.

Risk assessment and risk identification should be brought together into the risk register, the risk register is one document that sources all of the risks that have been identified through things like incidents, vulnerability assessments, penetration tests, as well as the user complaints, and of course risk assessment itself[8]. By having all of the risk in one place, it gives business the ability now to track and monitor the progress RMS will be making and addressing these risks. RMS should provide in the risk assessment report recommendations, things that management can consider in the next phase of risk response, for what should or shouldn't be done about the identified and assessed risks. One of the things that's important to recognize is that risk is not owned by the risk practitioner. Risk is owned by management. They are the only ones who can determine what is an acceptable level of risk, and RMS needs to work with management what they understand and what is their responsibility. RMS advise them of the risk levels, but in the end, it's up to management what level of risk they would like to accept.

In summary, we must remember that RMS obligation as a risk practitioner is to assess and determine the severity of each of the risks facing the organization, all of the risks related to people, processes, and technology. All the risks that RMS have identified and assessed will be reported to senior management. To complete whole risk management cycle.

IV. CONCLUSION

Risk management specialist has a complex work which requires vast amount of knowledge. Starting from IT hardware, software, architecture to business processes, procedures and methods for risk management but is not limited to mentioned fields. Full risk management cycle includes risk identification, assessment, mitigation and monitoring (

Fig. 1). In order to provide good representation of risks for any given business extra attention and expertise has to be placed on risk identification (not forgetting any significant risks) and risk assessment to provide qualitative and possibly even quantitative values. Risk management has a many more methods and methodologies for accomplishing accurate results, but due to this article limit its not feasible to mention all of them.

Author thinks this article has managed to capture most relevant methods for risk identification and risk assessment phases. Therefore providing good base for further research which will be done on risk mitigation methodologies and risk monitoring.

REFERENCES

[1] National Research Council, (2005) The Owner's Role in Project Risk Management pp.32-33, ISBN:978-0-309-09518-1

[2] Harold F. Tipton, Micki Krause, Will Ozier, Information security management, volume- Risk analysis and Assessment, (2000), pp. 247-285, ISBNm1-8493-9829-0

[3] Anthony Mills, (2001) "A systematic approach to risk management for construction", Structural Survey, Vol. 19 Iss: 5, pp.245 – 252

[4] Heather Douglas, Philosophy of Science, Inductive risk and values in science, 67 (December 2000) pp. 559-579. 0031-8248/2000/6704-0001

[5] Pluralsight course, Risk management Information systems control risk assessment, https://app.pluralsight.com/library/courses/risk-management-information-systems-control-risk-assessment/table-of-contents (2016)

[6] ISO/IEC 27005:2011 second edition, Information technology Security techniques Information security risk management, (2011), pp.17

[7] NIST Special Publication 800-30 Revision 1, Guide for conducting Risk Assessment, (2012), pp 4-37

[8] ISACA, The risk IT framework (2009) Ppp.75-76