A Conceptual Framework on Risk & Incident Management in IT Sector & it's Current Benchmark

Author: Keerthana M, Muthukumaran R

Corresponding Author: Mohammed Sadiq Hussain

qad@srmtech.com

Abstract: *Changes in a dynamic environment expose a company to a variety of risks. If risks are not adequately handled, they will have a detrimental impact on businesses now and in the future. Risk management is a key component of Information Technology (IT) governance. The goal of risk management in IT projects is to create a safe environment for IT initiatives. Risk management has evolved into an important aspect of IT project success. This article looked into the risk of IT projects and whether there was a link between risk management and project success. The strategy used was a literature review of several scientific articles published between 2010 and 2014.*

According to this study, the presence of risk management and risk managers has an impact on the project's success. The subjective performance of IT projects is closely linked to risk analysis, risk monitoring, and risk control. The chances of a project's success can be boosted if risk management is appropriately implemented.

Keywords: *Risk, Risk management, Incident, IT project*

Introduction

Risk management is an activity that includes recognizing risk, assessing risk, devising risk management strategies, and mitigating risk with managerial resources. The primary goal of risk management is to make various risk-related domains acceptable. Risk management is required to deliver and improve stakeholder value over time in our organization. Because effective risk management necessitates better data and information, organizations

should focus on risk-related tasks and endeavor to address them.

Risk management teams must facilitate and encourage acquiring, analyzing the current and forward-looking risk information. It will be easier for management to make better judgments and take measures that create more dependable outcomes if risk can be predicted. It may also reduce the risk coming from client deliverables. In many firms, risk management in the information technology (IT) sector is crucial. Hardware and software failures, human error, spam, viruses, and malicious assaults, as well as natural calamities like fires, cyclones, and floods, are all examples of IT hazards.

Risk management is the process of identifying, analyzing, appraising, and controlling hazards to an organization's capital and profitability. Financial risks, legal liabilities, strategic management failures, accidents & natural disasters are just a few of the dangers and risks that could occur. [1]

In this study, we've attempted to summarize the relationship between risk and incident management in IT, as well as how the evolution of IT has influenced the risk and incident management area.

Risk management is more painful, and it is not a natural human activity.

Risk management process

After the company's specific risks are identified and the risk management process has been implemented, there are several different strategies companies can take with different types of risk [1]

- **Risk avoidance**: While it is rare to eliminate risks altogether, a risk avoidance strategy aims to deflect as many risks as possible in order to avoid disruptive effects.
- **Risk reduction**: Companies can sometimes reduce the impact of particular hazards on their operations. This is accomplished by altering particular components of a project's general plan or company process, or by lowering the scope of the project.
- **Risk sharing**: The effects of risk are sometimes shared or dispersed among numerous project participants or corporate units. A third party, such as a vendor or business partner, could also be informed of the danger.
- **Risk retaining**: Companies sometimes feel that risk is worth taking from a business standpoint, and they choose to keep the risk and deal with the consequences. When a project's expected return is greater than the expenses of its potential risk, companies will often keep a certain level of risk.

Risk Management Standards

Risk analysis, internal audits, and other methods of risk assessment have become crucial components of business strategy. These guidelines are designed to help firms identify specific threats and assess unique vulnerabilities to calculate risk, identify solutions to mitigate risk, and implement risk reduction initiatives according to corporate strategy.

- The procedure should add value to the company.
- Any doubt must be addressed explicitly.
- It should be organized and systematic.
- It must be specific to the project.
- It must account for the possibility of errors.
- It must be able to adapt to change.
- To be monitored regularly

Managing the Uncontrollable

External risks, the third type of risk, are often not reducible or avoidable using the same methods used for preventable and strategic risks. External risks are largely beyond a company's control; organizations should concentrate on detecting them, assessing their possible impact, and determining how to best reduce their impacts if they materialize.

Some external risk events are close enough in time that managers can handle them in the same way that they manage strategy risks. One of the organizations, for example, identified a new risk related to its goal of developing a global workforce during the economic slowdown following the global financial crisis.

Natural and economic disasters with immediate impact:

These dangers can generally be predicted. However, their occurrence is not always predictable. They can be predicted only using a few flimsy indicators.

The consequences are usually severe and quick when these hazards occur, as we saw with the 2011 Japanese earthquake and tsunami.

When the sun shines, there are no clouds on the horizon. Similarly, a company's ability to weather storms is determined based on risk management.

Enterprise risk management (ERM)

ERM is a risk management framework that identifies specific events or conditions (risks and opportunities) relevant to the organization's objectives, analyzes them in terms of likelihood and magnitude of impact, decides on a response strategy, and tracks progress [3]

Governance, risk management, and compliance (GRC)

Organizations grow to the point where they need to coordinate GRC activities in order to function properly. [4] Each of these three disciplines generates useful data for the other two, and they impact the same technologies, people, processes, and data. When governance, risk management, and compliance are managed separately, significant duplication of duties occurs. GRC operations that overlap and duplicate one other have a detrimental impact on both operational costs and GRC matrices. [5]

Risk Information's

Management should be able to continuously capture, evaluate, analyze, and respond to risks resulting from changing internal operations, external markets, or legislation using an effective risk program. Failure to effectively manage these changes can result in financial losses, unfavorable publicity, and a reduction in the organization's ability to achieve its goals and missions.

Risk Management and Information Technology

Information technology has influenced every aspect of our lives such as education, marketing, business, entertainment, and politics. Whereas Risk management requires new technologies such as Big Data, analytics, mobile apps, cloud computing, enterprise resource planning (ERP), and governance, risk, and compliance (GRC) solutions. There are also several essential well-known service providers, such as Microsoft [6], as well as a number of alternative applications, such as CORAS threat modeling [7].

Social Media

Some organizations are now actively monitoring social media content to gather timely information on customer service, product quality, and service delivery difficulties.

In this case, readily available social media content provides valuable insights into the public's perceptions of the company's products and services, providing management with tools to promptly resolve service and product quality issues before they have a severe impact on the

brand or franchise, allowing the company to avoid reputational damage [8]

Data Mining

Data mining techniques are used to predict component or machinery failure, uncover fraud, and even forecast business profitability in an organization. To determine whether a transaction is fraudulent, you could use credit card authorization techniques [9]

Risk Methodology

The risk is assessed in an organization using three ways which are mentioned below,

- **Confidentiality**: Information should be confidential & should not disclose to a third party.
- **Integrity**: Safeguarding the accuracy and completeness of information assets.
- **Availability**: Documents accessed only by the authorized entity.

The CIA of information security plays a significant role in risk. In starting to evolve your information security risk management methodology, conflicts and priorities are looked at often in addressing CIA-based risk [11]

Risk identification

An information asset tied to an internal/external issue could be the source of the risk.

Risk analysis

Once you know the risks, you need to consider the likelihood and impact (LI) to allow you to distinguish between (say) low likelihood and low impact, versus higher ones.

Risk evaluation

You can then prioritize expenditures where they are most required and conduct assessments based on the likelihood and impact positioning after considering the risk. The risk assessment can be done using criteria that vary from extremely low to very high likelihood.

Risk treatment

Treatment of the risk, which is also known as 'risk response planning' must include the evidence behind the risk treatment.

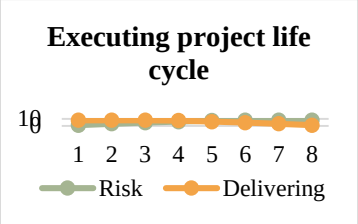
Vulnerabilities

Organizations that want to protect themselves against cyber-attacks should think about a variety of issues. While many cyber dangers may be systematically avoided, human factors can have a significant impact on an organization's vulnerability.

> Vulnerability is not weakness; it's our most accurate measure of courage

As a result, it's critical to assess your firewalls and how your company divides internal LAN traffic.

Risk/ Impact



The graph depicts the total cost impact is less if the risk event will occur earlier and therefore it is very important to use that period to minimize or mitigate around a potential risk. Moreover, as it goes further into the project phase the increase in cost is very steep. [13].

Downtime

Because of a lack of system patching, sufficient monitoring, and internal and external security measures, events could result in downtime, creating an exposed vulnerability [11]

Ransomware, for example, can cause significant disruption until a reliable backup is restored or files are unlocked. Frequent occurrences of downtime lead to large financial losses and an under-productive workforce.

Data encryption

Companies that process or maintain personal information are responsible for information protection. There are standards for credit card processing, medical records, and privacy that could result in hefty legal fees, credit protection service costs, and implications on the organization's reputation if that data is lost or stolen. Encrypting that data both in motion and at rest is mandatory under many of these standards [12]

Ransom

A ransom is a payment made to a harmful actor to restore a working environment. When a user visits an infected site or clicks on a link within an e-mail, malware downloads files or data without the user's knowledge. Ransom ware is also seen as a breach.

According to many experts, the question isn't when you'll be infected by malware or when you'll be compromised, but when you'll realize you've been compromised. In order to avoid being hacked, you'll need appropriate defenses that can actively monitor and correlate activities that occur in your computing environment. Building a partnership with a respected third party with forensic competence could be beneficial.

Reputation

It takes a lifetime to build a good reputation, but just a moment to destroy it. Strong organizations possess good reputations when they maintain good practices and provide exceptional products and services. Consumers expect organizations to protect their data. When this happens, the organization's reputation is also compromised. Reputation can also be compromised when an organization's website is attacked, sensitive data is likely exposed and the site's content is changed, or a denial of service prevents consumers from accessing the website.

Data Loss / Data Theft

Data is located in many places. It can be located on printed documents, mobile devices, backup media, databases, flat files, file stores, websites, and any number of other places. Organizations should have a data classification policy that identifies critical data. The more sensitive the data, the more valuable they are, and the higher access controls should be in place.

Data Loss

It is essential to know where data is in your environment, so that you can ensure appropriate access. Data loss is when data is not where it is supposed to be. Say you store your backup tapes at a specified location, and all backups are supposed to be there. One day you need to perform a restore of the data and realize the backup is not there. This is data loss.

Data Theft

Data theft, is when your environment is breached, and that data is taken. Data theft could also occur internally when an employee transfers sensitive data to cloud storage or portable storage, like a USB stick. Your organization's policy should indicate who has access to sensitive data and how it should be handled.

Breach

A breach is referred as an unauthorized access to a network, system, application, or data occurs. A breach can occur with or without the knowledge that it occurred by the owner or custodian of the network, system, application, or data.

Incident Management

The IT team uses incident management to respond to an unanticipated occurrence or service outage and return the service to its operational state. The IT team will investigate the incidents that end-users reported.

The IT operation team will log the incident and attempt to categorize it, as well as rank it as low, medium, or high priority. Once the incident status is understood, they will attempt to resolve and shut the event depending on the project team's escalation. Once the end-user disturbance has been minimized, the team can work on a long-term solution to the problem. Because the same events may occur often, IT staff evaluates and logs the incidents for future reference. This reduces the length of time it takes to recover from a specific incident.

Levels in incident management

IT incident management is usually divided into three tiers of support, usually, put together in a help desk or service desk. Most firms utilize a support system for incident categorization and priority, such as a ticketing system. IT employees handle incidents according to their priority level.

An incident manager ensures that the IT support and service delivery teams follow proper incident response and management procedures.

Every occurrence in a company should be viewed as an opportunity to learn and grow.

Incident management tools

Help desk and incident management teams employ various tools to address events, including operations data monitoring tools, root cause analysis systems, incident management and automation platforms, and other support solutions. IT personnel can use monitoring tools to gather data from numerous systems, including on-premises and cloud-based hardware and software.

Root cause analysis tools aid in the examination of operational data provided by systems management, application performance monitoring, and infrastructure monitoring tools, such as logs.

Case Study

Strategic information is primarily designed to help decision-makers manage risk. However, as the world becomes increasingly reliant on information technology, non-financial operational risks such as cyber risk have gotten increased attention from practitioners and scholars in recent years.

An information security management system's (ISMS) purpose is to protect data assets while also providing a systematic risk management strategy. As a result, it assists businesses in achieving their own information security goals as well as those of their customers, in addition to adhering to legal information security rules.

Conclusion

This paper presents a brief introduction of risk management, and a few occurrences have been managed and recorded in an organization. The risk-related process, as well as methodologies and standards, are detailed.

Identification of vulnerabilities and threats to information resources, risk assessment, and risk control are all steps in risk management that can help decrease the risk to an acceptable level. This study discovered that by using appropriate project delivery techniques, risk and incidents in the IT sector can be decreased. It is successful when the project's outcome is as good as or better than the planning. Proper risk management leads to its success only if the risks and how to control them in the project have been identified before the project has begun.

It can also help the project team realize their aim of delivering high-quality work products, as well as lead to the organization's continual progress. One of the future projects that might be undertaken is to investigate the risks posed by the use of information technologies in order to analyze the hazards in an organization.

References

[1]Margaret Rouse, “What is risk Management?”, URL: http://searchcompliance.techtarget.com/definition/risk-management, Date accessed: 2017–12–23

[2] ISO organization , “ISO 31000 — Risk management”, URL: https://www.iso.org/iso-31000-risk-management.html, Date accessed: 2017–12–26

[3] Thomas H. Stanton, “Enterprise Risk Management”, URL: https://www.youtube.com/watch?v=voGyHN-tWMg, Date accessed: 2017–12–25

[4] OCEG, “GRC Capability Model”, URL: https://go.oceg.org/grc-capability-model-red-book,Date accessed: 2017–12–25

[5] OCEG, “Risk Management is at the heart of GRC and Principled Performance”, URL: https://www.oceg.org/about/people-like-you-risk/, Date accessed: 2017–12–26

[6] Microsoft, “Microsoft Threat Modeling Tool 2016” , URL: https://www.microsoft.com/en-us/download/details.aspx?id=49168, Date accessed: 2017–12–26

[7] “The CORAS method”, URL: http://coras.sourceforge.net/, Date accessed: 2017–12–26

[8] Tom Patterson, “The Use of Information Technology in Risk Management”, Date Published: Septembet-2015

[9] ICAR, “How does Big Data help with financial risk management?”, URL: https://www.icarvision.com/en/how-does-big-data-help-with-financial-risk-management-, Date accessed: 2017–12–25

[10] Martin Brown, “Data mining techniques”, URL: https://www.ibm.com/developerworks/library/ba-data-mining-techniques/, Date accessed: 2017–12–23

[11]https://towardsdatascience.com/how-information-technologies-influenced-risk-management-7eb3a38d253

[12] https://www.isms.online/iso-27001/information-security-risk-management-explained/

[13] http://apppm.man.dtu.dk/index.php/Risk_management_process