The Factor Cloud Computing in IT Risk Management

N. I. Yusupova
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: yussupova@ugatu.ac.ru

U. Konrad
Helmholtz-Zentrum Dresden-Rossendorf e.V.
Department of Information Technology
Dresden, Germany
e-mail: u.konrad@hzdr.de

V. J. Penzina
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: penzina.vladislava@gmail.com

Abstract[1]

In XXI century, information, along with other factors, is a valuable and vital component of the organizations. Meanwhile using the information technology, risk management plays a crucial role in protecting their information. Effective risk management is one of the most important parts of a security program in IT department of organization. This paper represents definition of risk management, first steps of the process and influence of cloud computing according to vulnerability identification and controls and measures analysis subprocesses.

1. Risk management

In the present digital age, organizations use information technology IT, for processing their information to fulfil their mission.

Risk is a probability or threat of damage, injury, liability, loss, or other negative occurrence that is caused by external or internal vulnerabilities, and that may be neutralized through pre-emptive actions.

Risk management (RM) is the process to identify and access risk and to apply methods to reduce it to an acceptable extent. The main goal of risk management is to help organizations better manage risks associated with missions of the company.

An effective risk management process is the most important part of a highly reliable IT system.

The IT Risk Management (IT RM) is the application of risk management to Information technology context in order to manage IT risk. IT risk – the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. [1]

Risk management is a process that allows IT managers to balance the operational and economic costs of achieving goals with the protection of IT systems and capabilities of organizations to achieve missions. Fig.1 shows main steps of Risk Management process.

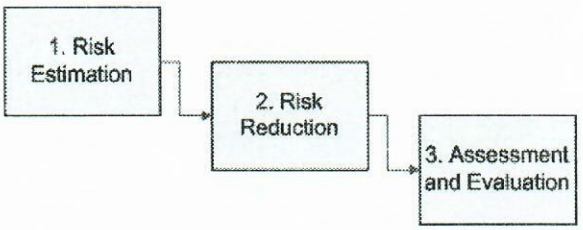

Fig. 1. The process of Risk Management

Correct scale of risks will be the basis for the categorization of information circulating in the company in the future, and will simplify the process of risk assessment in general. According to company's needs and experts knowledge particular significant risks sources were segregated (Fig.2).

The first step in the definition of the action scope is system characterization (Fig.3). In this step, for assessing the risks of the IT system, the field for risk assessment is imposed, the boundaries of a valid application are drawn and essential information is provided. In this step resources, information and IT system boundaries are defined. The question of requirements for fulfilling the criteria of the five Datacenter Stars categories (1–5 stars) of the DC Star Audit certification was also included in the Input field.[7]

[1] **Proceedings of the 14th international workshop on computer science and information technologies CSIT'2012, Ufa – Hamburg – Norwegian Fjords, 2012**

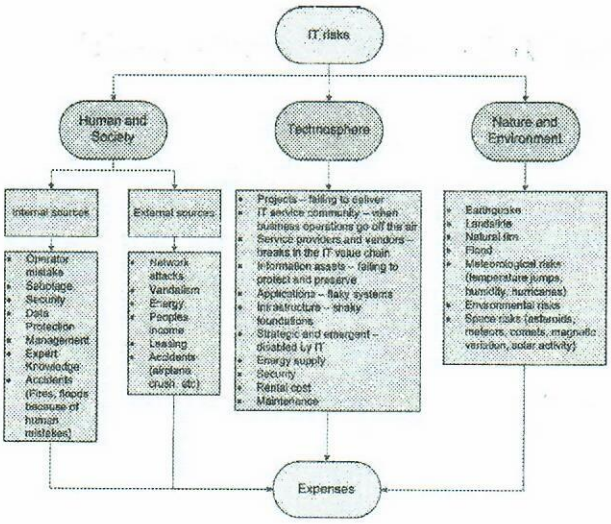

Fig. 2. IT risks classification

The features of an assessed IT system, give a good image of IT system environment and describes the system boundary.

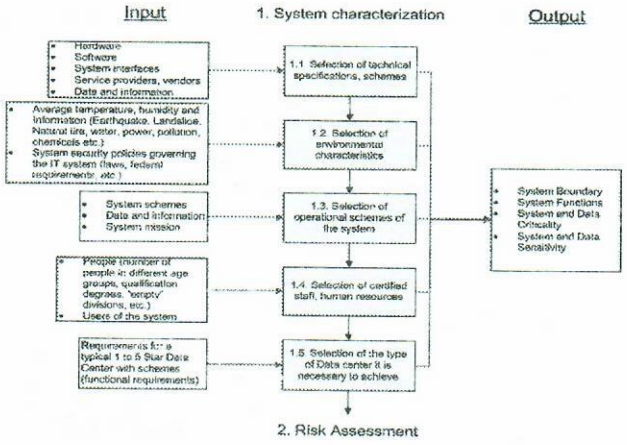

Fig. 3. System characterization subprocess of IT RM

Fig.4 represents risk assessment subprocess of IT RM.

A risk assessment is a process to determine what information resources exist that require protection, and to understand and document potential risks from security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for the stewardship of IT assets.

Main steps in risk assessment subprocess are:

- Threats identification – a specific threat source, vulnerability is potentially successful performance. In determining the probability of a threat, the person must consider threats resources, potential vulnerabilities and the existing controls. In output field: list of threats resources that could create some damage;
- Vulnerability identification – analysis of threats in IT systems should include analysis of vulnerability with consideration of the system environment. The purpose of this step is the development of system vulnerabilities list (deficiencies and weaknesses) that could potentially be used by the threatening sources. In output field: a list of system vulnerabilities that could potentially be used by threatening sources;
- Controls and measures analysis – the purpose of this step is analysis of the controls that are applied by the organizations in order to minimize or limit the likelihood of threats becoming practical in a vulnerable system. In output field: a list of current or designed controls used for IT systems, so that the risk of vulnerability and incompatible events can be reduced.

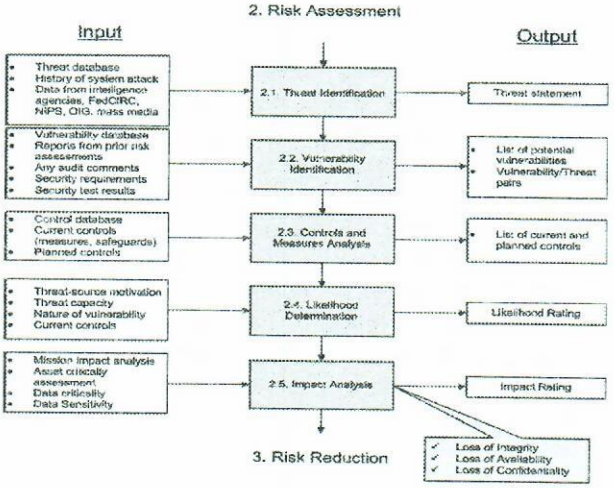

Fig. 4. Risk Assessment subprocess of IT RM

2. Cloud Computing

Cloud computing is a new computing paradigm and the evolutionary offspring of parallel computing, distributed computing, utility computing and grid computing, and the developmental outcome of network storage, virtualization and load balance. Cloud computing is introducing huge changes to people's lifestyle and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always in focus, and a big barrier for its widespread applications. The main idea of cloud computing is to build a virtualized computing resource pool by centralizing abundant computing resources connected with network and present the service of infrastructure, platform and software. This network that offers various computing resources is called "cloud".

Major corporations including Amazon, Google, IBM, Sun, Cisco, Dell, HP, Intel, Novell, and Oracle have invested in cloud computing and offer individuals and businesses a range of cloud-based solutions, like social networking (Facebook, LinkedIn, Twitter, etc), e-mail

(Microsoft, Yahoo, Google, etc.), document, spreadsheet, other hosting services (Google Docs, Zoho Office, Onit, etc.) and other cloud-based solutions.

Since the cloud computing specification of National Institute of Standards and Technology (NIST) has been proposed, the definition of NIST about cloud computing becomes the most authoritative one widely accepted by researchers. The cloud computing definition of NIST includes five essential features, three service models and four deployment models as figure 5 shown. [8]

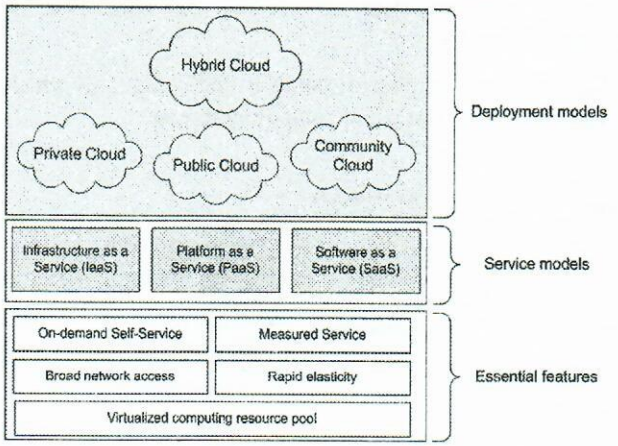

Fig. 5. Cloud Computing NIST definition

Laws and legal provisions regulating the use, processing and storage of data have to be adhered to when storing data in the cloud. This applies to all parties involved: the cloud user who stores data in the cloud, the cloud provider who offers cloud storage services and potential subcontractors who provide resources or infrastructures for the cloud provider. Each of the aforementioned parties is subject to legal regulations and provisions of the country in which the respective party is based. These legal regulations and provisions may concern personal rights (e.g. data privacy), data security or access rights for fiscal or law enforcement authorities and may differ from country to country.

In Germany several legal provisions and laws regulate the use, processing and archiving of data. Those legal requirements must be adhered to by cloud users when storing data in the cloud. Which regulations have to be followed when using cloud computing services depends on the kind of information being stored in the cloud. Data which concerns the personal rights of others, so-called personal data, has to be protected according to the German Federal Data Protection Act 10 (Bundesdatenschutzgesetz (BDSG). [9]

For this reason it is important to clearly identify the types of information circulating in the company and determine which ones could be placed in the "cloud".

3. Cloud Computing Cube Model

There are several "cloud formations" - or forms of cloud computing. Each offers different characteristics, varying degrees of flexibility, different collaborative opportunities, and different risks. Thus one of the key challenges that organizations face when considering cloud computing as an option is to determine how to choose the cloud formation best suited to their various types of operations.

Cloud cube model is a figuration description of security attribute information implied in the service and deployment models of cloud computing and certain selected parameters as figure 6 shown. [2]

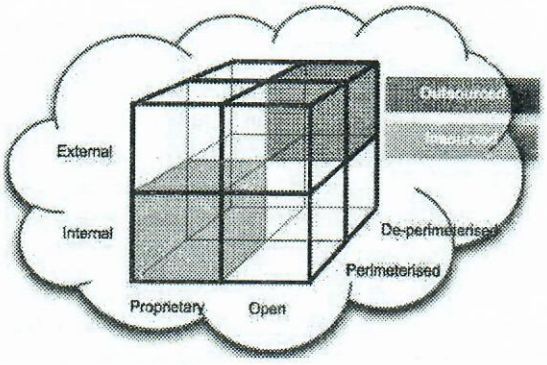

Fig. 6. Cloud Computing Cube Model

In cloud cube model, the definitions of model parameters are as follows:

- Proprietary/Open: a model parameter to define the ownership of cloud's technology, service and interface etc. This model parameter indicates the degree of the portability of data and application between proprietary system and other cloud modalities, and the ability of transforming data from a cloud modality to other cloud modality without any constraint. Proprietary means that a cloud service provider holds the ownership of facilities providing cloud services, hence the operation of cloud is proprietary and customers can not transfer their applications from one to another cloud service provider without great effort or investment. The technologies used in public cloud are generally open and uniform, meaning more available service providers and less constraint on data share and incorporation with business partners.
- Internal/External: a model parameter to define the physical location of data storage. If the physical location is inside of the data owner's boundary, then the model parameter value is internal. For example, the data center of a private enterprise cloud is internal, and the data center of Amazon's SC3 is external. But the cloud with internal data storage is not more secure than the one with external data storage. The combination of internal and external data storage maybe present more secure usage model.
- Perimeterised/De-perimeterised: a model parameter to describe the "architectural mindset" of security protection, i.e. a customer's application is inside or

outside of traditional security boundary? Perimeterised means that a customer's application operates within traditional IT security boundary signalled by firewall that blocks the incorporation of different security zones. In fact, customers running some applications inside of security zone can extend/shrink their application perimeter to/back from external cloud environment by VPN. De-perimeterised means that the fade way of traditional IT security boundary and the exposure of a customer's application operation.

- Insourced/Outsourced: a model parameter to define the 4th dimension that has two states in each of the eight cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO). Insourced means that cloud service is presented by an organization's own employees, and Outsourced means that cloud service is presented by a third party. These two states answer the question "who do you want to build or manage your cloud service?"

In cloud cube model, other attributes such as Offshore and Onshore are also relevant to cloud computing.

Cube model provide the key considerations that need to be taken into account when deciding which parts of information and data could be operated in which of the available cloud formations.

According to the IT-Grundschutz Catalogue (Germany) a list of elementary threats for a typical medium data center was compiled. [3] Also was taken into consideration main threats which occur when using cloud computing services. (Fig.7)

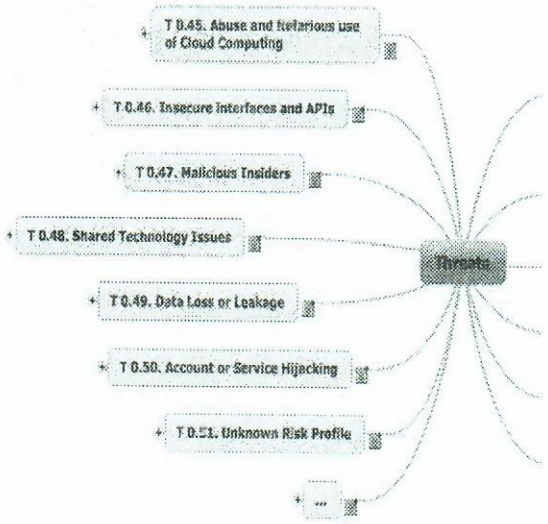

Fig. 7. Top Threats to Cloud Computing

Criminals and spying organisations continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited. For example, reliance on a weak set of interfaces an APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability. The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation.

The next phase of risk management is intended to provide exactly required steps to prevent the realization of potential threats.

Fig.8 shows a number of controls and safeguards which are directed against cloud computing threats.

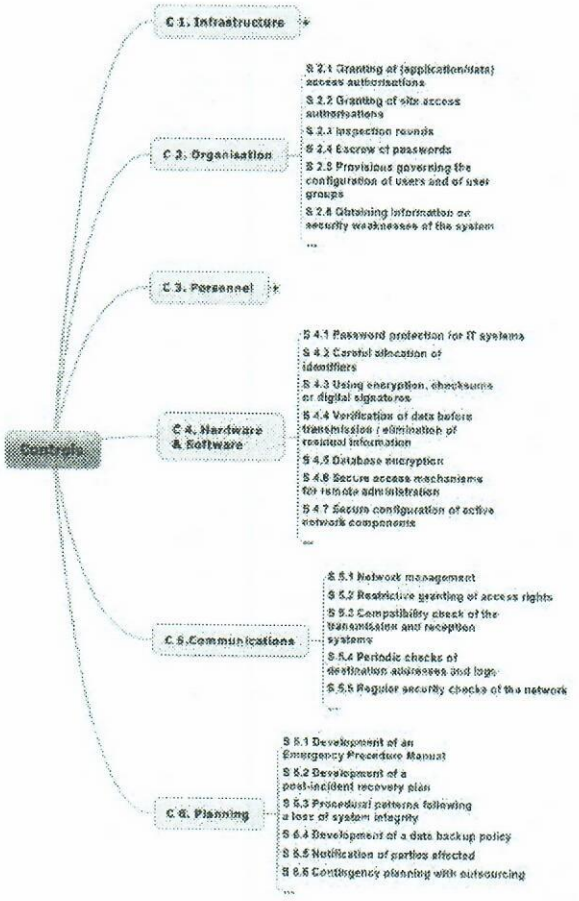

Fig. 8. Controls and Safeguards for Cloud Computing threats remedation

At present, the classification of countermeasures to reduce the likelihood of threats has a classic character. Companies assign safety and sourcing as a more important fields.

Due to the role of IT systems in organizations and considering the potential and actual existing threats and vulnerabilities in these systems, a management plan and program to curb these risks is essential. Understanding of

risk management processes and the people who play an important role in running these processes their existence can secure organizations in reaching their missions and it is something important and necessary. To achieve this goal also depends on broad support and participation of managers, members and officials of the organization.

4. Conclusion

Cloud Computing represents one of the most significant shifts in information technology. Customers are excited at the prospects of Cloud Computing. However, customers are also very concerned about the risks of Cloud Computing if not properly secured, and the loss of direct control over systems (information or data) for which they are nonetheless accountable.

IT Risk Management can provide such a protection. Use of risk management methods gives opportunity if not to eliminate, at least significantly reduce probability of damages or negative occurrences of threats.

In this article the principle of risk management in IT, influence of Cloud Computing on IT RM was investigated. Therefore the definition and a model of Cloud Computing ware considered. Finally threats and controls were expanded.

Acknowledgements

The research is supported by the Russian Fond of Foundation Research grant № 12-07-00377-a, the research work is performed within the state work on development of software tools support decision-making for different kind of management activity in industry in the conditions semi structured data based on the technology of distributed artificial intelligence.

References

1. Hamid Tohidi "The Role of Risk Management in IT systems of organizations", Procedia Computer Science 3 (2011) 881-887
2. Jericho Formu "Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration" April, 2009. http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf.
3. BSI Standard 100-2 IT-Grundschutz Methodology, 2008 Bonn, Germany
4. Cloud Security Alliance. Top Threats to Cloud Computing, 2010. http://www.cloudsecurityalliance.org [accessed on: March, 2010].
5. Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan "Study on the security models and strategies of cloud computing", Procedia Engineering 23 (2011) 586 – 593
6. Moritz Borgmann "On the Security of Cloud Storage Services", SIT-TR-2012-001, March 2012 Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany
7. Levels of Performance Datacenter Star Audit, November, 2010, www.dcaudit.de, eco – Association of the German Internet Industry, Köln, Germany
8. The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, September 2011
9. Federal Data Protection Act, Germany (Bundesdatenschutzgesetz (BDSG)) Online Available http://www.bfdi.bund.de