AARMS Vol. 15, No. 3 (2016) 279–290. **10.32565/aarms.2016.3.8**

Risk Management of New Technologies

Tamás SZÁDECZKY[1]

Nowadays businesses face multiple issues regarding new phenomena like cloud computing, which is a great business impetus: with the minimization of capital expenditure (CapEx) on IT infrastructure and personnel the efficiency can be improved. Technically this is not a new invention, but it is changing the approach to IT service, which has become outsourced, highly adaptive and scalable. Of course, the change in the technical landscape always implies security issues. Information security is not just a set of technical countermeasures: it is also a business requirement. It will help to avoid financial loss, avoid bad reputation or increase trust among clients.

The article analyses business alignment of information security in the case of cloud services. It shows the results of research, where the theoretical and practical issues of risk assessment-based business decision support were analysed and proved. Its finding was that there are cases when we can do examination, but general automatized tools are inadequate. However specialized tools and sometimes third party certifications should give more support.

Keywords: *risk management, cloud computing, IT security*

Introduction

In the early decades of IT history, the security profession fought for legitimacy of cyber security, and attention of high level management which did not really understand the importance of this field. The question now, at the beginning of the twenty-first century is not the why but the how and the how much information security. In the private sector, especially in times of economic crisis, cost constraints can be severe. Management's objective is to invest usually minimal resource on IT security elements, systems and networks. We find every day that the decrease in IT budget implies more decrease in security budgets at companies.

The aim of the research was to find out if risk assessment techniques are useful to support the above-mentioned security decisions or not. Security risks of implementing a cloud-based technology have been analysed from theoretical and practical views. A small company which is using cloud services actively lets the author do field research and do the risk assessments in a live environment thus analysing business drivers of information security. The full monography about the research is source [1].

---

1 Ph.D., National University of Public Service, Faculty of Political Sciences and Public Administration, Institute of E-Government; e-mail: szadeczky.tamas@uni-nke.hu

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled "Public Service Development Establishing Good Governance" in the Miklós Zrínyi Habilitation Program.

Discussion

Cloud computing is a kind of outsourcing from the business side. “In the realm of information systems (IS), outsourcing involves making arrangements with an external party for the partial or total provision of the management and operation of an organization’s information technology (IT) assets or activities.” [2: 624]

According to NIST 800-145, by definition the cloud services have five essential characteristics: virtualized computing resource pool, broad network access, rapid elasticity, on-demand self-service and measured service. [24: 2] These features make the difference from classical server-based on-line service provision. Cloud computing is a well-developing IT service, it was already a $17 billion business in 2014. [3] Nowadays numerous conventional outsourcing or server-based service providers claim that they provide a cloud service, despite not meeting the above mentioned minimum requirements as Avram emphasizes. [4] This is actually a misrepresentation and a breach of contract. Cloud service providers build their computing centres geographically dispersed. Resources between systems are dynamically allocated, no matter where we are using the service to store our data at the moment. [5] As Mense points out, the security features of a private cloud are highly different: we can achieve a much higher security level with that than the public one. [6]

Virtual systems are scalable, flexible and redundant, when they are built according to general best practice. But the hypervisor is a new single point of failure, because it is generally not redundant. According to Metalidou, human factors are always an issue in information security, therefore awareness should be increased. [7] As Suicimezov and Georgescu point out, cloud systems typically involve Big Data issues during operation. [8] According to Brunette, the answers to those problems are to keep a high level of compliance according to Cloud Security Alliance’s recommendations. [9] Because of the scale, with the concentration of capital a cloud service provider may invest more money on security than a bank. [10]

If we are about to implement security measures in a cloud system, one choice is to use general best practice, but it is not favourable, as it cannot be audited objectively. Information Systems Audit and Control Association’s (ISACA’s) Control Objectives for Information and Related Technology (COBIT) are a de facto information security standard, as the framework system of IT governance as detailed in source [11]. The International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27000 family of standards was set off in the United Kingdom and now they are well-known and used all over the world and there are currently 45 members published or in preparation. The standard is process-centred, and applies the Plan-Do-Check-Act (PDCA) model and the implemented system integrated into existing quality control (ISO 9001) and environmental management (ISO 14001) systems. Payment Card Industry Data Security Standard (PCI DSS) is a standard for payment card security and it can be used in special cases when debit or credit cards are accepted by a merchant. As detailed in [12] data protection can be regarded as a legal area, which has a high impact on information security, especially in cloud systems.

Risk management theory

The risk-based thinking, which relies on mathematical rules, came into existence by the work of Blaise Pascal in the 17th century. Despite it roughly meaning uncertainty, according to Habegger, it is a key element in all political and economic activity. [13] There is still a debate if risk is equal to uncertainty according to Belyacz. [14] During the next century it became daily used: insurances, sampling, expectancy calculations were made. For a long time, risk management dealt with a sole issue, typically with decision making and financial analyses.

Decision making is a management and policymaker's issue with large literature based on mathematical statistics. Decision making in a well-known case can be described as a vector, but the more uncertainty is in the system, the larger table has to be made for the description. [15] The concept of decision making is that there is a goal or objective to achieve, but there are more alternative courses of action to achieve that, but our knowledge on the issue is imperfect, which creates doubt, but this doubt may be reduced. [16]

Financial markets are more complex than to be able to describe their mechanisms with Gaussian or Lévy distributions. They also depend on external factors, like news. This is how it became more and more complicated and therefore new methodologies have to be developed like 'Δ' hedging and Black-Scholes limit. [17]

In the 1980s the professional thinking on the coordination of previously unconnected risks started by the Fortune magazine's article "The Risk Management Revolution".

As analysed in regard to security controls in Section 3, there is a possibility to do things on our own, or using standards for a professional problem has advantages. In 1980, risk was generally $R = I \times P$ where I is the impact and P is the possibility, but this became more sophisticated nowadays. [18]

The first governance tool capable for general risk management was the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework. [19]

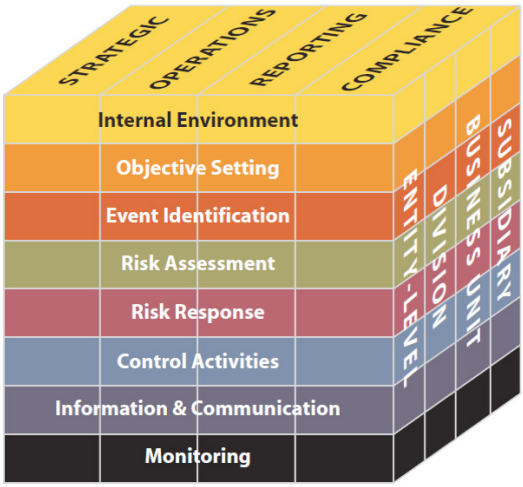

Figure 1. Components of Enterprise Risk Management. [20: 23]

The aim of COSO ERM is to provide value to the stakeholders with alignment of risk appetite and strategy, enhancement of risk response decisions (risk avoidance, reduction, sharing, and acceptance), reducing operational surprises and losses, identifying and managing multiple and cross-enterprise risks, seizing opportunities, and improving deployment of capital. In order to achieve them it provides a complete framework with multiple-level components as shown on Figure 1. Despite this being a general framework, it is frequently thought that it is only for banking, financial or back-office process-related use cases. This can happen because the founders are financial accounting-related companies. Also, its complexity may be frightening for the potential user. [19]

However, there are numerous widely used frameworks and de facto standards, the international standardisation lies in the hands of ISO. There numerous valid risk-related international standards. Below you find a non-exhaustive list of them.

General risk management ISO and IEC standards:

- ISO 31000:2009 Risk management – Principles and guidelines;
- IEC 31010:2009 Risk management – Risk assessment techniques;
- ISO/TR 31004:2013 Risk management – Guidance for the implementation of ISO 31000;
- ISO Guide 73:2009 Risk management – Vocabulary.

Specialised risk management ISO and IEC standards:

- ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management;
- ISO 14798:2009 Lifts (elevators), escalators and moving walks – Risk assessment and reduction methodology;
- ISO 14971:2007 Medical devices – Application of risk management to medical devices;
- ISO/TR 11633-1:2009 Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis;
- ISO 17666:2003 Space systems – Risk management;
- ISO/IEC 16085:2006 Systems and software engineering – Life cycle processes – Risk management;
- IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities;
- ISO 10993-1:2009 Biological evaluation of medical devices – Part 1: Evaluation and testing within a risk management process;
- ISO/TS 10303-1467:2011 Industrial automation systems and integration – Product data representation and exchange – Part 1467: Application module: Risk management;
- ISO 15743:2008 Ergonomics of the thermal environment – Cold workplaces – Risk assessment and management;
- ISO 22442-1:2007 Medical devices utilizing animal tissues and their derivatives – Part 1: Application of risk management;
- ISO/TS 22367:2008 Medical laboratories – Reduction of error through risk management and continual improvement;
- ISO 12100:2010 Safety of machinery – General principles for design – Risk assessment and risk reduction;

- ISO/TR 14121-2:2012 Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods;
- ISO 13073-1:2012 Ships and marine technology – Risk assessment on anti-fouling systems on ships – Part 1: Marine environmental risk assessment method of biocidally active substances used for anti-fouling systems on ships.

The most important general risk management standard is ISO 31000:2009 Risk management – Principles and guidelines. This became the gold standard of the general risk management, in spite of its main components are also present in other standards.

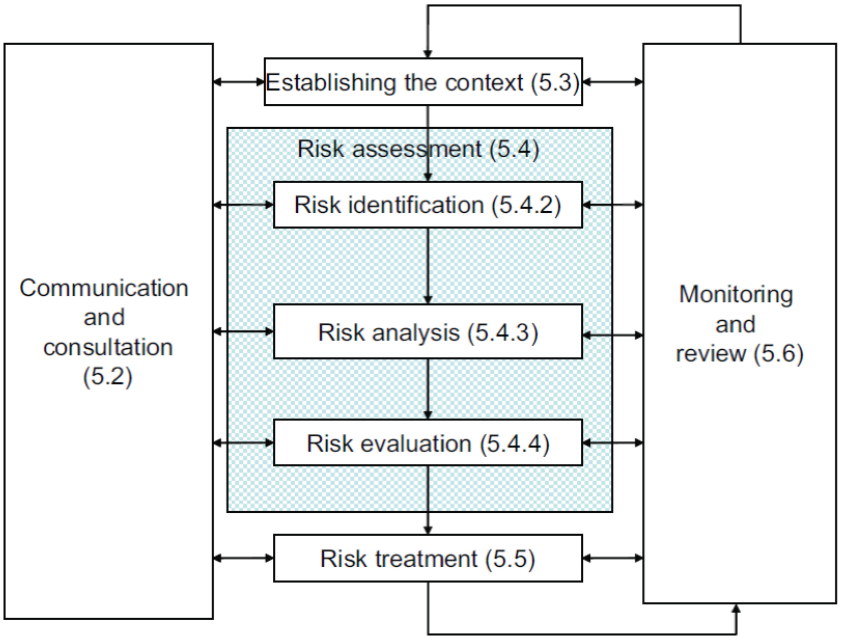

Figure 2. Risk management process. [25: 14]

One of its main elements is the risk management process, which is shown in Figure 2, is very similarly present in ISO/IEC 27005:2011 Figure 2. Risk management process is a "systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring (2.28) and reviewing risk (1.1)" according to ISO Guide 73:2009, definition 3.1. [26]

In spite of this not being a brand-new thing, it is very useful for standardising the process itself. The establishment of such a risk management project is presented in Figure 3.

There are numerous risk management and risk analysis methods. As an example, I introduce the Method for Harmonized Analysis of Risk (Méthode harmonisée d'analyse des risques – MEHARI) here, developed by French Information Security Club (Club de la Sécurité de l'Information Français – CLUSIF). MEHARI's actual version is 2010. It is a qualitative[2]

2 Using scales in contrast to quantitative methods, where precise numbers are calculated like probability for a certain threat is p = 0.078

risk assessment and risk management method that also includes (in Excel files) the list of threats, generic risk situations, with some best practice probability presumptions based on French inputs. With those spreadsheets, it is possible (manually) to conduct the calculations. It is compatible with ISO/IEC 27005 and includes pre-built compliance checks for ISO/IEC 27001.

Phases of risk analysis:

- context establishment with scope definition and boundaries;
- valuation of assets;
- risk identification with confidentiality, integrity and availability factors and probability of threats;
- risk analysis: risk scenarios are set by default, however you can fine-tune it;
- risk evaluation on a 4-level scale.

Phases of risk management:

- risk assessment: display of critical risks;
- risk treatment: treatments options can be selected from reduce, accept, transfer and avoid;
- risk acceptance can be done on an individual basis;
- risk communication: stakeholder assignment can be done since the start of analysis.

The questionnaire can be assigned and tailored to stakeholders. In the case of MEHARI, there is a so called basic tool, with which we can do the calculations in excel sheets. However, this is a quite straightforward way, a more complex tool can make the risk management mechanism easier.

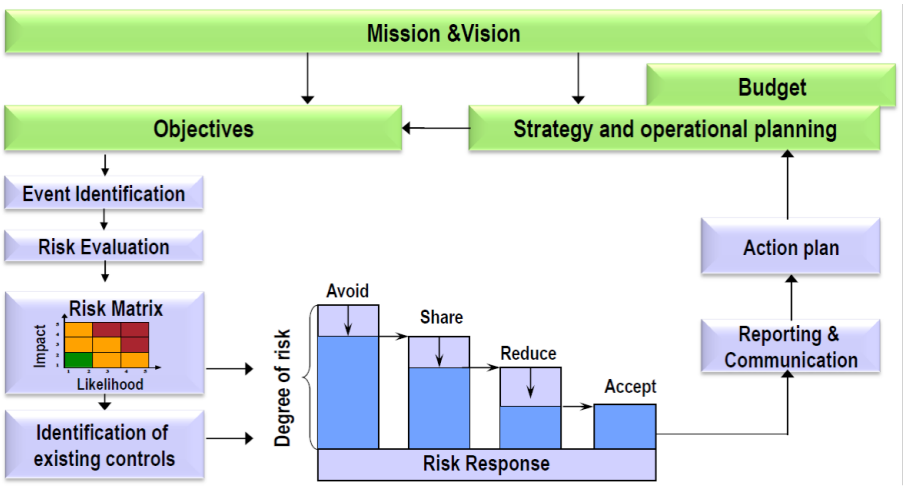

Figure 3. Establishing a risk management process. [19: 15]

Results

In order to research the business alignment of cloud computing, I decided to do a field study. The selected company is a small Hungarian software development Ltd., which is using public cloud services intensively. Actually, their whole business process is based on cloud services: for company e-mail they are using Gmail at Work, for data storage Google Docs and development related servers are in Microsoft Azure.

I have conducted a risk assessment with the above-mentioned ISO/IEC 27005-based MEHARI method, with the usage of the MEHARI-Risk tool. The scope of the assessment has been set to as narrowly as possible. The full research documentation is available in source [1].

After setting up of the scope and primary classification, a questionnaire is generated, which is 58 pages long, so approximately 930 individual questions were answered two times, because the on-premises and the cloud-based were two different assessments. It the answers, all known problems were included, such as interoperability problems of different used technologies. [21] As well as harm to cyberterrorist attacks because of sole online presence. [22]

The formal interviews were conducted in March 2014, and July 2014, in an ISO/IEC 27001 audit and the remaining questions were answered in an interview in February 2015. As soon as all the questions were answered, MEHARI-Risk generated a 25 page long report. At the end of the report we find radar diagrams, which show the findings.

At the end of the report we find two radar diagrams, which show the findings. In Figures 4 and 5 I show the "Risk seriousness for selected causes" radar diagrams for the on-premises and the cloud-based services next to each other. The description below the diagrams is the same for both. In the table the bold rows shows the differences.

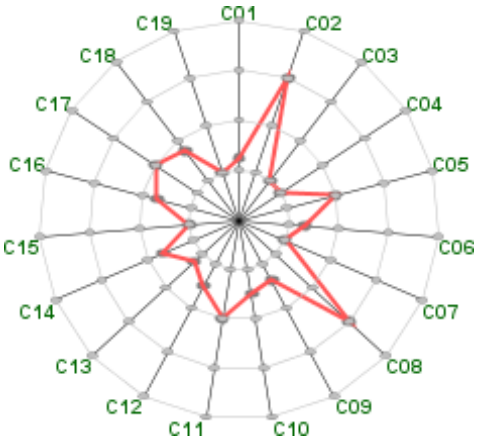

Figure 4. Risk seriousness for selected causes, on-premises.
[Generated with MEHARI-Risk, edited by the author.]

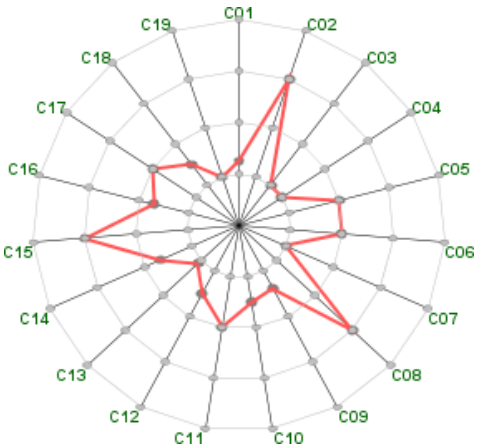

Figure 5. Risk seriousness for selected causes, cloud service.
[Generated with MEHARI-Risk, edited by the author.]

Cause	Cause description
C01	Theft of written or printed documents
C02	Accidental crash of a disk drive
C03	Absence of personnel
C04	Loss of documents by accident
C05	Data erased by a logical bomb
C06	**Access and consultation of system data**
C07	Theft of data media
C08	Accidental erasure of software
C09	Transient information pick up
C10	Accidental loss of files
C11	Theft or erasure of removable media
C12	Media erased by virus
C13	Accident or failure of one or several hardware resources
C14	Complete unavailability of premises
C15	**Diversion of temporary information created by the systems**
C16	Access to file servers and copy of office related files
C17	Deliberate erasure of media
C18	**Maintenance unavailable**
C19	Diversion of information during transmission

We see that there are three changes:

- C15 Diversion of temporary information created by the systems: this is much higher in the case of a cloud-based system. This should be because of the lack of audit possibilities; however, the magnitude of the change seems to be not proportional.
- C06 Access and consultation of system data: this is slightly higher in the case of a cloud-based system. This is because we do not have enough control over the system and especially the hypervisor.
- C18 Maintenance unavailable: this is slightly lower in the case of a cloud-based system. This is because the pool of IT engineers present at the provider and the very high level of maintenance contracts and spare parts.

On the next diagrams (Figures 6 and 7), called “Risk seriousness for selected scenarios”, we see five major scenarios. The on-premises and cloud-based diagrams are again next to each other, with the common table.

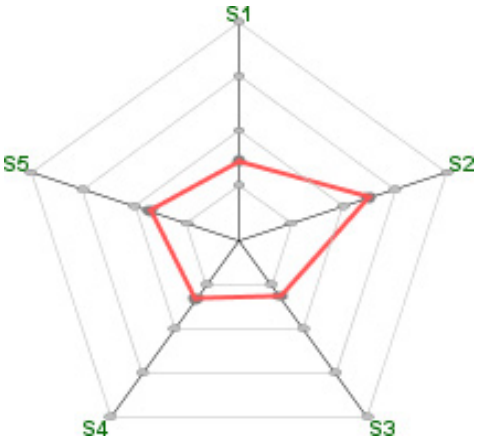

Figure 6. Risk seriousness for selected scenarios, on-premises.
[Generated with MEHARI-Risk, edited by the author.]

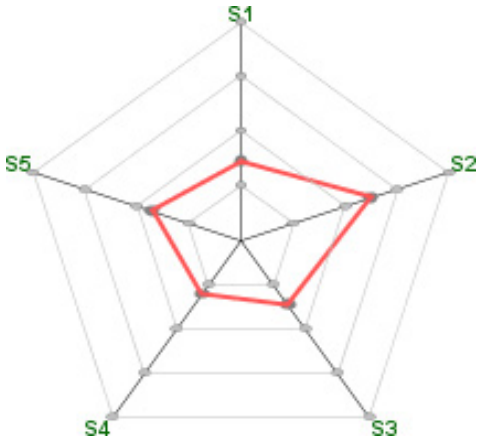

Figure 7. Risk seriousness for selected scenarios, cloud service.
[Generated with MEHARI-Risk, edited by the author.]

Scenario	Scenario description
S1	Loss of data files or documents
S2	Software destruction
S3	**Disclosure of data or information**
S4	**Temporary unavailability of resources**
S5	Diversion of data files

The changed scenarios are with bold. These are the following:

- S3 Disclosure of data or information: this is slightly higher in the case of a cloud-based system. This is because of the lack of auditing possibilities.
- S4 Temporary unavailability of resources: this is slightly lower in the case of a cloud-based system. This is because higher redundancy and resilience of systems.

If the risk analysis software is not prepared for new elements and new threats, the risk manager has to deal with them. For example, the MEHARI-Risk software did not fully contained the hypervisor and other cloud-related elements (just in one question) and failure of separation as a threat, therefore the professional judgement of the expert is required to adapt the answers and interpret the results correctly.

In contrast to the general scope-based case above, let us deal with the company's e-Business solution. In the case of card payments, the e-Business or web shop provider must obey PCI DSS, the data security standard for major payment cards. The standard has well-defined requirements for these cases. During the research, they were also analysed and risk of non-compliance was assessed. The level of full compliance is achieved if all numbers are 3. When there is any number, which is smaller than 3, the full compliance cannot be stated, thus the PCI DSS audit will fail. In the field study, we got different numbers varying from 1 to 3. In

this case, generally we are not allowed to accept the main payment cards. As a result of our risk/compliance level assessment we can state that the security risks of using a cloud service cannot be precisely evaluated from the user's perspective, thus the compliance level cannot be assessed on our own. However, Google Cloud Platform achieved PCI DSS certification in the end of 2014. If we accept a PCI DSS Qualified Security Assessor (QSA) audit, this problem is solved. To be precise, this is an issue of trust. Trust in the depth and thoroughness of the audit and "luck" in sampling. This means that system audits like PCI DSS and ISO 27001 are always based on sampling: not all the procedures, sites, systems, etc. are evaluated. Sampling must be statistical sampling, so it is representative to the whole. According to the European Union Agency for Network and Information Security (ENISA) we shall use third party certifications in this case, which could be used for decreasing the top-level risk "loss of governance". [23]

Consequences

We can conclude that in a business case alignment we can use risk management tools in order to provide input for the business decision, but we should not overestimate its importance or make a decision automatically based on some radar diagrams. As the field study showed us, even on a smaller scope, we had to answer almost two thousand questions and results can only be visualized in a simple way, however the problems are more complex and multi-dimensional. For example, we do not have only two choices like on-premises or a cloud-based system, but we can also differentiate on prices, security options, hybrid solutions and so on. As a matter of fact, the knowledge and experience of a professional cannot be excluded from the security-related decision making (with the usage of this tool and other above mentioned constraints), but it can be effectively supported with risk assessment techniques and tools. Visualization functions help the businessmen to make some problems understandable.

There is another mode of decision support: we can check the probability of compliance. This is not a brand-new thing: Common Criteria (ISO/IEC 15408) does the same with the Evaluation Assurance Level (EAL) logic. Conformance is a yes or no question, but the question is how sure are we about the answer. According to this logic a noncompliance risk assessment based on the requirements of PCI DSS was applied in field study. The requirements were focused on Shared Hosting Providers, which also includes cloud service providers. With those requirements, a rapid assessment was made on this scenario. Because of the deep evaluation required by PCI DSS the conformity cannot be evaluated without privileged access to the system. But as an interim solution we can accept the PCI DSS certification, which was achieved by the cloud service provider a half year before. Of course, this also has a level of uncertainty, but there is no perfect solution in this case.

There are cases when we have no chance to do a thorough examination, which could be precise input to our risk management procedure. We shall use third party certifications in this case, which could be used for decreasing risk.

References

[1] SZÁDECZKY, T.: *Business alignment of information security: Analysing risks of new technologies.* Saarbrücken: AV Akademikerverlag, 2016.

[2] SA-SOARES, F. de, SOARES, D., ARNAUD, J.: Towards a Theory of Information Systems Outsourcing Risk. *Procedia Technology*, 16 (2014), 623–637. DOI: https://doi.org/10.1016/j.protcy.2014.10.011

[3] BORT, J.: *Business Insider.* www.businessinsider.com/synergy-research-amazon-dominates-16-billion-cloud-market-2015-2 (Downloaded: 11 6 2015)

[4] AVRAM, M.: Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, 12 (2014), 529–534. DOI: https://doi.org/10.1016/j.protcy.2013.12.525

[5] SPIVEY, J.: *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives.* Rolling Meadows: ISACA, 2009.

[6] MENSE, A., SCHIEMER, M., CIHLAR, M., WAHL, H., ECKKRAMMER, F., GOLLNER, H.: Security considerations in Cloud Computing: Are Private Clouds to handle different? In. *Las Vegas International Academic Conference.* Las Vegas, 2012.

[7] METALIDOU, E., MARINAGI, C., TRIVELLAS, P., EBERHAGEN, N., SKOURLAS, D., GIANNAKOPOULOSA, G.: The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia – Social and Behavioural Sciences*, 147 (2014), 424–428.

[8] SUICIMEZOV, N., GEORGESCU, M. R.: IT Governance in Cloud. *Procedia Economics and Finance*, 15 (2014), 830–835. DOI: https://doi.org/10.1016/S2212-5671(14)00531-0

[9] BRUNETTE, G. a. M. R.: *Security Guidance for Critical Areas of Focus in Cloud Computing.* Vol. 2. Seattle: Cloud Security Alliance, 2009.

[10] BOSE, R., LUO, X., LIU, Y.: The Roles of Security and Trust: Comparing Cloud Computing and Banking. *Procedia – Social and Behavioral Sciences*, 73 (2013), 30–34.

[11] SZÁDECZKY T.: Pillars of IT Security. In. BALOGH Z. G. (Ed.): *Studia Iuridica Auctoritate Universitatis Pécs Publicata.* Pécs: University of Pécs, 2010.

[12] SZÁDECZKY T.: *Regulated security. The theory and practice of the regulation of information security and the methodology designed to make its application easier.* (in Hungarian). Pécs: University of Pécs, Faculty of Law, 2011.

[13] HABEGGER, B. (Ed.): *International handbook on risk analysis and management. Professional experiences.* Zürich: ETH, 2008.

[14] BÉLYÁCZ I.*: Changing role of risk in value calculation.* (in Hungarian). Budapest: Hungarian Academy of Sciences, 2013.

[15] MEZEY G.: *Decision and risk.* (in Hungarian). Budapest: St. Stephan University, 2009.

[16] EWART, P. J., FORD, J. S., LIN, C-Y.: *Probability for statistical decision making.* Englewood Cliffs: Prentice-Hall, 1974.

[17] BOUCHAUD, J-P., POTTERS, M.: *Theory of financial risk from statistical physics to risk management.* Cambridge: Cambridge University Press, 2000.

[18] NAGY G.: *Need for security.* Budapest: Sociology Research Institute, 1993.

[19] HAELTERMAN, J.: *Introduction to ISO 31000.* Brussels: Grant Thornton, 2010.

[20] STEINBERG, R. M., EVERSON, M. E. A., MARTENS, F. J., NOTTINGHAM, L. E.: *Enterprise Risk Management Integrated Framework Executive Summary.* Jersey City: COSO and AICPA, 2004. www.theiia.org/media/files/virtual-seminars/COSO_ERM_Integrated_Framework.pdf (Downloaded: 11 6 2015)

[21] MUNK S.: Component based IT interoperability solutions, a novel approach. *AARMS*, 13 1 (2014), 31–46.
[22] HAIG ZS., KOVÁCS L.: New way of terrorism: Internet- and cyber-terrorism. *AARMS*, 6 4 (2007), 659–671.
[23] CATTEDDU, D., HOGBEN, G. (Eds.): *Cloud Computing. Benefits, risks and recommendations for information security.* Heraklion: ENISA, 2009.
[24] MELL, P., GRANCE, T.: *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.* Gaithersburg: Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology, 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (Downloaded: 11 6 2015)
[25] *ISO/IEC 27005:2011 Information security risk Management.*
[26] *ISO/Guide 73:2009 Risk management – Vocabulary.*