Business alignment of information security

Nowadays businesses face multiple issues regarding new phenomena like cloud computing, which has a great business driver: with the minimisation 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 the IT service, which 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: information security is also a business requirement. It will help to avoid financial loss, avoid bad reputation or increase trust among clients. The work shows the technical features and the security issues of cloud systems. It gives a global overview of information technology's industrial security standards that are widely used internationally, such as ISO/IEC 27001:2013, PCI DSS and COBIT. It also shows some legal regulation in the field of IT security. In the last part the author is presenting the results of a field research which compares two possible risk analysis methods in the case of cloud computing.

Dr. Tamás Szádeczky graduated in engineering, in security politics and in information systems management. He wrote his PhD thesis about the regulation of IT security. He has been working in the field of information security since 2003 and he is a lecturer of the topic since 2008. He is a CISSP, CISM, CISA, PCI QSA and IRCA ISO 27001 lead auditor.

978-3-639-88484-5

Social Sciences Series

Tamas Szadeczky

Business alignment of information security

Analysing risks of new technologies

AkademikerVerlag

Tamas Szadeczky

Business alignment of information security

Tamas Szadeczky

Business alignment of information security

Analysing risks of new technologies

Social Sciences Series

Impressum / Imprint
Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Bibliographic information published by the Deutsche Nationalbibliothek: The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Coverbild / Cover image: www.ingimage.com

Verlag / Publisher:
AV Akademikerverlag
ist ein Imprint der / is a trademark of
OmniScriptum GmbH & Co. KG
Bahnhofstraße 28, 66111 Saarbrücken, Deutschland / Germany
Email: info@akademikerverlag.de

Herstellung: siehe letzte Seite /
Printed at: see last page
ISBN: 978-3-639-88484-5

Table of Contents

1 Introduction

There was a huge advance in the last seven decades in information technology. From the time the first Turing complete computer was made by Konrad Zuse in 1941 and the building of ENIAC, the first really universal computer in 1946, information security has been continuously part of information technology. (Kopeczi, 1974) In the beginning information security had a small focus, but it has been dynamically widened.

We should remark that computers have been processing sensitive data from their early application, for example ENIAC was used to solve mathematical problems regarding US military operations like the calculation of artillery firing tables. In these days physical security measures were enough to prevent unauthorized access. The general use of computer technology began with the implementation of multi-user mainframe computers from the 1950s mostly by IBM. Due to the fact, that multiple users were accessing the mainframe systems, logical access control measures had to be implemented. Universities were the playgrounds for hackers, who were testing the boundaries of those systems. Soon, interconnecting of standalone computers became a usual solution to increase efficiency and collaborations. According to (Kita, 2003, p. 63) the first point-to-point (P2P) RS-232 serial cable-based connections were inefficient, thus the Advanced Research Projects Agency (ARPA) started the ‘Intergalactic Network’ initiative to use the existing telex telecommunication network for computer communication in 1962. Later the ARPANET network was started by ARPA in 1969 which connected University of California, Los Angeles (UCLA), Stanford Research Institute's Augmentation Research Center, University of California, Santa Barbara (UCSB) and University of Utah's Computer Science Department in the beginning, but later it was broadened and around 1980 its name changed to Internet. Networking technologies has ignited the development of a new branch of information security: network security. Network security deals with phenomena like eavesdropping and man-in-the-middle attacks, and at the same time the importance of cryptographic measures has become more important than in the case of the defence of an unconnected computer. Recently with the usage of mobile or portable computers, notebooks, mobile phones, smartphones and tablets and especially with bring your own device (BYOD) phenomenon the integration and secure connection (e.g. VPN) to protected networks and security of data on the move have become new issues. Cloud computing technologies soothed some problems of reliability and business continuity, while at the same time clouds also generated new issues in outsourcing security, data portability and segregation.

The cyberspace, a whole virtual world, has emerged on the basis of these technologies. Despite of its virtual properties, the real world crimes occur in this virtual world with more or less the same symptoms as in the real life. Criminologists and lawyers can dispute that the perpetration of certain crimes in the virtual world and real world differs or not, but the method of protection and security technology unanimously differs from the real world crime

prevention, because you don't have to set up ACLs or firewall rules in the real life. Information security also absorbs elements from the traditional security areas such as military defence, burglar alarm systems or fire prevention, but it also has new attributes.

New IT technologies are appearing each year. Lot of them are causing new problems and open new vulnerabilities which should be solved by information security. This is in fact a major security professional problem. Information security solutions are always following controls by nature, because there is a natural delay between the implementation of the new technology and the implementation of the effective and adequate security control. One of the main reasons is that at the time of development the developers find out some security issues and implement some security controls against them, but more problems and vulnerabilities are visible afterwards, when the product is at the user's premises and hackers start challenging systems. At this point we have to implement always newer and newer controls to protect systems. This is a never-ending story which needs continuous security update and awareness.

Intensive improvement of technology, high business demands and low time-to-market times inhibit application development industry to enhance security controls with the same speed as functional features, so security of network-based activities did not reach acceptable security level. E.g. improvement and legal application of public key cryptography and strong secret key algorithms gave way to computer users for secure communications, but deficiencies of encrypted transmission protocols appearing continuously.[1] Security of computer hardware elements, computer systems or networks depends on the full hardware- and software architecture and the environment, thus the weakest link determines the security level of the overall system.

In those early decades of IT history the security profession fought for legitimacy of cyber security, and attention of high level management which not really understood 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* in information security. In the private sector, especially in times of economic crisis, cost constraints can be severe and we cannot imagine any compulsory expenditure from which managers don't want to cut off. Management's objective is to invest usually minimal resource on IT security elements, systems and networks. Goals for citizens, shareholders, stakeholders and the government are to establish and maintain adequate information security level. We find every day that the decrease in IT budget implies more decrease in security budgets at companies. Also home computer users often don't install minimum preventions such as free security tools. Obviously this can happen because of many reasons: for example lack of experience, technical knowledge, information, money, or interest. But the most important is that most users don't draw enough attention to this area, despite of the fact that later they might be liable for consequences. By the regulator's point of view, everything can be improved and

[1] See BEAST, Heartbleed, FREAK or similar SSL/TLS attacks

the main goal is to reach 100% perfection in the area. Therefore the field of information security also deals with the general problem of security awareness as detailed in (Szadeczky, 2014).

The aim of this work is 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 has been analysed from theoretic and practical views. A small company which is using cloud services actively let the author to make a field research and do the risk assessments in live environment thus analysing business drivers of information security.

2 The cloud-phenomenon

Nowadays businesses face multiple issues regarding new phenomena like cloud computing. Because of its major impact on businesses nowadays, it will be analysed in this chapter.

The innovation of ICT[2] services runs parallel with the development of computers and networks as detailed in (Szadeczky, 2012). “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.” (de Sá-Soares, et al., 2014, p. 624) The outsourcing of certain services started from 1962 when H. Ross Perot established the company called Electronic Data Systems (EDS), the ancestor of the outsourcing business. The company specialized in performing the IT operational tasks which their clients did not want to perform within their organisation. There were only a few experts available on the US market at that time, so outsourcing solved the problem of lack of personnel, too. The standardisation of office workstations and central software management can be provided in an outsourcing contract. The service supplier can take over the operation of the servers and can even run the services on behalf of the client together with the services of other clients on its own hardware. In such a case the service provider shall guarantee the secure separation of those services. The most important element of an outsourcing contract from technical side is to include a Service level Agreement (SLA), which stipulates all essential terms and conditions: availability ratio, time to repair and recovery, time to respond, penalties, rewards etc. The precise tracking of SLA indicators is required to see the risk of an outsourcing project. (ISACA, 2013, p. 280)

Outsourcing the secondary, supplementary tasks has a great business importance. In Hungary MATÁV, the wired telephone service provider also outsourced its IT operational activity to EDS in the ‘90s and it is still outsourced within the group. According to (Racsko, 2011) management information systems which ensure information for decision-making in an adequate form were used from 1990 in Hungary. Data stores for assisting decision-making were created in 1995 and data mining also started these times. Integrated business management systems appeared at the end of the 1990s. Customer Relationship Management (CRM) systems became widespread in 2000 and these times electronic retail trade (Amazon, e-Bay and web shops) started flourishing. They have the ordered goods delivered by courier services. Social networks like wiw.hu (2002), facebook.com (2004) and twitter.com (2006) appeared.

Outsourcing IT services slowed down and came to a halt in the first decade of the new millennium due to the cheap IT devices and the great number of well-trained IT experts.

[2] Information and Communication Technology

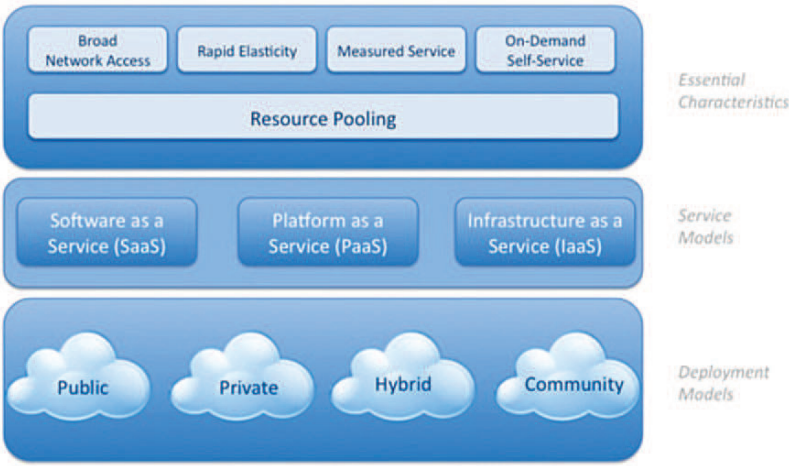
During the past decade a new way of outsourcing emerged. It changed into service optimization and huge multinational IT service providers started to offer their services which can replace most of the in-house IT services operated at the premises of other organisations. That service was provided from a computing cloud. The name comes from the icon used in IT in which a cloud stands for networks whose inner structure is not important, only the input and output has any importance.

As regards to the technical part, the corner stone of the service is virtualization, which has been on the market for a decade but gained real significance and become really widespread only in the recent years. In virtualization one or more virtual systems (guest) are running on one or more physical systems (host). The hardware running the virtual system is a standardised fictive system but obtains its resources from the host system. In a virtualized system the resources of the host system can be allocated among the guest systems anyhow. Virtual systems are supervised by the hypervisor, the surveillance programme. With virtualization, complete systems can be created also with virtual network elements. In this way, for example five servers separated by firewalls may be running on three physical machines while processor time and RAM memory are granted depending on needs. It is hard to know that which physical host is used by a given guest server. It can be determined only with the help of the hypervisor, but it also may run on all the three hosts.

Despite the basics are common, cloud computing differs from virtualization. According to NIST,[3] 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. These features make the difference from classical server-based on-line service provision.

There are four deployment models of cloud computing: public cloud, community cloud, private cloud, and hybrid cloud. Public clouds are the most well-known: these are services open to the public use, no matter if they are free or paying services. A community cloud is run by a smaller group of individuals or companies with restricted access. This is closer to the private cloud. A private cloud is a cloud service of an institution or company for internal use. In this case the above mentioned five essential features shall be also met. As (Mense, et al., 2012) points to that, the security features of a private cloud is highly different: we can achieve much higher security level with that than the public one. However, its CAPEX need is enormously high. So it does not provide the financial features of the public clouds, this is why the majority of the companies decide to use public clouds. Hybrid cloud is a mixture of the other three models. When I use the term ‘cloud’ later on, I think of public cloud services.

[3] National Institute of Standards and Technology



1. Figure: NIST Visual Model of Cloud Computing definition[4]

Cloud services can be classified according to the service model. Each service model is called XaaS – something as a service. The most important are infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). In addition to those three major categories there are other forms, like development as a service (DaaS) used by Salesforce. In the case of IaaS service model, the supplier provides a virtual hardware environment for the client. This includes a virtual system with storage space and network infrastructure operated by the supplier. The operating system and the programs are installed and maintained by the client. In the case of platform as a service, the scope of the supervision of the supplier is broader: it provides the operating system, a database, some applications and development tools in addition to the virtual system. The client installs and supervises applications and uploads data. In the case of SaaS, the supplier provides all elements of the environment, so the client has access to the functionality of the software. The environment is usually accessed with a thin client (web browser). The user uploads data and she is responsible only for them. The user may use certain on-line applications, like word processors, spreadsheets, other office applications and any special software or CRM systems. The service fee may be calculated on the basis of the number of accesses or usage time but in either case the client pays only for the actual use.

Nowadays numerous conventional outsourcing or server-based service provider claims that he is providing a cloud service, despite of that they don't meet the above mentioned minimum requirements as (Avram, 2014, p. 533) emphasizes. This is actually a misrepresentation and a breach of contract.

[4] NIST 800-145

Nowadays more and more public cloud services with broad scope are available. Google offers office applications. Amazon, Rackspace Hosting, Yahoo and Microsoft offer virtual machines, Salesforce provides an application (CRM system) Google and Zoho all of these.
Google provides a SaaS service under the name Google Apps.[5] In Gmail for Business a business email system can be created, for which 25GB disc space, spam filtering and 99.9% availability is provided. It allows using a common company-wide calendar, scheduling events, sharing calendars and synchronizing the contents of such calendars with the calendars of desktop and mobile devices. Google Apps for Work includes document management, text files, spreadsheets and presentations can be uploaded and edited. Company email groups can be created, contents can be shared and archived and all contents can easily be retrieved. Websites can be created with the company's own domain name, secure connections and separate sites can be established thus company intranet can be replaced with this service. Internal video sharing is also possible. The fee of the service is quite reasonable, $ 50 per user per year. It is far cheaper for SMEs than maintaining such infrastructure and services from their own sources. Besides, assistance is available on the phone and via email 24/7. Guaranteed availability means eight hours of service interruption per year. Web based customer service is provided on a self-service basis through an encrypted channel. The filtering of unwanted emails (spams) can be individually customized. Google Cloud Platform is an IaaS and PaaS service including the following elements: Hosting + Compute, App Engine, Compute Engine, Cloud Storage, Cloud Datastore, Cloud SQL, Big Data BigQuery, Cloud Endpoints Service, Translate API and Prediction API.[6]
Another software as a service (SaaS) provider is Salesforce.[7] It offers various applications to businesses, such as software automating sales and managing customer relationship (CRM) and tools performing customer service and support. The use of the software development tool (force.com) starts from $25/user/month and any application using the above services can be developed by this tool, such as data processing, process supporting and business intelligence applications. Its low fee enables smaller organisations to use high level tools for developing their applications. Available applications include for example debt management, human resource management, time management and food ingredient management. A great advantage of this pricing is that development costs can be directly assigned to the different organisational units. In this way it can be counted how much the particular departments spent and how many time units can further be assigned to them.

[5] See. Google Apps for companies. http://www.google.com/intl/hu/enterprise/apps/business/ [16 05 2015]
[6] https://cloud.google.com/ [16 05 2015]
[7] See Salesforce.com http://www.salesforce.com/ [02 04 2015]

The third provider in our example is Amazon, which provides infrastructure under the brand name Amazon Elastic Compute Cloud (EC^2) and not service or platform.[8] This practically means that a virtual machine can be used for a fee which includes a computing capacity, RAM capacity and hard disk store space. This environment can be used with various operating systems and other system level applications, such as databases, application development tools and authentication management. Own virtual guest environments can also be uploaded. Invoicing for the service is based on the resource usage. Computing performance is measured in EC2 compute units. The service can be tried for free for one year with a basic Red Hat or SUSE LINUX or Windows Server package. The price of the services ranges from $0.015 to $16.439 per hour in the European region.[9]

Another well-known provider is Microsoft, which offers an infrastructure or a .NET platform as a service under the brand name Windows Azure.[10] It can run any Windows application on practically any platform. The guaranteed, more correctly the stated, availability is 99.95%. Prices are basically calculated similarly to Amazon. The price in the Western European region ranges from $0.018 to $50.54 with Oracle Database (EE) per hour.[11] On Microsoft's homepage there is a calculator for determining the total cost of ownership (TCO) of the Azure services for a period of three years and it can be compared with the cost of the systems operated on the premises of the business. Not surprisingly, the Azure is the winner in the calculations.

Similarly to public utility services, cloud services are generally cheaper than the systems operated at the particular company even if it actual use entails higher costs for a definite time period. Dynamic resource allocation is always favourable than planning based on prediction. If the prediction is not accurate enough, the resource is simply wasted. The total cost of the service is the sum of the various partial costs. The resource needs are summed up and in this way the otherwise fluctuating tendency of use is levelled up. Due to the huge computing capacity in the cloud, it is better protected against different distributed attacks. Parallel processing can substantially accelerate business intelligence (BI) applications. As the resources are allocated to different premises, the system is more reliable and less vulnerable to natural disasters as opposed to the company's data centre, which is generally located on the premises of the company; the data centres of the cloud are established at optimal places for energy and telecommunication connections.

Gartner, an advisory company acting on the market of IT products and services which is famous for its technical predictions, prepares the expected lifecycle curve of technologies in 2. Figure: Gartner Hype Cycle for Emerging Technologies, 2014. Cloud applications have commanded a great interest since 2009, than they nearly reached the peak in 2010

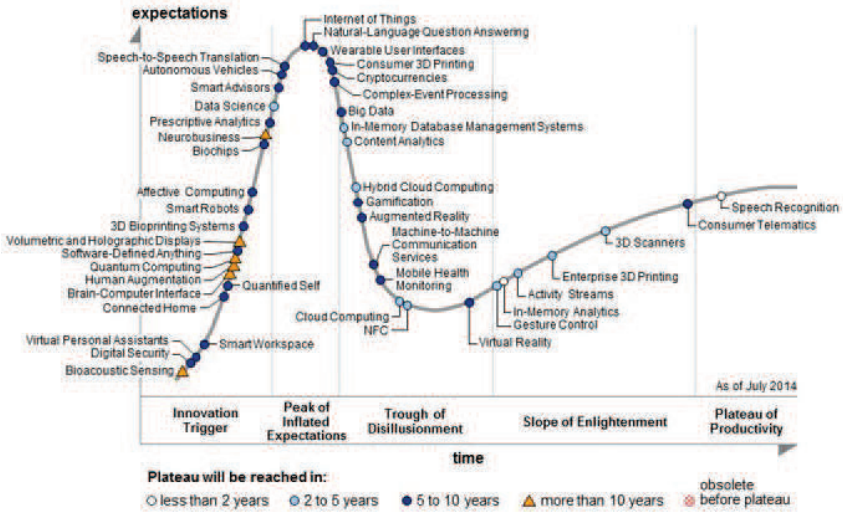
[8] See Amazon Elastic Compute Cloud. http://aws.amazon.com/ec2/ [21 02 2015]

[9] Frankfurt prices at http://aws.amazon.com/ec2/pricing/ [17 05 2015]

[10] See Windows Azure. http://www.windowsazure.com/ [21 02 2015]

[11] http://azure.microsoft.com/hu-hu/pricing/details/virtual-machines [21 02 2015]

and now almost hit the ground in 2015. They are predicted to become fully ripe within two to five years. The next similar area will be the creation of public clouds.[12]



2. Figure: Gartner Hype Cycle for Emerging Technologies, 2014[13]

One of the advantages of cloud services is that in return for a relatively low fee you get a well scalable system which can easily be configured with shared resources and network operation. In respect of cloud services, being bound to a service provider represents the utmost security challenge according to (Catteddu & Hogben, 2009). This means that the systems and applications currently deployed in the cloud are not following standards and do not allow for permeability on the small market. While importing data to the service is easy and supported by the provider, exporting data is extremely irksome and is sometimes deliberately made difficult by providers once the service is cancelled. A further special problem is that in the case of software as a service (SaaS) exporting data does not make any sense, because relations stored in a CRM database in the cloud is difficult to interpret outside this database. This problem will quite likely happen, its impact is moderate and on the whole its risk level is high according to ENISA's report. In such a case when the service provider stops operating, the whole database may be lost.

[12] Gartner blog. http://blogs.gartner.com/hypecyclebook/2010/09/07/2010-emerging-technologies-hype-cycle-is-here/ [21 02 2015]

[13] http://www.gartner.com/newsroom/id/2819918 [21 02 2015]

A further risk is the loss of control over the system operating in the cloud, which may occur due to the uncontrolled allocation of roles, the undetermined system of responsibilities and the inaccessibility of the source code. Its likelihood is regarded to be quite high; its impact quite high in the case of IaaS, but low in the case of SaaS and the resultant risk is high.
The third greatest risk is unsuitability. The suitability of the systems must be certified for the sake of compliance with different legal regulations and standards, but the cloud does not fit them. Its reason is that assuring the possibility of an audit would mean an excessive cost for the provider who is not forced to better cooperate with the client on the seller's market. Its likelihood is regarded to be quite high, its impact quite high and its resultant risk is high.
Operation of cloud services can be really cost effective, big corporations install their computer fleet in the neighbourhood of power plants and transatlantic data cables so that their operating cost can be the fraction of their own server operated on the premises of the corporation. Considering the increased price sensitivity of business entities due to the economic recession, the price of the service is the main factor to be taken into consideration when purchasing. In the case of an in premises service provision, the building, the maintenance of environmental conditions (temperature, humidity), electricity, expert personnel, etc. must be paid for. In the case of a cloud service, it is enough to pay for an IT expert and the service which, in addition, is a well traceable cost element.
Cloud computing was a $17 billion business in 2009 and anticipated to be worth $45 billion in 2013 according to the prediction by IDC (in 2009). However, in contrast to the expectations, it still was only a $17 billion business in 2014 according to (Bort, 2015). The tendency of no change may change when the service will fully develop. Although costs and environmental pollution can be minimized by this solution, it raises security and statutory compliance issues which seems hard to be solved in Europe. Cloud service providers build their computing centres geographically dispersed. Resources between systems are dynamically allocated, no matter where are we using the service or store our data are at the moment. (Spivey, 2009) According to European data protection directive data can be transferred to third countries where data protection level is the same as in Europe, consequently it will exclude most of the premises of the providers. Individual contracts cannot be signed with the providers (in case of small and medium enterprises) and neither do they undertake the requirements concerning availability and compliance which were standard in the case of outsourcing agreements. At present this is a seller's market thus service providers not really care with these needs and concerns, however, as the market gets saturated, they will offer more sophisticated solutions. For instance European personal data may exclusively be managed in cloud servers located in Europe[14] or a new huge European supplier may enter the market just for this reason. Entering the market requires a real fortune, suppliers currently present on the market offer the resources of their systems built formerly for other purposes in the framework of cloud services.

[14] Some service providers are allowing the user to set up restrictions like this.

In addition to cloud service risks, employees' data are threatened by spyware, monitoring traffic and phone tapping. A spyware is an application collecting data on the victim's computer. It may record the activities or stored data on the computer and then send this information to a third party. It can also be used by employers to send a report to the employer for example about the time spent on working on the computer, websites visited or even characters typed and mouse activities. Monitoring network traffic for surveillance purposes can be performed at all network nodes but it typically occurs at the external firewall of the company (protecting the internet connection) or external routers. External network traffic can be monitored and recorded there or even the whole traffic can be eavesdropped. The employer typically records the visited websites and can permit or prohibit access to websites in a whitelist- or blacklist-based manner. If there is no recording only filtering, there are no data protection issues to its implementation, however, in all other cases there is. Activity recording devices which are especially produced for monitoring system administrators in an unchangeable and inaccessible manner are now available on the market. Such systems allow recording the activities of privileged users in an undeletable way. It is an essential issue that who have access to it, delete and modify such recorded data. System administrators are typically authorized to have access to all systems and may modify anything. This must be taken into account when determining rules. Recorded data should be viewed by a panel consisting of the managing director, the human resource manager and the representatives of the employees. Technical (not only legal) measures ensuring lawful access ought to be introduced.

There has been a need of employers for a long time to know the geolocation of employees, but its technical possibility is quite new. Tachygraphy could only record the distance of drive and the speed at the beginning of the '90s, but nowadays real-time monitoring is possible which is mainly ensured by global navigation satellite systems and wireless telecommunication systems. The position of the employee can be collected for the purposes of the protection of life and property (e.g. protected persons, transport of valuables), recording the work performed (e.g. transport of goods) or simply recording working hours (where is the employee during office hours?). The most precise method of monitoring is to place a GPS receiver in one of the devices (typically in the company car) of the employee and it sends the actual position to the data centre through the data connection of the built-in GSM module. A further available possibility which can be ordered at mobile phone companies is to collect the approximate position of the mobile phone from the network data and then send it to the company. This service is typically available to fleet subscribers.

A new technical solution always implies security issues so cloud computing is also no excuse. These issues can be partly solved with usual information security methods, but in some cases new solutions are needed. Elements of the traditional information security according to the CIA triad are Confidentiality, Integrity and Availability. Confidentiality stands for the protection of data, prevention of access of unauthorized persons. It includes access control, physical security controls, cryptography, and transmission security and so

on. Confidentiality issues in cloud systems are similar to those in classic computer systems, but separation is required as a new need. Separation is a control against the access between virtual appliances. It is enforced by the hypervisor or virtual machine monitor (VMM), which is a piece of computer software, firmware or hardware that creates, runs and controls virtual machines. Internal attacks from other virtual systems on the same host can be quite effective. Forensics can be very hard, because the user usually have very few opportunities to log analyse. Integrity deals with protection against malicious or unintentional modification of data stored in virtual storages and sent through communication channels. According to standard information security practice redundancy and error checking are the most common measures of integrity controls. In virtual data storages also concurrent and collaborative access issues became important. Availability is the ability to access data whenever required. Redundant data storage and processing, backup and business continuity management are the standard controls for that. Virtual systems are scalable, flexible and redundant, when they are built according general best practice. But the hypervisor is a new single point of failure, because it is generally not redundant.

Despite of generally good security controls, virtualized systems are not invulnerable. Amazon EC2 Easter outage in 2011 April is an example for cloud failures, when more thousands of websites were unreachable because of a configuration error, which was possibly a human error. According to (Metalidou, et al., 2014, p. 427) human factor is always an issue in information security, therefore awareness should be increased. In February 2013 there was a Windows Azure outage due to SSL certificate expiration. In April 2013 Google suffered an outage because a failure of their sign-in system. There are several special problems which are typical in virtual environments. (Shengmei, 2011, p. 174 – 179) Lock in is a problem of cloud services. When a service is being used, there is no easy way to get out: export of data is much complicated then input. Loss of control is the inability take control of our data: the operator may do anything with that. Compliance is an issue of internationally used services, where the operator must comply with all legal requirements, despite if they can be antagonistic. A change in legal environment can disrupt the business model. Personal data protection is one of the most problematic legal issues, as detailed before. Fail of separation is an error in hypervisor, which let a virtual system to access another virtual system. According to (Suicimezov & Georgescu, 2014, p. 834) cloud systems typically involve Big Data issues during operation. A network management error can disrupt the whole service, because the network connection is a vital part of the cloud service.

According to (Brunette, 2009) answers to those problems are keeping high level of compliance according to Cloud Security Alliance's recommendations. The use of well-known and broadly accepted management standards is favoured. Just like ISO/IEC 27001, as information security management system standard, and ISO/IEC 20000, as the

information technology service management system standard based on ITIL. Management system standards enforce Deming-cycle or PDCA[15] based continuous improvement and process-based approach. Users of those standards must sacrifice time to think on security of provided services, which enhances security and service quality. Application of EU Directive on Personal Data Protection and local data protection laws are required to achieve compliance.[16] From a bottom-up aspect the elements must be secure in order to the whole system to be secure. Today the only internationally accepted standard for IT security product certification is Common Criteria, which is far too complication to be followed in cloud computing cases. Obeying technical standards (RFCs, programming rules) during development can be a good decision also. The audit possibility of clients shows the openness of the cloud service provider and also helps clients who are interested or who must obey strict security rules. Because of the scale, with the concentration of capital a cloud service provider may invest more money on security than a bank. (Bose, et al., 2013, p. 33) But there is no ultimate answer yet for all security issues, total security does not exist.

[15] Plan-Do-Check-Act

[16] See Section 3.5

3 Security requirements

I would like to show the most important regulations which are related to the cloud services in conjunction with the cybersecurity strategy of the Hungarian government.

3.1 Using best practice

If we are about to implement security measures, one choice is to use general best practice. This chapter shows what measures are expectable from a middle sized information-oriented company.

When designing buildings, we must pay attention to architectural (building) security. The aim is to have multiple layers of protection around the building. This needs the implementation of adequate shell and outdoor protection also. As an example the computer room should be located on the ground floor of an inner building, so that even if the attacker breached trough the outer skirt a layer still remains. This also shows the principle of layered security, where we are designing multiple layers around assets thus the intruder must breach all to have access. Possible points of physical entry have to be secured preferably with technical controls (e.g. RFID entry cards) and life force.

Shielding against electromagnetic radiation should also be taken into consideration in special cases. For underground parts of buildings the structure of reinforced concrete in itself can be regarded sufficient. For parts of buildings above ground level the protection against electromagnetic radiation can be implemented by a Faraday cage or shielding of each electronic device. This kind of protection is called EMI or TEMPEST protection.

One of the most important resources of a server room is electrical power, of which the adequate normal and emergency supply must be ensured at several levels. Input power to the facility should be fed from two separate substations. Multiple inputs from public utilities decrease the possibility of blackouts significantly. Continuous power supply should be ensured by applying uninterruptable power supplies (UPS) which can solve short (typically 5-10 minutes) power disruptions. For cases of longer interruptions aggregators (diesel generators) can be installed with the appropriate supply of fuel.

It is important to maintain adequate environment when we run multiple servers or store data for a longer period. The temperature and humidity of the air can be maintained with air conditioners. At the installation redundancy (at least n+1 piece) and possibility to replace should be kept in mind. Air conditioners should be installed in pairs thus it is handful if a neighbouring unit can perform the task of another appliance in the case of a shortfall. Either we save data online or offline (on a data carrier) we also have to deal with the relative humidity of the area.

3. Figure: Water tanks and cooling towers of Google in Belgium[17]

In addition to the fire alarm equipment (typically smoke detectors) usual in buildings, the protection of server rooms should meet stricter requirements in terms of more effective fire-detection, fighting and damage minimization. Aspirating smoke detectors, which sense fire faster and with more certainty, are widely used in these cases. It consists of a network of sampling pipes to draw in air and an analysing appliance (typically a laser-based smoke detector) built in the server room. As this solution is rather costly, optical smoke detectors are still more widespread. Use of an automatic fire extinguishing system is typical, in spite of it is generally not obligatory. Fire is usually extinguished by some inert gas, but there are attempts to use water fog fire extinguishers. In certain cases detection and protection against explosives and chemicals also has to be implemented. We also need protection against natural and artificial waters (pipeline leakage).

Although server rooms and data storages are guarded similarly to other facilities, creating protected sectors and role-based differentiating between authorized accesses have more importance. Typically authentication is centralised and two-factor authentication is used, for example an RFID card and PIN code together. Authorisations are stored in a central unit and given with the joint consent of the direct superior of the given employee and the person in charge of the business process or the operational security manager of the server. User rights allocated in this manner should be reviewed at least annually together with the automatic or manual comparison of authentications and permits. The cause of any derogation should be investigated. Logging entries into the facility can be stored only for a limited period of time because of EU data protection regulations. That is why any illegal entries and authentication rule violations have to be detected and investigated within this period. Data that can be used as evidence can usually be stored longer, until a report is

[17] http://www.google.com/about/datacenters/gallery/#/places/7 [20 02 2015]

made to the police or a disciplinary proceeding has started. When forming security zones, areas used by maintenance and logistics staff should be physically separated from server rooms or office area. Servers should also be placed in different spaces according to the different functional and security aspects. The closed-loop camera (CCTV) surveillance of protected zones, especially passageways and working areas is also necessary. Recordings made here should also be kept for a certain amount of time, according to Hungarian legislation, generally three days. Server rooms should not have windows or doors opening to unprotected spaces, windows are absolutely useless. If they do, the protection of such rooms requires utmost attention by glass break detectors and passive infrared (PIR) sensors installed on the protected side.

Passive infrared motion detection sensors should also be used in the protected area in all cases. There might be air-lock doors for security purposes but for the protection of life there must be an emergency opening mechanism e.g. a door handle from the side of the server room or emergency exit key placed next to the door. Its purpose is to ensure immediate escape in the case of fire or operating of fire extinguisher. A press-button for cancelling the release of extinguishing gas must also be placed inside the protected room for the protection of life, because it might cause choking.

Internal network of the information system should be separated from the Internet, which is implemented by network segregation, typically with hardware-based firewalls. All outside traffic shall flow through firewalls and network traffic encryption protocols (e.g. HTTPS, SFTP, SSH) ought to be applied.[18] Traffic inside the server room may stay unencrypted provided that data leakage from the network and unauthorized access can be effectively prevented. Logging in the servers should be enabled, with restricted access. Both successful and unsuccessful logins to the servers should be logged. In the case of strictly protected systems each activity should be logged, which is considerably problematic. Balabit's Shell Control Box[19] is a straightforward way to trace the activities of system administrators. The security logs should also be well protected. Logs should be gathered in a centralised location (log server) where only the staff of the security department shall have access. Logging activity is essential for the purposes of evidencing and detecting illegal acts. Log files should be saved frequently, for example daily, just like the data itself. These backup files should be stored at a different site, which will not be affected by the same disaster striking the server room. If traffic flows electronically between premises, it should be done in an encrypted form. Sent and received contents should be compared with each other (checksum control). If data exchange is performed physically, the security procedures for transporting valuables should be followed.

[18] Numerous bugs are affecting network traffic encryption nowadays from the Heartbleed-bug to the deficiencies in the iOS AFNetworking so regular update of cryptographic libraries is essential.

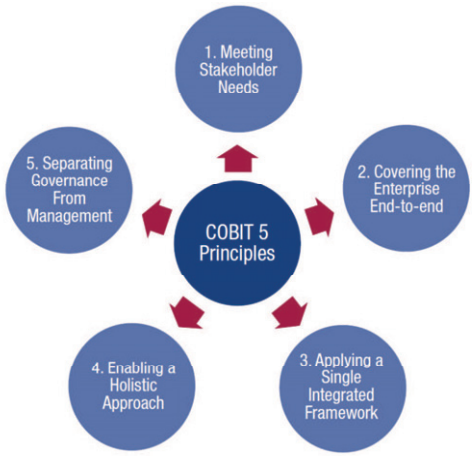
[19] See https://www.balabit.com/network-security/scb

Disaster situations deserve particularly careful attention and planning in the case of important systems in which the infrastructure of the organisation can significantly be damaged or destroyed. The technical documentation of disaster-related planning is called Disaster Recovery Plan (DRP), which contains the technical tasks to do in the case of disaster with the detailed technical description of recovery. This includes the steps of installing and configuring the replacement systems to be used, the method of recovering the data and the provision of the appropriate operating staff. For disaster recovery reasons a spare system, which is identical with the live system, may be kept running continuously (hot site) or switched off (warm site) outside the operational premises. Another solution is to sign a contract with the hardware and software distributor in which he undertakes to provide the appropriate system within a reasonably short time. An often forgotten task is to carry out disaster testing to check the feasibility and usability of the plan. During disaster testing it is useful but risky to shut down the live systems since it can cause shortfalls in the service if plans and measures are not appropriate. A method more frequently used is to do staff practise (desktop review). In this case the steps of the disaster-related plans are drilled. Business Continuity Plan (BCP) is another plan in connection with disasters which approaches the problem from a business aspect. It is about ensuring the continual operation of business processes with alternative (e.g. paper-based) methods.
The procedures and methods described above are best practices of the IT service provision. However they depend very much on the real situation and budgetary issues. For instance in the case of financial institutions the authorities expect the fulfilment of the above mentioned strict security requirements, while legal provisions are not so strict against webhosting service provider or other non-regulated sectors.

3.2 COBIT

ISACA (formerly known as Information Systems Audit and Control Association), an internationally appreciated American IT auditor association, and IT Governance Institute (ITGI) jointly developed the Control Objectives for Information and Related Technology (COBIT) a de facto IT audit and information security standard in 1992 as detailed in (Szadeczky, 2010). COBIT defines rules for information-related processes. COBIT is a generally accepted collection of practices based on business needs. It has never become a de jure international standard and conformance cannot be certified against COBIT. COBIT 5 contains 37 governance and management processes in four domains:

- Evaluate, Direct and Monitor, (EDM)
- Align, Plan and Organise (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)



4. Figure: COBIT 5 Principles[20]

According to COBIT the focus areas of IT governance are as follows (Szadeczky, 2012):

- Strategic alignment focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- Resource management is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.
- Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

COBIT pays attention to the theoretical basics of IT governance, so it analyses the essence, the areas of IT governance, the interference and interrelation between the various requirements from a number of aspects. Although connections to other standards are not included in the COBIT itself, numerous mappings have been made for example

[20] (ISACA, 2012, p. 13)

with ITIL, PMBOK, ISO/IEC 27002, PRINCE2, COSO ERM, NIST FISMA standards and the Sarbanes-Oxley act.
In order to support the application of COBIT 5 ISACA made the following publications available:

- COBIT 5 Implementation
- COBIT 5: Enabling Processes
- COBIT 5: Enabling Information
- COBIT 5 for Information Security
- COBIT 5 for Assurance
- COBIT 5 for Risk
- Process Assessment Model
- Self-Assessment Guide
- Assessor Guide

COBIT is a not certifiable standard, so the compliance check is called assessment and no certification is achievable but an assessment report is given to the assessed organisation. Lack of certification also means that no information is available that how widespread its usage is. The Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM) exams, which are among the most important globally recognised information security examinations also recognised by the United States Department of Defense (DoD)[21], are based on COBIT.

3.3 ISO/IEC 27000 series

A family of information security standards flourished from a single British standard in the last two decades and now the main family members are well-known and used all over the world. BS 7799 was a UK national standard developed in 1995 by the Department of Trade and Industry (DTI). DTI collected information security control requirement best practices applicable at management level. This became an international standard under the name ISO/IEC 17799 in 2000. BS 7799-2 was developed as a standard for information security management system in 1999 and it was related to the former BS 7799, which was renumbered as BS 7799-1. It became an international standard in 2005 under the name ISO/IEC 27001, after which ISO/IEC 17799 was also renumbered to ISO/IEC 27002 and this was the start of the development of ISO 27000 family of standards. Some of its elements are similarly formed as ISO 9000 series management system standards. The ISO 27000 family is under revision nowadays: ISO/IEC 27001:2013 is the new main standard and other updates are also coming in 2015. It is an important feature of the original standard that it specified security requirements arising from business needs in a top-down approach. ISO/IEC 27001 was developed to serve as a model for the

[21] Department of Defense Directive 8570

development, implementation, operation, monitoring, auditing, maintenance and improvement of information security management systems (ISMS).[22] The standard is process-oriented and it applies the Plan-Do-Check-Act (PDCA) model[23] or Deming-cycle and the implemented ISMS can be integrated into an existing quality management (ISO 9001), environmental management (ISO 14001), IT service management (ISO 20000), business continuity management (ISO 22301) or similar systems.

The most important members of the currently 45 element ISO/IEC 27000 standard series published or in preparation[24] are as follows:

- ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27003:2010 Information technology – Security techniques – Information security management system implementation guidance
- ISO/IEC 27004:2009[25] Information technology – Security techniques – Information security management – Measurement
- ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management
- ISO/IEC 27006:2011[26] Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2011 Information technology – Security techniques – Guidelines for auditors on information security controls
- ISO/IEC 27010:2012 Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011:2008 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013:2012 Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014:2013 Information technology – Security techniques – Governance of information security
- ISO/IEC TR 27015:2012 Information security management guidelines for financial services

[22] ISO/IEC 27001:2005 p. 19.

[23] Despite of it is not included in the 2013 version.

[24] NP, WD, CD, DIS, FDIS and standards without publication years shows different levels of preparations. These standards are unpublished yet.

[25] Under update, CD stage

[26] Under update, DIS stage

- ISO/IEC DIS 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC TR 27019:2013 Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO/IEC 27039:2015 Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)
- ISO/IEC 27040:2015 Information technology – Security techniques – Storage security
- ISO 27799:2008[27] Health informatics – Information security management in health using ISO/IEC 27002

The chapters of ISO/IEC 27001:2013 standard are as follows:

0 Introduction

1 Scope

2 Normative references

4 Context of the organization

5 Leadership

6 Planning

7 Support

8 Operation

9 Performance evaluation

10 Improvement

Annex A (normative): Reference control objectives and controls

For the detailed information on control objectives and controls in Annex A of the ISO/IEC 27002 standard should be used.

Considering that compliance with the standard can be certified, it may bring a business advantage to the company. Such a well-known certification logo is shown in 5. Figure. As certification is performed by private companies and there is no mandatory register, it is nearly impossible to specify the exact number of certified companies in the world.

[27] Under update, DIS stage

5. Figure: ISMS certification logo[28]

However, there is an international register where certification bodies can voluntarily have their certificates registered. According to this register, the last known number of ISO 27001 certificates is 7940. The certificates broken down to countries are as follows:[29]

Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian Federation	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1
Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4	**Total**	**7940**

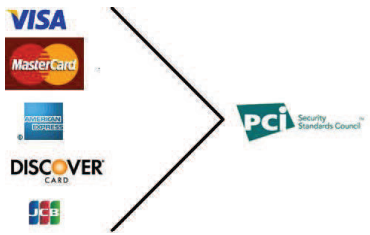
[28] http://www.certipedia.com/logos/000/157/022/9108622669_en.png?1418391023 [30 01 2015]

[29] International Register of ISMS Certificates. http://www.iso27001certificates.com/ [13 11 2012] Version 215 August 2012 (Updates discontinued after this date)

These figures are not reliable but can be regarded as partly correct, because lot of certification bodies did not reported to this database due to sensitivity.[30] The number of certificates issued does not mirror the number of organizations certified. One organization may obtain several certificates because of the validity of scope wording or included sites.
Due to the fact that this standard is used globally and it is certifiable according to internationally accepted rules, it is particularly suitable for compliance purposes. In case an inspected organization has an ISO/IEC 27001 certificate covering the scope of the inspection, there is no need to examine again whether these requirements have been met or not.

3.4 PCI DSS

In order to increase bank card payment security VISA, MasterCard, American Express, Discover and JCB has founded Payment Card Industry Security Standards Council (PCI SSC) on 15th December 2004.



6. Figure: Founders of PCI[31]

The council formed more de-facto security standards, which are required in certain cases from the merchants[32] by the above mentioned card issuers. The actual set of the standards is the following:

- Payment Card Industry Data Security Standard (PCI DSS) Version 3.1 April 2015
- Payment Card Industry Payment Application Data Security Standard (PA-DSS) Version 3.0 November 2013
- Payment Card Industry Point-to-Point Encryption (P2PE) Solution Requirements and Testing Procedures: Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware) Version 1.1.1 July 2013

[30] Number of active clients can be regarded as business secret.
[31] http://wiki.cas.mcmaster.ca/index.php/File:PCICouncil.JPG [2015.05.05.]
[32] Merchants are points where card payment is accepted, e.g. shops, webshops

- Payment Card Industry PIN Security Requirements (PTS) Version 2.0 December 2014
- Payment Card Industry Card Production Logical Security Requirements Version 1.1 March 2015

The flagship among them is the first one, the PCI DSS. As a proprietary de facto standard it defines technical security measures against typical shortcomings in IT systems. In contrast to ISO/IEC 27001, requirements of PCI DSS are much deeper and testing procedures are also provided.
The conformance to this standard can be certified. The audits are conducted by PCI Qualified Security Assessors (QSA) who are employed by PCI QSA Companies. During the audit the assessor is checking the Requirements via the Testing Procedures included in the standard.

3.5 Data protection

Data protection is a set of legal rules for processing of personal data[33] also including information security requirements. But as it is well analysed in (Szadeczky, 2010) and (Szadeczky, 2011) these are superficial regulations, giving just hints on technical issues. Generally all entities managing and processing personal data, except private users for self-usage are falling under data protection laws. In the European Union the Data Protection Directive (95/46/EC) is giving a framework to the national legislation. In Hungary the first data protection act was Act LXIII of 1992 on the protection of personal data and the disclosure of information of public interest, which was adapted to the EU directive in 2004. Now the Act CXII of 2011 on informational self-determination and freedom of information is in force. The security requirements were changed minimally. The law says that "Data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing."[34] As analysed by (Jori, 2005, p. 258) in his handbook we can say that data or information security is included in the scope of data protection regulation. According to the next subsection 'Data must be protected by means of suitable measures against unauthorized

[33] In the USA it is referenced as personally identifiable information (PII). Common law also uses the expression 'privacy', but is has a broader meaning than personal data, it also includes private sphere and the data subject's body.

[34] Hungarian Act CXII of 2011 on informational self-determination and freedom of information Section 7 (2)

access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.'[35] The legislator is giving examples of threats which in general correspond to information security best practices. As it is emphasized in this work, it is important to do a risk analysis about risks threatening the personal data. The risk management is not directly included in the act. The law is not detailed and there are no controls built into it. According to (Reidenberg, 1998, p. 584) requirements are generally superficial in data protection acts. Its main reason is technology-independence, but this superficiality makes more difficult the application of law.

Medical data processing might be more risky than client data processing. Prevention of misuse of medical personal data has higher interest worldwide US HIPAA[36], ISO 27799 and ISO 22857 are good examples of that as (Kokolakis & Lambrinoudakis, 2005, p. 49) shows it. In Hungary there is also a designated act on healthcare data protection, but is performing inefficiently as (Alexin, 2010, p. 104) proves. In (Trocsanyi, 2007) the reader can find case law of the Commissioner for Data Protection on the topic.

According to (Balogh, et al., 2002, p. 325) data protection measures may be checked with a data protection audit internally or externally according to Roßnagel's German model. According to (DeJarnette & Morin, 2010) there is also a need for data protection audit in the USA, in spite of there is no federal data protection regulation there.

3.6 Cybersecurity legislation in Hungary

Development of information technology made local system security improvements necessary. In case of e-government systems a higher level of problem also exists: attack against multiple systems or against the full critical information infrastructure. This can be done during a conventional war, which we can call cyberwar, or may be an unconventional attack called cyberterrorism.
Cyberterrorism is a quite debated term. Multiple scientific papers analyse this topic, so we should take an important note on the issue. According to (Gorge, 2007, p. 9) the word cyberterrorism should be interpreted by its syllables, where cyberspace is the mass of computer communication networks, primarily based on the Internet. The term was created by William Gibson and was first used in science fiction novel Neuromancer which was

[35] Hungarian Act CXII of 2011 on informational self-determination and freedom of information Section 7 (2)
[36] Health Insurance Portability and Accountability Act

written in 1984. It was a term for the collective hallucination by billions of people. In the beginning of computer networking the concept of 'network' has had only a technical meaning. The term cyberspace emphasizes the close relationship between interconnected networks, relationships (interdependency) between humans and networks and social networks based on IT networking and services. According to (Netanjahu, 1995, p. 20) "Terrorism is the deliberate and systematic murder, maiming, and menacing of the innocent to inspire fear for political ends." According to the U.S. Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." (Tiefenbrun, 2002, p. 371)

We have to notice that a cyber-terrorist does the same or very similar technical steps as an "ordinary" online criminal does. Differences are only in the impact of the attack and the invested effort. Thus we have to defend all individual systems in order to protect the entire infrastructure. (Szadeczky, 2014, p. 111)

From the government's viewpoint generally the local and national defence systems have to be planned and prepared against such actions.

The first comprehensive security and defence policy system in Hungary after the political change in 1989 did not recognised cyber threats. Neither the security- and defence policy principles of Republic of Hungary,[37] nor the National Security Strategy of Republic of Hungary,[38] nor the National Military Strategy of Republic of Hungary[39] included cyber defence as an objective. According to these policies and strategies the defence against cyber-attacks are treated individually, even in the legal regulation.

We have to say that a relatively low awareness is observable in usage of international IT security standards even from the legislator and the business. This happens in spite of its significance and the high risk in some areas. No obligation can be found in Hungarian acts for enforcement of standards in IT security. There are self-control procedures in some acts, but their efficiency is questionable in practice.

A small change had commenced in 2009 with the adoption of act on electronic public services.[40] It has highlighted security as a basic principle and requirement. There were four government decrees, which detailed requirements, but they were not really helpful because of less details and lack of audit.

In 2009 there was a proposal on information security, but it never came to force. However it had a remarkable impact on the area.[41] The bill was a draft legislation framework, a so

[37] National Assembly resolution no. 94/1998 (XII. 29.)

[38] Government resolution no. 2073/2004. (IV. 15.)

[39] Government resolution no. 1009/2009. (I. 30.)

[40] Act LX of 2009

[41] MeH, Draft of act on information security, 2009.

called lex specialis. The bill's scope was all IT systems and services in Hungary, including private computers. It was applied to the service providers, operators and users, also. The requirements were broken to five security levels and there was a mandatory audit at levels four and five. The social impact of the law would have been significant, mostly because of its wide scope. It was never accepted probably because if this.

The current National Security Strategy[42] requires the strengthening of the security of electronic information systems to enhance the protection of critical information infrastructure (CII), and the development of adequate cyber defence measures. According to this statement, the Hungarian Government adopted the National Cyber Security Strategy of Hungary as well.[43] The legislator realised that recently experienced cyber wars and cyber terrorist attacks worldwide justify the acceptance of a modern Hungarian Information Security Act and on 25th April 2013. The publication of Act L of 2013 on electronic security of state and local government organizations was a huge milestone for the administrative control of information.

According to (Muha & Krasznay, 2013) the scope of the act, despite of its title and scope definition in Section 2, is significantly wider as it sounds. It is because of the following entities in the personal scope: data processors of national data assets, national and European critical infrastructure system elements. These elements significantly extend the scope also with private companies, so typically public utility providers, electronic communications services, financial organizations are included. The law requires confidentiality, integrity and availability, known as CIA triad in information security field[44], as essential information security requirements in electronic information systems and data.

The Act prescribes integrity and availability of information systems in a closed, complete, consistent way, proportionate to the risks (aligned with risk assessment) for the electronic system and components. It is important to explicitly include the security control implementation's proportionality to risks and usage of risk assessment in the governmental information security requirements, because security controls are typically implemented in an ad hoc manner, to minimize security budgets.

In order to protect electronic information systems and data, in proportion to the risks, the Act states that the electronic information systems must be classified according security risks. This classification is based on confidentiality, integrity and availability properties in a scale of 1 to 5 where 1 is the lowest security level without protection required. From this section of the act it seems that each part of CIA factors (confidentiality, integrity and availability) has to be evaluated separately, but in other parts of the IT security act we don't find this distinction.

[42] Government Decision no. 1035/2012 (II.21.)

[43] Hungarian Government decision no. 1139/2013. (III.21.)

[44] Hungarian Act L of 2013 on Electronic Security of State and Local Government Bodies

The security classification depends primarily on the security classification of information controlled, this act, in contrast to the earlier proposal, does not specify what minimal security controls shall be applied to data. Although it determines the minimum security level classification for designated organizations. This probably will have the typical consequence that the security needs of data will be just on the end of the list, but the minimum-list will be used as an aim for data processors. Public sector organisations try to invest the smallest amount possible in security. According to the act the manager of the organization may set a lower security class in *exceptional circumstances* which is, according to (Muha, 2013) another easy way to avoid spending on security. The only thing that can stop this expected downward bidding is the strict decisions of the National Electronic Information Security Authority,[45] what will be in charge of oversight.
The minimum grades in the Act per organizations are the following:[46]

- Level 1: empty, there are no requirements at this level
- Level 2: Office of the President, Office of the National Assembly, the Constitutional Court 's Office, Office of the Commissioner for Fundamental Rights, local and national self-governmental bodies, the administrative authority associations
- Level 3: central state administration bodies, the National Judicial Office, courts, prosecutors' offices, the State Audit Office, National Bank of Hungary, the capital city and county government offices
- Level 4: Hungarian Defence Forces
- Level 5: data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law

As it was mentioned earlier the act does not define what these security levels are, or how should the classification be conducted exactly and what are the detailed rules for the level. A decree is provided to do that.[47]
The manager of the organization have to appoint a person in charge of the electronic information system security,[48] who is responsible for tasks related to the protection of electronic information systems. Her tasks include responsibilities of a conventional chief information security officer (CISO).
The Act set up the National Electronic Information Security Authority[49] under the Ministry of National Development, now it us under the Ministry of Interior. As a specialized authority, National Security Authority in involved in their activities with forensic log analysis and vulnerability testing in case those are required. The existing Government Computer Emergency Response Team (GovCERT) responsibilities were handed over to Special

[45] formed by Act L of 2013 Section 14 Para 1
[46] Act L of 2013 Section 9 Para 2
[47] 77/2013. (XII. 19.) NFM decree
[48] Act L of 2013 Section 11 Para 1 (c)
[49] see http://www.neih.gov.hu/?q=en

Service for National Security. According to Section 23 the National University of Public Service is developing and overseeing trainings for those responsible for the security of electronic information systems and staff organizations.

There is a trend of more definite legal regulation, even with inception of technical standards in legal regulations. Due to the wide range of important legislation and emerging social effects, improvement of information security awareness is expected. Probably the standard-based (e.g. ISO 27001 or COBIT) systems will also spread, given the fact that the organizations will already comply with the security rules. This change in strategy and regulations will result in greater security and the national security risk will decrease in the area of information and communication technologies in the long term. The new act is a good step in the direction of the appropriate level of government information security, but it still provides loopholes from the application of the rules.

4 Risk management

As shown above, risk management became a basic element of security standards and security-related legislation. According to (Zhiwei & Zhongyuan, 2012, p. 1293) it is also becoming a main tool for the business alignment of security-related decision support is risk analysis, which is also forced in the international standards. In this section I analyse some risk management theories and practices.

4.1 Risk management theory

The risk-based thinking, which is lying on mathematical rules, came into existence by the work of Blaise Pascal in the 17th century. Despite of it roughly means uncertainty,[50] according to (Habegger, 2008, p. 19), it is a key element in all political and economic activity. 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 (Mezey, 2009, p. 10). 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 makes doubt, but this doubt may be reduced. (Ewart, et al., 1974, p. 1)

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. (Bouchaud & Potters, 2000, p. 158)

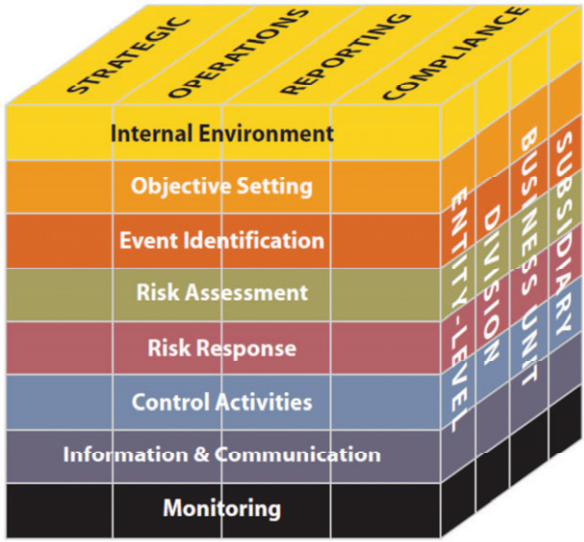
In the 1980s the professional thinking on the coordination of previously unconnected risks started by the Fortune magazine's article "The Risk Management Revolution".

As analysed in regard of 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 the 1980 risk was generally R=I*P where I is the impact and P is the possibility, but this became more sophisticated nowadays. (Nagy, 1993, p. 19)

The first governance tool capable for general risk management was the COSO51 Enterprise Risk Management (ERM) framework. (Haelterman, 2010, p. 3)

[50] There is still a debate if risk is equal to uncertainty according to (Belyacz, 2013, p. 13)

[51] The Committee of Sponsoring Organizations of the Treadway Commission



7. Figure: Components of Enterprise Risk Management[52]

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 7. Figure. Despite of this is a general framework, it is frequently thought that it is only for banking, financial or back-office process-related use cases.[53] Also its complexity may be frightening for the potential user. (Haelterman, 2010, p. 6)

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

[52] (Steinberg, 2004, p. 11)

[53] This can happen because the founders are financial accounting-related companies

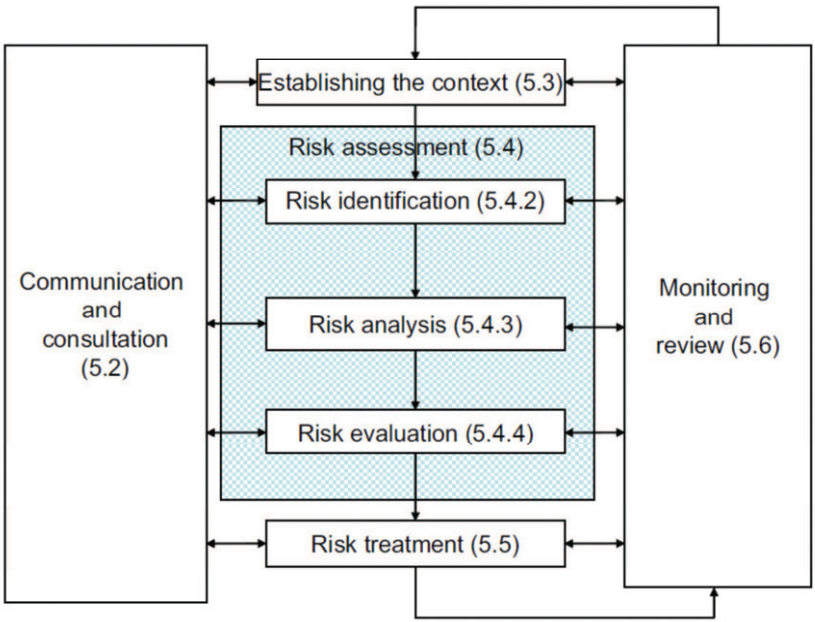
General risk management ISO and IEC standards:

- 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

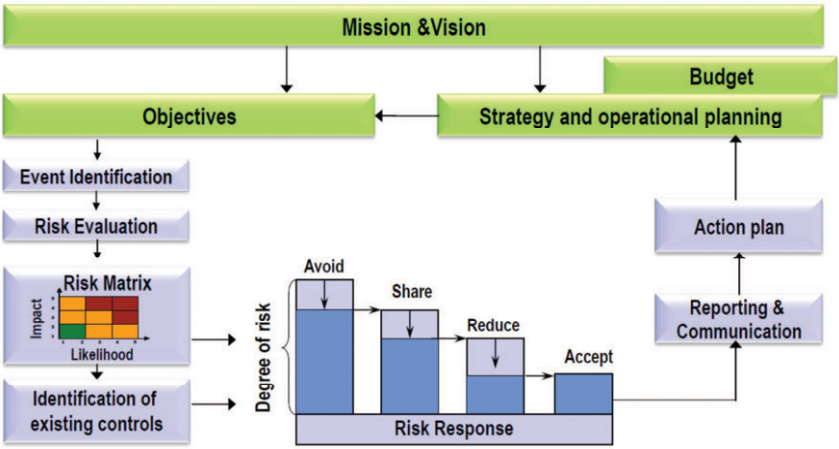
The most important general risk management standard is ISO 31000:2009 Risk management – Principles and guidelines. This became the gold standard of the general risk management, in spite of its main components are also present in other standards.



8. Figure: Risk management process[54]

One of its main elements is the risk management process, which is shown in Fig. 8, is very similarly present in ISO/IEC 27005:2011 Fig. 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 (2.1)"[55]
In spite of it is not a brand new thing, it is very useful for standardising the process itself.

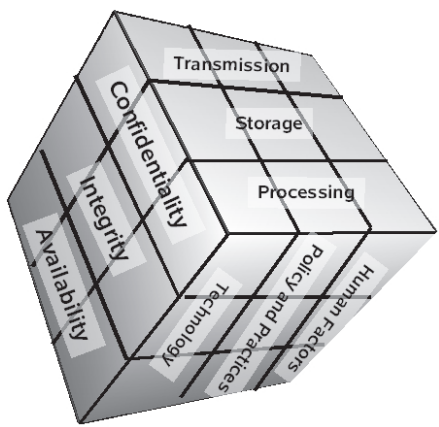
[54] ISO 31000:2009 Fig. 3
[55] ISO Guide 73:2009, definition 3.1



9. Figure: Establishing a risk management process[56]

The establishment of such a risk management project is presented in 9. Figure.

Another risk management model is the McCumber Cube shown in 10. Figure.



10. Figure: McCumber Cube[57]

[56] (Haelterman, 2010, p. 15)

[57] Source: http://upload.wikimedia.org/wikipedia/en/5/50/Mccumber.jpg [2015.01.10.]

This has a narrower scope then COSO ERM: it's just an information security risk management model made by John McCumber, which considers the interconnections of different factors of information assurance. (McCumber, 2004, p. 99)
Data protection as analysed in 3.5 has also a risk management principle (rather than a methodology), which is not really detailed. It is called privacy impact assessment (PIA), which is a process for the assessment of the impact of a certain technology, policy, product, service, etc. on the privacy of individuals (Wright & De Hert, 2012, p. 5). I say principle, because in the context of a technical writing it is actually under defined and no real toolset exists for conducting a PIA. I the new EU General Data Protection Regulation a similar, but in scope tighter, principle is introduced, called Data Protection Impact Assessment (DPIA).

4.2 Risk management practice

Despite of the above mentioned risk management standards and frameworks seem to be well detailed, in fact nobody can do any risk assessment just according to that. We need a methodology fist to help in the implementation of the framework.
One option is the CCTA Risk Analysis and Management Method, abbreviated as CRAMM. It was developed by UK's Central Computer and Telecommunications Agency (CCTA), now Office of Government Commerce (similarly to ITIL).

There are numerous risk management and risk analysis methods. Some examples are the following:

- Cramm
- Dutch A&K Analysis
- Ebios
- ISAMM
- ISF Methods
- Magerit
- Marion
- Mehari
- MIGRA
- Octave
- RiskSafe Assessment
- SP800-30

As an example I introduce the MEHARI[58] method here, developed by CLUSIF[59]. MEHARI's actual version is 2010. It is a qualitative[60] 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:

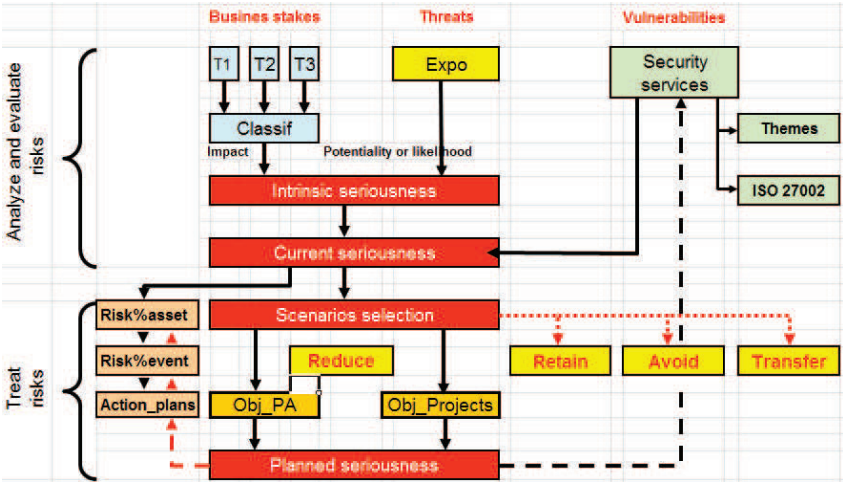
- Risk assessment: display of critical risks see Fig. 13
- Risk treatment: treatments options can be selected from reduce, accept, transfer and avoid.
- Risk acceptance can be done on an individual basis
- Risk communication: stakeholder assignment can be done since the start of analysis. The questionnaire 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.

[58] Méthode harmonisée d'analyse des risques

[59] Club de la Sécurité de l'Information Français http://www.clusif.asso.fr/

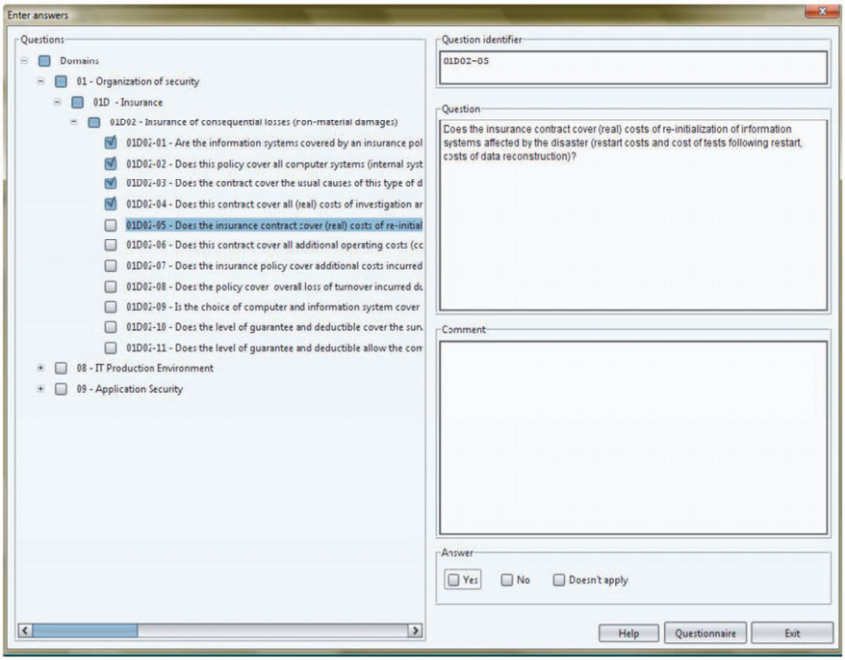
[60] using scales in contrast to quantitative methods, where precise numbers are calculated like probability for a certain threat is p=0.078



11. Figure: Navigation in the knowledge base[61]

For the MEHARI method there is Polish tool, called MEHARI-Risk, developed by 4GI Sp. z o. o. This is also based on the excel sheets, but makes the interviews, answering and reporting easier. The screenshot of the questionnaire is shown on 12. Figure: Answering questions in MEHARI-Risk.

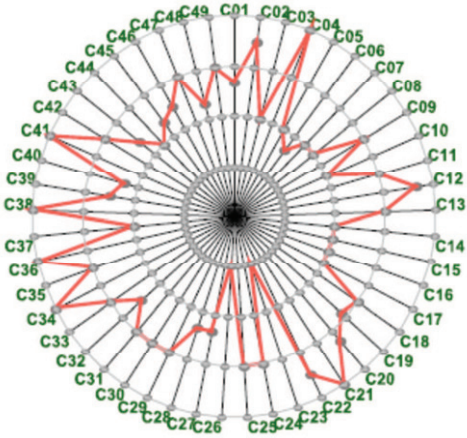
[61] Screenshot from (CLUSIF, 2010) Mehari 2010 knowledge base release 2-2



12. Figure: Answering questions in MEHARI-Risk[62]

To be honest, the reporting to senior management is a vital part of risk management. If the risk manager is just showing an overcomplicated excel sheet to the board of directors, no one will be really convinced about the findings. Visualisation make much easier to digest the findings. MEHARI-Risk has a visualisation capability with radar diagrams. Below you can find the radar diagrams from a report and their descriptions. All those descriptions are included in (CLUSIF, 2010).

[62] (4GI Ltd., 2011, p. 17)

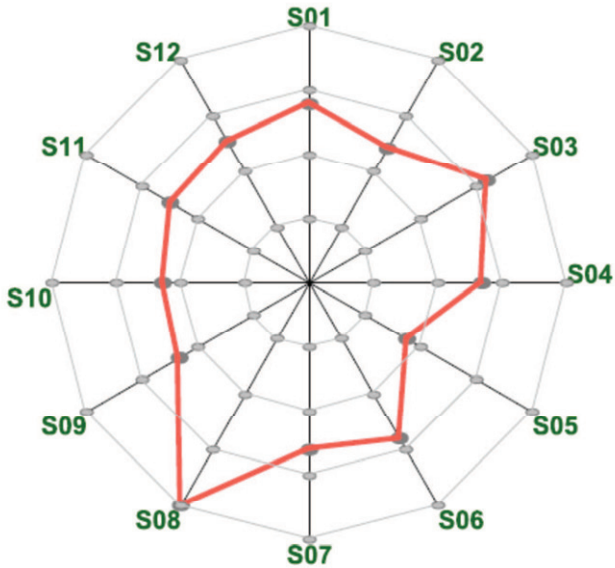


13. Figure: Risk seriousness for selected causes[63]

Cause	Cause description
C01	Intentional modification of the expected functions of an application
C02	Theft of written or printed documents
C03	Manipulation of data files
C04	Accidental crash of a disk drive
C05	Erasure or destruction of user software configurations
C06	Loss of documents by accident
C07	Intentional change of media
C08	Violation of intellectual property rights
C09	Hardware change
C10	Deliberate erasure of data media
C11	Accidental erasure of software
C12	Data capture error
C13	Remote attack of a third organization or competitor
C14	Files erased by a logical bomb
C15	Access and copy of business application data
C16	Accident during data processing
C17	Accidental loss of files

[63] Copied from the report generated by MEHARI-Risk software 1.14

Cause	Cause description
C18	Theft of media containing application business data
C19	Diversion of program source code
C20	Transaction replay
C21	Fire
C22	Access to file servers and copy of office related files
C23	Maintenance unavailable
C24	Alteration of message
C25	Absence of personnel
C26	Access and consultation of system data
C27	Data erased by a logical bomb
C28	Configuration or program code erasure
C29	Vandalism from inside
C30	Malevolent alteration of software functions by a logical bomb or a back door
C31	Transient information pick up
C32	Data fiddling during transmission
C33	Intentional or accidental modification of the expected functions of an office application
C34	Vandalism from outside
C35	Theft or erasure of removable media
C36	Media erased by virus
C37	Faulty data capture
C38	Diversion of temporary information created by the systems
C39	Accident or failure of one or several hardware resources
C40	Flooding
C41	Deliberate erasure of media
C42	Software change
C43	Natural or accidental Disaster
C44	Diversion of information during transmission
C45	Software bug
C46	Excessive use of computing or networking resources
C47	Malevolent excessive use of computing or networking resources



14. Figure: Risk seriousness for selected scenarios[64]

Scenario	Scenario description
S01	Data fiddling
S02	Loss of data files or documents
S03	Software destruction
S04	Disclosure of data or information
S05	Alteration of data
S06	Alteration of software
S07	Degradation of performances
S08	Non-conformance to legal or regulation requirements
S09	Disaster affecting data globally
S10	Temporary unavailability of resources
S11	Diversion of data files
S12	Destruction of equipment

[64] Copied from the report generated by MEHARI-Risk software 1.14

Using tools based on methodologies help to increase the efficiency of the risk management process. Despite of methodologies are freely acceptable, tools can be enormously expensive.

5 Field study on business alignment

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. They also have an e-Business service, which is developed and run by them, also in the cloud.

5.1 General scope

Fist we state a general research question: “Does the usage of cloud services fit the risk appetite of the company?”
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 a narrow one as described below.

Included function:

- SwDevelFunction: the main business function of the company

Inputs:

- InputResources: Inputs of SwDevelFunction

Outputs:

- OutputResources: outputs of SwDevelFunction

Buildings:

- ServiceLocation: In the on-premises case the main address, in the cloud case a Google server farm

Hardware:

- Servers: In the on-premises case some blades in a rack, in the cloud case virtual appliances or host machines (depends on the question)

Network:

- ServiceNetwork: the network connecting the servers and the users

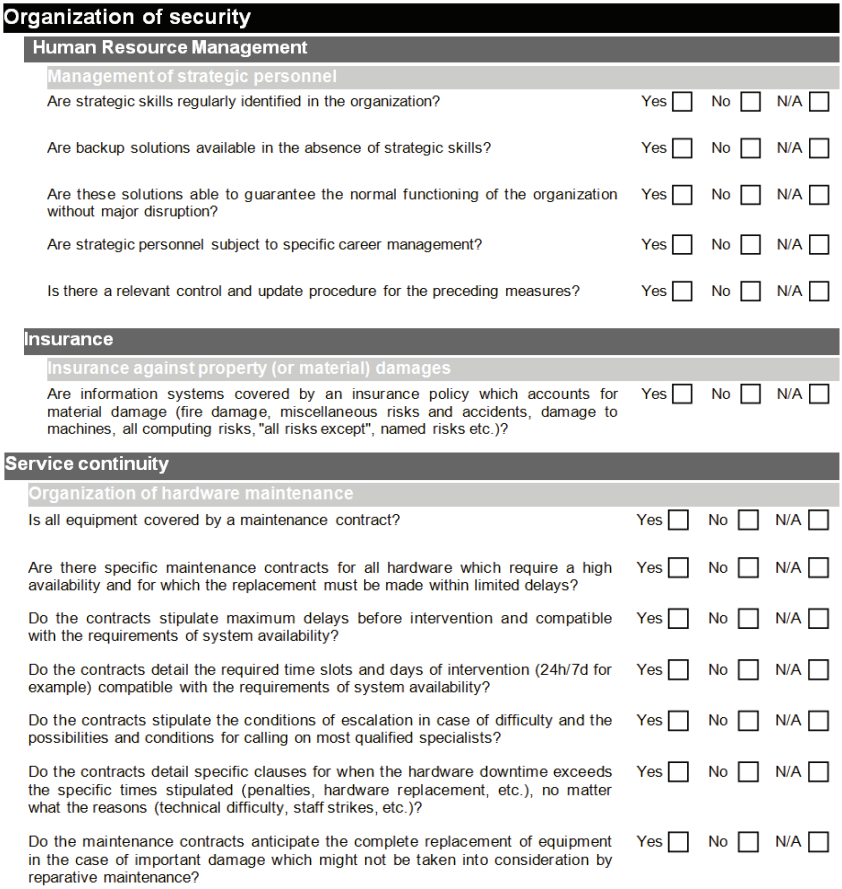
Media:

- NetworkStorage: In the on-premises case RAID SAN in a rack, in the cloud case virtual storage or physical hard drives (depends on the question)

Software:

- SwServices: In the on-premises case internal services (change management, development support, intranet), in the cloud case internal and public services

After setting up of the scope and primary classification, a questionnaire is generated, which is 58 pages long (just because we selected a small scope), so approximately 930 individual questions were answered two times, because the on-premises and the cloud-based were two different assessments. 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. Some sample questions are included in 15. Figure.



Organization of security

Human Resource Management

Management of strategic personnel

Are strategic skills regularly identified in the organization?	Yes ☐	No ☐	N/A ☐
Are backup solutions available in the absence of strategic skills?	Yes ☐	No ☐	N/A ☐
Are these solutions able to guarantee the normal functioning of the organization without major disruption?	Yes ☐	No ☐	N/A ☐
Are strategic personnel subject to specific career management?	Yes ☐	No ☐	N/A ☐
Is there a relevant control and update procedure for the preceding measures?	Yes ☐	No ☐	N/A ☐

Insurance

Insurance against property (or material) damages

Are information systems covered by an insurance policy which accounts for material damage (fire damage, miscellaneous risks and accidents, damage to machines, all computing risks, "all risks except", named risks etc.)?	Yes ☐	No ☐	N/A ☐

Service continuity

Organization of hardware maintenance

Is all equipment covered by a maintenance contract?	Yes ☐	No ☐	N/A ☐
Are there specific maintenance contracts for all hardware which require a high availability and for which the replacement must be made within limited delays?	Yes ☐	No ☐	N/A ☐
Do the contracts stipulate maximum delays before intervention and compatible with the requirements of system availability?	Yes ☐	No ☐	N/A ☐
Do the contracts detail the required time slots and days of intervention (24h/7d for example) compatible with the requirements of system availability?	Yes ☐	No ☐	N/A ☐
Do the contracts stipulate the conditions of escalation in case of difficulty and the possibilities and conditions for calling on most qualified specialists?	Yes ☐	No ☐	N/A ☐
Do the contracts detail specific clauses for when the hardware downtime exceeds the specific times stipulated (penalties, hardware replacement, etc.), no matter what the reasons (technical difficulty, staff strikes, etc.)?	Yes ☐	No ☐	N/A ☐
Do the maintenance contracts anticipate the complete replacement of equipment in the case of important damage which might not be taken into consideration by reparative maintenance?	Yes ☐	No ☐	N/A ☐

15. Figure: Example questions

As soon as all the questions were answered, MEHARI-Risk generates a 25 pages long report. The report includes calculations as defined in the MEHARI method with the risk

reduction factors as seen in the table below. The most of the report is not intended for management use, because the calculations are raw tables, so it hard to understand without the knowledge of the method itself.

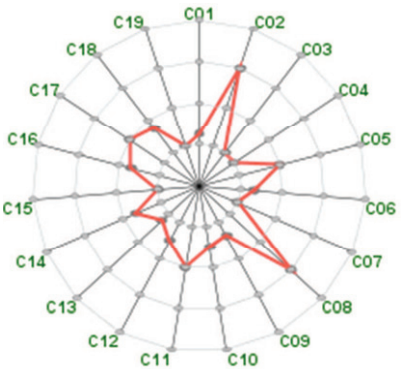
Factor	Description
SERIOUSNESS	Risk seriousness for specific scenario
STATUS-DISS	Effectiveness of dissuasive measures
STATUS-EXPO	Natural exposure
STATUS-I	Impact - depends on maximum consequences and impact reduction factors
STATUS-P	Potentiality of event described by risk scenario - depends on natural exposure and effectiveness of measures
STATUS-PALL	Effectiveness of palliative measures
STATUS-PREV	Effectiveness of preventive measures
STATUS-PROT	Effectiveness of protective measures
STATUS-RECUP	Effectiveness of recuperative measures
STATUS-RI	Impact reduction calculated from PROT, PALL, RECO

Internal audit results: risk reduction factors and risk seriousness

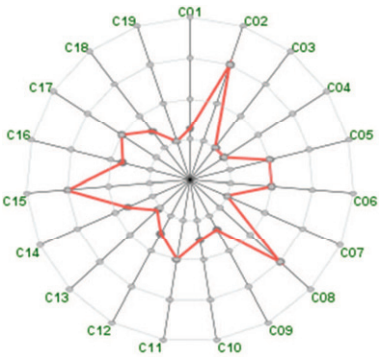
	Disclosure of data or information			
	Access and consultation of system data			Diversion of information during transmission
	On line access to business information, by a hacker using a port left open to the internal network	On line access to business information, by a person authorized within the premises and gaining access to the local network (using a LAN plug in a meeting room, etc.)	On line access to business information, by a staff member, though unfaithful	Diversion of faxes, by phone extension transfer initiated by a staff member
SERIOUSNESS	2	2	2	1
STATUS-DISS	1	1	1	1
STATUS-EXPO	3	3	3	3
STATUS-I	2	2	2	1
STATUS-P	2	2	3	3
STATUS-PALL	1	1	1	1
STATUS-PREV	3	3	2	1
STATUS-PROT	4	4	4	1
STATUS-RECUP	1	1	1	1
STATUS-RI	3	3	3	1

16. Figure: Example calculations

At the end of the report we find two radar diagrams, which show the findings. In 17. Figure and 18. Figure I show the 'Risk seriousness for selected causes' radar diagrams for the on-premises and the cloud-based services next to each other. Description below the diagrams is the same for both. In the table the bold rows shows the differences.



17. Figure: Risk seriousness for selected causes, on-premises



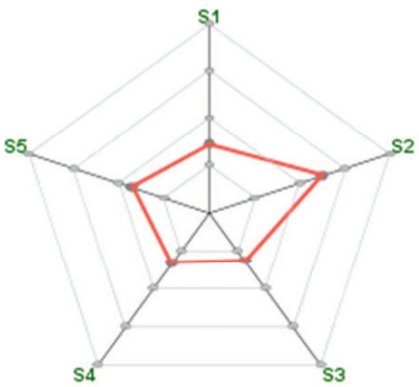
18. Figure: Risk seriousness for selected causes, cloud service

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

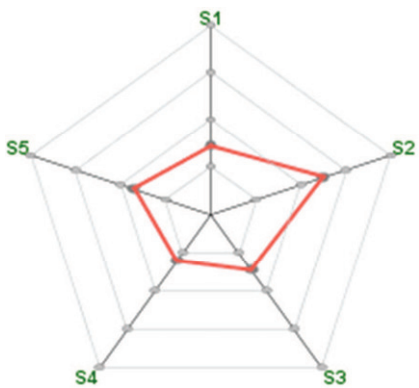
We see that there are three changes:

- 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 logging and 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 don't 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.

In the next diagram, 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.



19. Figure: Risk seriousness for selected scenarios, on-premises



20. Figure: Risk seriousness for selected scenarios, cloud service

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

The changed scenarios are again 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 element and new threats, the risk manager have 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.

5.2 E-Business service

Let's analyse a different scenario, which was also hidden inside the above mentioned scenario. In contrast to the general scope-based case above, let's deal with the company's e-Business solution. Let's tighten the research question: "Does the usage of cloud services for the e-Business service fit the risk appetite of the company?"
Now we have much definite requirements. In the case of card payments, the e-Business or web shop provider must obey PCI DSS. Regardless of it has to be audited or just a self-assessment has to be made, the payment solution providers require compliance to PCI DSS. We are lucky in this case, because we have few direct requirements as listed below:[65]

Requirements	Testing Procedures	Guidance
A.1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfil these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below:	*Appendix A* of PCI DSS is intended for shared hosting providers who wish to provide their merchant and/or service provider customers with a PCI DSS compliant hosting environment.

[65] PCI DSS v3.1 Appendix A, p.110.

A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID. • All CGI scripts used by an entity must be created and run as the entity's unique user ID.	If a merchant or service provider is allowed to run their own applications on the shared server, these should run with the user ID of the merchant or service provider, rather than as a privileged user.
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin). A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) Important: An entity's files may not be shared by group. A.1.2.c Verify that an entity's users do not have write access to shared system binaries. A.1.2.d Verify that viewing of log entries is restricted to the owning entity. A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU	To ensure that access and privileges are restricted such that each merchant or service provider has access only to their own environment, consider the following: 1. Privileges of the merchant's or service provider's web server user ID; 2. Permissions granted to read, write, and execute files; 3. Permissions granted to write to system binaries; 4. Permissions granted to merchant's and service provider's log files; and 5. Controls to ensure one merchant or service provider cannot monopolize system resources.
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**A.1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review by the owning entity. • Log locations are clearly communicated to the owning entity.	Logs should be available in a shared hosting environment so the merchants and service providers have access to, and can review, logs specific to their cardholder data environment.
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.	Shared hosting providers must have processes to provide quick and easy response in the event that a forensic investigation is needed for a compromise, down to the appropriate level of detail so that an individual merchant's or service provider's details are available.

These requirements are the “Additional PCI DSS Requirements for Shared Hosting Providers” as the title of the Annex states. In an e-Business case this is the cloud service provider itself. All the above layers, which depend on the service model (XaaS), are treated by the core part of the PCI DSS and belong to the user or service provider. If we would like to do a risk assessment on our own, we can do the following:

Requirements	Result	Reason
A.1.1 Ensure that each entity only runs processes that have access to that entity’s cardholder data environment.	2	Only the entity’s cardholder data environment can be analysed.
A.1.2 Restrict each entity’s access and privileges to its own cardholder data environment only.	2	A.1.2.a: Only the current users’ applications and processes can be evaluated. A.1.2.b: File system permissions can be evaluated only at the current user’s drive space A.1.2.c: This can be tested indirectly, but the ACL lists can’t be accessed. A.1.2.d: Unauthorised viewing of logs can be tested indirectly only A.1.2.e: Vulnerabilities can be tested in black box manner, but needs previous authorisation.
A.1.3 Ensure logging and audit trails are enabled and unique to each entity’s cardholder data environment and consistent with PCI DSS Requirement 10.	3	Available in Google Apps for Business since March 2012[66]
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	1	Forensic investigation is not allowed for the end user.

Where Result field shows the following:
3: provable fact
2: partly provable, partly based on assumptions
1: not provable

The level of full compliance is achieved if all numbers are 3. When there is any number, which is smaller then 3, the full compliance is cannot be stated, thus the PCI DSS audit would fail. 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.

[66] http://googleappsupdates.blogspot.hu/2012/07/search-gmail-logs-in-administrator.html [2015.04.11.]

However, according to the Google Cloud Platform Blog[67] Google Cloud Platform achieved PCI DSS certification in the end of 2014.

If we accept a PCI DSS 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.

[67] http://googlecloudplatform.blogspot.hu/2014/12/google-cloud-platform-now-pci-data-security-standard-certified.html [2015.05.02.]

6 Conclusions

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 visualised in a simple way, however the problems are more complex and multi-dimensional. For example we don't have only two choices like on-premises or cloud-based system, but we can also differentiate on prices, security options, and hybrid solutions and so on. As a matter of fact the knowledge and experience of a professional can't 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. Visualisation functions help the businessmen to make some problems understandable.

There is another way of decision support: we can check the probability of compliance. This is not a brand new thing: Common Criteria (ISO/IEC 15408) is doing the same with the Evaluation Assurance Level (EAL) logic. Conformance is a yes or no question, but the question is that how much are we sure about the answer. According to this logic the paragraph 5.2 E-Business service is showing an example of noncompliance risk assessment based on the requirements of PCI DSS applied on the 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 a 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 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 a precise input to our risk management procedure. We shall use third party certifications in this case, which could be used for decreasing risk.

7 Bibliography

[1] 4GI Ltd., 2011. *MEHARI-Risk User Manual Software version 1.3,* Ledziny: 4GI Ltd..

[2] Alexin, Z., 2010. Our Privacy Act – with minor defects (in Hungarian). *Infocommunication and Law,* 7(38), pp. 104-109.

[3] Avram, M., 2014. Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology,* 12(0), pp. 529-534.

[4] Balogh, Z. G., Jori, A. & Polyak, G., 2002. *Establishing "best practice" of data protection in electronic public administration (in Hungary).* Pecs: PTE ÁJK IKJK.

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

[6] Bort, J., 2015. *Business Insider.* [Online] Available at: http://www.businessinsider.com/synergy-research-amazon-dominates-16-billion-cloud-market-2015-2
[Accessed 24 02 2015].

[7] Bose, R., (Robert) Luo, X. & Liu, Y., 2013. The Roles of Security and Trust: Comparing Cloud Computing and Banking. *Procedia - Social and Behavioral Sciences,* 73(0), pp. 30-34.

[8] Bouchaud, J.-P. & Potters, M., 2000. *Theory of financial risk from statistical physics to risk management.* Cambridge: Cambridge University Press.

[9] Brunette, G. a. M. R., 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing.* V2.1 ed. Seattle: Cloud Security Alliance.

[10] Catteddu, D. & Hogben, G. eds., 2009. *Cloud Computing. Benefits, risks and recommendations for information security.* Heraklion: ENISA.

[11] CLUSIF, 2010. *MEHARI 2010,* Paris: CLUSIF.

[12] de Sá-Soares, F., Soares, D. & Arnaud, J., 2014. Towards a Theory of Information Systems Outsourcing Risk. *Procedia Technology,* 16(0), pp. 623-637.

[13] Dedinszky, F., 2008. *Information security requirements (in Hungarian),* Budapest: MeH-EKK.

[14] DeJarnette, K. & Morin, J., 2010. *Privacy and Data Protection Audit and Assessment Strategies.* San Francisco, Deloitte, San Francisco ISACA Chapter.

[15] Ewart, P. J., Ford, J. S. & Lin, C.-Y., 1974. *Probability for statistical decision making.* Englewood Cliffs, NJ: Prentice-Hall.

[16] Gorge, M., 2007. Cyberterrorism: hype or reality?. *Computer Fraud & Security,* Issue 2.

[17] Habegger, B., ed., 2008. *International handbook on risk analysis and management. Professional experiences.* Zürich: ETH.

[18] Haelterman, J., 2010. *Introduction to ISO 31000,* Brussels: Grant Thornton.

[19] ISACA, 2012. *COBIT 5 Framwork,* Rolling Meadows, IL: ISACA.

[20] ISACA, 2013. *CRISC Review Manual 2014.* Rolling Meadows, IL: ISACA.

[21] Jori, A., 2005. *Handbook of data protection. Theory, practice and commentary (in Hungarian).* Budapest: Osiris.

[22] Kita, C. I., 2003. J.C.R. Licklider's Vision for the IPTO. *IEEE Annals of the History of Computing,* Issue 3.

[23] Kokolakis, S. & Lambrinoudakis, C., 2005. ICT Security Standards for Healthcare Applications. *UPGRADE European Journal for the Informatics Professional, 2005, Vol. VI, issue No. 4, p. 49.,* 6(4), pp. 47-54.

[24] Kopeczi, B., 1974. *From man-machine to machine-man (in Hungarian).* Budapest: Minerva.

[25] McCumber, J., 2004. *Assessing and Managing Security Risk in IT Systems : A Structured Methodology.* Boca Raton, FL: Auerbach.

[26] Mense, A. et al., 2012. *Security considerations in Cloud Computing: Are Private Clouds to handle different?.* Las Vegas, Las Vegas International Academic Conference.

[27] Metalidou, E. et al., 2014. The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences,* 147(0), pp. 424-428.

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

[29] Muha, L., 2013. *Interpretation of the Act on Information Security.* Budapest, Hacktivity.

[30] Muha, L. & Krasznay, C., 2013. Cyberdefense in Hungary: bless or curse? (in Hungarian). *HWSW ONLINE,* Issue 5026.

[31] Nagy, G., 1993. *Need for security.* Budapest: Sociology Research Institute.

[32] Netanjahu, B., 1995. *Fight against terrorism (in Hungarian).* Budapest: Alexandra.

[33] Racsko, P., 2011. *Cloud computing – informatics and communication in the cloud (in Hungarian).* Budapest, OBH-NKI.

[34] Reidenberg, J. R., 1998. Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review,* 76(3), p. 584.

[35] Shengmei, L. e. a., 2011. *Virtualization security for cloud computing service.* s.l., International Conference on Cloud and Service Computing (CSC).

[36] Spivey, J. e. a., 2009. *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives.* s.l.:ISACA Rolling Meadows, IL, USA.

[37] Steinberg, R. M. e. a., 2004. *Enterprise Risk Management Integrated Framework Executive Summary.* USA: The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

[38] Suicimezov, N. & Georgescu, M. R., 2014. IT Governance in Cloud. *Procedia Economics and Finance,* 15(0), pp. 830-835.

[39] Szadeczky, T., 2010. *IT Security Regulation and Practice in Hungary.* Budapest, ZMNE.

[40] Szadeczky, T., 2010. Pillars of IT Security. In: Z. G. Balogh, ed. *Studia Iuridica Auctoritate Universitatis Pécs Publicata.* Pecs: University of Pecs, pp. 247-268.

[41] Szadeczky, T., 2010. Problems of Digital Sustainability. *Acta Polytechnica Hungarica,* 7(3), pp. 123-136.

[42] Szadeczky, T., 2011. *Regulated security. The theory and practice of the regulation of information security and the methodology designed to make its application easier (in Hungarian),* Pecs: PTE AJK.

[43] Szadeczky, T., 2012. Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary. In: G. L. Szoke, ed. Budapest: HVG-ORAC, pp. 311-337.

[44] Szadeczky, T., 2014. Information Security - Strategy, Codification and Awareness. In: A. Nemeslaki, ed. *ICT Driven Public Service Innovation Comparative Approach Focusing on Hungary.* Budapest: National University of Public Service.

[45] Tiefenbrun, S., 2002. A semiotic approach to a legal definition of terrorism. *ILSA J. Int'l & Comp. L.*.

[46] Trocsanyi, S., 2007. The practice of handling medical data. From the cases of the Commissioner for Data Protection (in Hungarian). *Infocommunication and Law,* 4(19), pp. 93-37.

[47] Viraszto, T., 2004. *Cryptography, data hiding.* Budapest: NetAcademia.

[48] Wright, D. & De Hert, P., 2012. *Privacy Impact Assessment.* London: Springer.

[49] Zhiwei, Y. & Zhongyuan, J., 2012. A Survey on the Evolution of Risk Evaluation for Information Systems Security. *Energy Procedia,* 17, Part B(0), pp. 1288-1294.

8 Table of Figures