OPPORTUNITIES AND RISKS OF IT SOLUTIONS FOR ERM

PETER MITTERBAUR [1], JOHANNA PESENDORFER [2], ELISABETH SCHMIDINGER [3]
[1] Greiner Packaging
[2] Oberbank AG
[3] University of Applied Sciences in Upper Austria

***Abstract**: Compliance with legal regulations as well as the increasing pressure from various stakeholders demand continuously growing standards in company risk management. Rising complexity of businesses due to issues like globalization or the evolving role of the internet forces companies to reconsider their risk management approaches. In order to implement enterprise risk management in a successful and holistic way, IT systems have proven to be essential. However, the increasing reliance on IT systems not only in case of risk management but also for use in daily business also poses a number of risks for companies. This paper analyzes advantages as well as potential threats in connection with the use of IT in companies.*

***Keywords**: Enterprise Risk Management, IT Framework, COSO, GRC, IT Integration, IT Compliance, IT Security, Data security, cloud computing*

Introduction

In recent years corporates developed initiatives to improve cooperation and integration among organizational levels and business units. In response to various scandals, numerous laws to improve company risk management have been adopted. The legislative and regulatory pressure is still increasing and companies attempt to meet the requirements using holistic and integrated ERM frameworks rather than previously used traditional approaches (Deloitte 2012). Shareholders and stakeholders also have a strong interest that companies implement effective risk management strategies. Furthermore, these groups demand the best possible business decisions to maximize enterprise value and minimize their risk. Both for the optimization of risk management, as well as for the operational and strategic areas of the company IT support is indispensable, whereas the use of IT enables an improved overview of business processes and risk areas. As a result, necessary decisions and adjustments can be made at an earlier stage (Teubner/Feller 2008).

Although the use of information technology brings numerous advantages, it has to be remembered that various risks are generated by its use (Tohidi 2011). Accidental or intentional misuse of IT (Baracaldo/Joshi 2013) as well as new trends, such as cloud computing, the use of mobile devices or IT outsourcing can be mentioned in that case (Deprecency 2011). For this reason, it is necessary to incorporate IT security and IT compliance as important topics of enterprise-wide risk management.

Controversial perspectives on the use of IT for ERM frameworks

In the recent past enterprises had to deal with numerous risk aspects. The prevailing volatility and uncertainty in global markets as well as legal requirements were the drivers for the further development of risk management. The specialized departments and business units created by the companies span a wide range of internal audit, risk management, business continuity management, compliance to IT-security, to name just a few examples (Beugelaar/Van Loon 2011). All these responsibilities are essential regarding to further existence of a company, but each ERM activity has its own specific characteristics and is limited to its area and organizational structure. The majority was aware that a separate perspective - the so called "silo thinking" - is not able to perform the effectiveness of risk management or to improve the efficiency of the ERM processes. According to the study “The Convergence Evolution”, conducted by KPMG International and The Economist Intelligence Unit in 2012, only 12% of the surveyed companies maintain a fully integrated IT system for ERM activities.

The stakeholders exert pressure to induce improvement of ERM functions. (KPMG 2012). The management seems to be most interested in the improvements and developments (KPMG 2012).

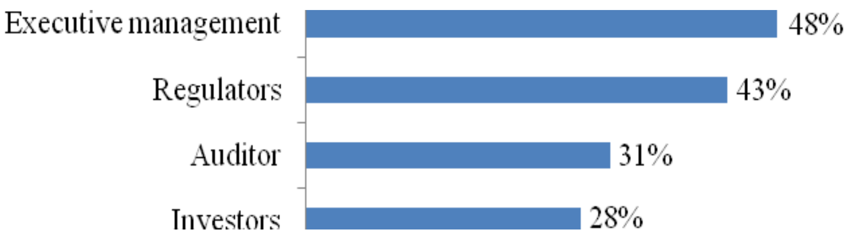

Figure 1: Pressure from the top (source: authors, adapted from KPMG 2012 p. 14)

Obviously, the management demands and supports the development of an integrated ERM framework, for a clear understanding of the important risks and their control as well for a transparent reporting.

Only the use of IT enables a company determining a holistic risk-return position (Götz et al. 2008). The need for the use of IT for efficient ERM processes is undisputed, nevertheless also possibly occurring disadvantages have to be considered. Technically supported risk management creates new risks that need to be monitored or solved in the best case. IT frameworks thus have a dual role, on the one hand IT supplies the databases for managing risks on the other hand IT itself causes new risks (Teubner/Feller 2008). Specifically, the company threatens the change or the loss of data. This can be done by technical infirmity, human error, internal sabotage, whistleblowing, identity theft or external attacks by viruses (Bayer 2013). Cloud computing, mobile devices and wireless transmission technologies such as WLAN, LTE, HSDPA and UMTS increase the risk for data leak. Efficient IT risk management is not able to exclude risks completely, but risks can be minimized.

The following section will analyze the opportunities and benefits of IT use for ERM frameworks.

Opportunities and benefits of IT use for ERM

The ERM approaches like COSO or GRC have a common goal: eliminate separate internal systems and existing redundancies among risk management activities by implementing a framework, supported by an IT platform. The use of IT infrastructure enables an improved and transparent insight into the status of risk and control. The implementation of ERM software can also significantly improve the manner, speed and effectiveness of reporting (Beugelaar/Van Loon 2011). Ideally, the application allows the preventive review of business opportunities for all enterprise divisions at all levels of the company concerning financial, legal and operational risks. Predefined programs and procedures enable the identification and analysis of risks and a promptly reaction to risk events. The monitoring of key risk indicators ensures the early detection of emerging threats. A suitable IT solution for ERM has become an important and indispensable tool for business management. The requirements are very complex and multi-layered because they are influenced by various different stakeholders.

In addition to the regulations of risk management and compliance individual state laws must be respected. Thereby the level of support for business processes trough IT continues to increase and consequently the implementation of the major part of requirements of risk managers depends largely on the performance of the IT infrastructure. The separation of duties for example is driven by the implementation of the Sarbanes Oxley Act. Compulsorily the ERM tool must provide an application for access and identity management (Hoffmann 2010). Primarily legal and economic reasons are crucial for the decision of IT use for ERM. Moreover, also operational reasons are mentioned mainly to exploit potential cost savings through IT operations. Furthermore, IT can also lead to a reorganization of the ERM processes and strengthen cooperation between the departments. Many companies see ERM as a necessary evil and as a cost factor, but the derived transparency can be used for streamlining the processes and compliance rules or even to reduce the manpower due to automated reporting and monitoring activities without interface problems.

Business Insights

In reality, it seems to be difficult to make the right decisions concerning the allocation of limited resources to perceive diverse ERM activities. According to the study “The Convergence Evolution” the annual costs for governance, risk and compliance activities are approximately at 5% of annual revenue.

A clear majority of interviewed senior executives admits that the risk and compliance processes are not sophisticated in their businesses and improvements are desired. (KPMG 2012). Furthermore, they agree that the currently used approach makes it difficult to determine the responsible person for particular functions (KPMG 2012). The consistency of data of the subsidiaries and the organizational processes across geographic boundaries are also reasons for dissatisfaction (KPMG 2012).

The following figure shows the perceived effectiveness of selected topics according ERM (KPMG 2012):

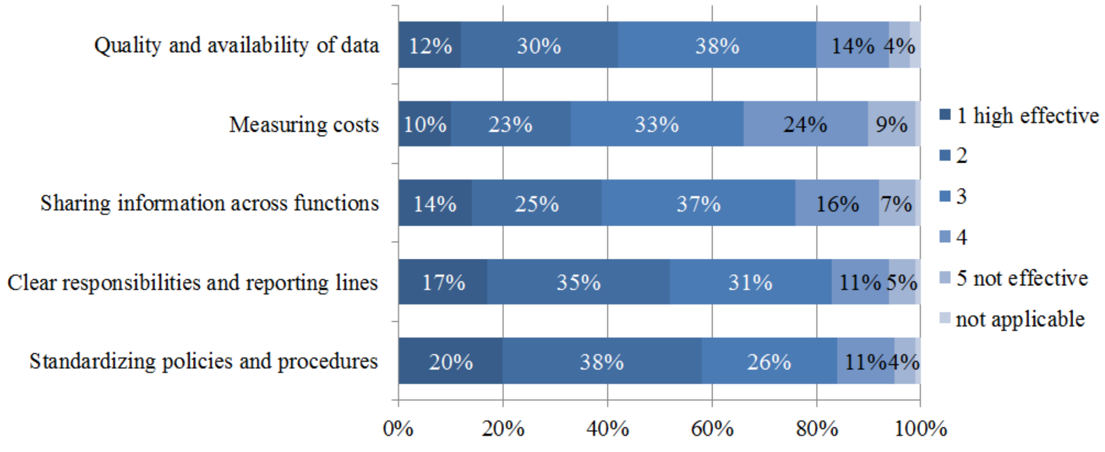

Figure 2: Effectiveness of ERM activities (source: authors, adapted from KPMG 2012 p. 6)

The result of the study leads to the assumption that the usage and degree of integration of ERM software tools is not very advanced today. A lot of dissatisfactions and many redundancies in ERM processes may be eliminated by the use of appropriate IT.

IT evolution for ERM frameworks

Due to the increasing number and complexity of regulatory, normative and internal requirements, also small and medium enterprises (SME) have to deal with ERM management systems. With implementing the ERM software it must be ensured that more value added instead of additional overheads can be created. A variety of SME use Microsoft Excel for data storage and administration of ERM activities. The requirements must be met with countless Excel spreadsheets. One challenge is to consolidate all data contained in these sheets and to be able to derive consistent statements (Haupt 2012). Then the results have to be processed and presented attractively in reports - based on past data.

The more complex and widely branched business organizations are the more software tools especially for ERM are recommended (Haupt 2012). If this applies it is feasible to create the added value of an integrated ERM approach to management. In order to add value through management systems, the collected data must support management in decision making. For this purpose, the information must be relevant, consistent, reliable and up to date. Because of this requirement, the use of database-driven software for an integrated ERM management is essential. In contrast to an Excel solution innumerable query options can be generated by multidimensional databases (Haupt 2012). As part of a specific metadata model the key entities such as objectives, risks, controls, employees and their relationship to each other must be created. The generated data cubes do not only provide the static reporting they also support sensitivity analysis and scenario planning.

To avoid redundancy and additional costs a verification of the use of any existing software components such as document management, workflow management and project management is recommended. Ideally, an embedding of ERM software into an existing IT infrastructure and the sharing of basic data is possible.

Many enterprises shy away from the high expenses incurred by an ERM software implementation or they even want to avoid change processes. If we consider the total cost of ownership ERM software normally performs noticeably better than Excel-based solutions (Haupt 2012). Additionally, ERM software provides other significant qualitative benefits and the possibility of gradual integration of other management systems. The implementation of several special solutions for ERM makes clear that an integrated data management is only possible with an elaborate and complex concept. (Hoffmann 2010). The consistency and patency of a stand-alone-solution for risk management, risk strategy, risk appetite, data design, implementation and monitoring is usually not the case (Hoffmann 2010). The realization of an integrated performance measurement system across all levels or integration into an internal control system or into the quality management system is hardly possible without an integrated framework.

At least in the consideration of IT risks as part of business continuity management a connection between the process level and the system level in terms of enterprise architecture management is essential (Hoffmann 2010):

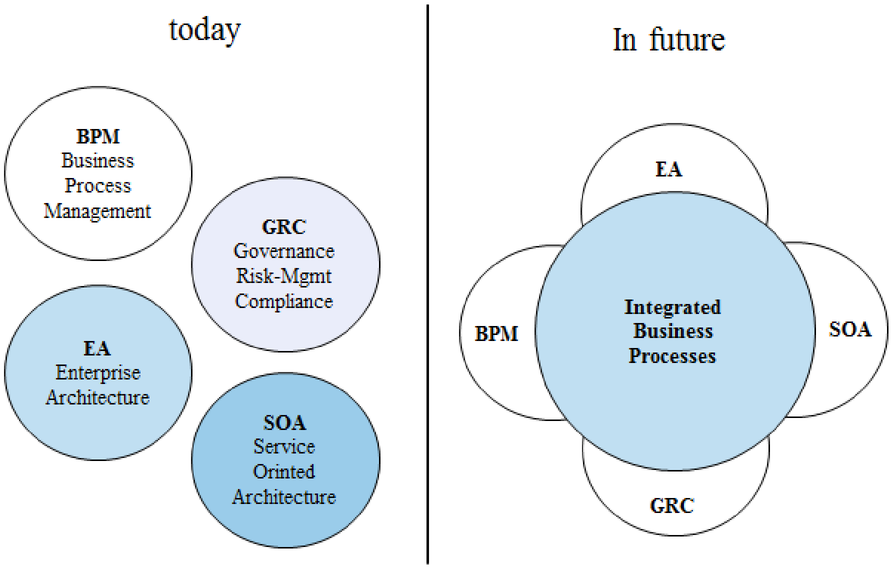

Figure 3: Integrated Business Process (source: authors, adapted from Hoffmann 2010 p. 10)

Greater and better control over risks

When companies grow or become active in new markets, organizational structures must develop accordingly. Controls must operate as efficient as possible even when the company pursue a growth strategy and maybe it needs to manage new types of risk.

In practice, the high complexity of the typically decentralized risk management cannot be solved without IT support (Gleißner/Romeike 2005).

For example, if a company exports its products to many countries, it needs to know all the country-specific regulatory requirements and act accordingly (Joseph et. al. 2010). Furthermore embargos or any kind of export prohibitions must be respected in order to preserve the image or even the existence of the company (Joseph et. al. 2010). A risk management optimized ERP solution can automate the compliance reports required for these activities.

The aim must be to install a risk management approach that allows a forward-looking and holistic view on controls, policies and procedures. By using modern technology and ERM software companies will benefit from the timely identification of risks and market opportunities. Risk management supported by efficient enterprise risk management tools is becoming more and more a success factor (Gleißner/Romeike 2005).

Particularly in compliance with laws and regulations, IT plays a significant role, especially in terms of technology-based transparency, security and accuracy of information processing (Teubner/Feller 2008). For example, the Sarbanes-Oxley-Act (SOX) defines rules to ensure the correctness of the accounting system (Teubner/Feller 2008). This takes place largely in IT-based ERP systems. The large number of legal requirements that IT management has to ensure and for which it must provide proof of lawful action, represents a major challenge. Especially for multinational and widely branched businesses, it makes sense to pair activities for governance, risk management and compliance with the existing ERP system. An essential requirement is the usability of the existing data for effective information flow to further processes. The assessment of hardly quantifiable risks can be done within integrated platforms including data modelling and analysis tools (Gleißner/Romeike 2005):

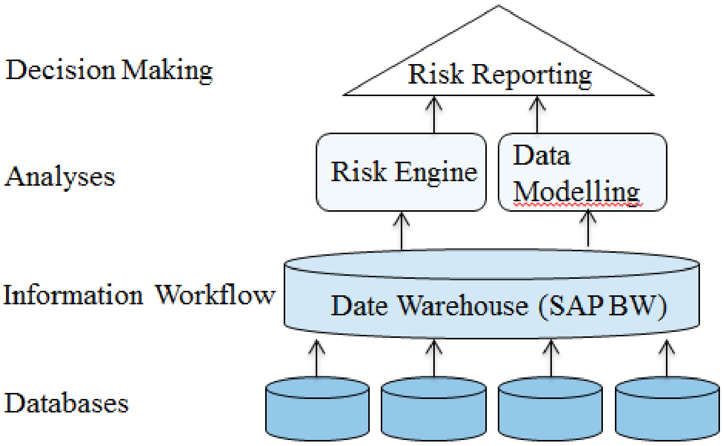

Figure 4: From data to decision making (source: authors, adapted from Gleißner/Romeike 2005 p. 155)

Provider of frontend solutions for ERM which are based on data from ERP are for example Oracle GRC Manager, SAP GRC Access Control or SAP GRC Process Control. These integrated systems assist in the monitoring of business risks, management of internal control metrics and support compliance processes.

The SAP Process Control application provides a single environment which shares corporate data and processes for many branches and different organizational structures. This GRC module includes real-time analysis as well as monitoring tools for compliance and risk procedures (SAP 2011). This ERM tool like SAP GRC enables executives to manage their risks proactively with one single framework. With users located around the world the management of an efficient user access risk is an audit concern for most companies. SAP GRC continues to serve a strategic solution for regulatory compliance and effective identity management (SAP 2011).

On the one hand the software helps to make risk management more efficient, on the other hand it supports enterprises to protect value and optimize organizational performance. Profit maximizing firms consider implementing an ERM program if the software can contribute to increase shareholder wealth (Hoyt/Liebenberg 2011).

The ability to control risks and to consider them adequately according to the corporate decision-making is one of the essential skills of sustainably successful companies. Only those companies that manage and control their risks efficiently are able to recognize and use their chances and to increase their enterprise value. A key role in achieving this goal plays the modern information technology, which enables an optimization of risk management. The IT has a key role as part of a powerful risk management but also as an object in the context of IT compliance and IT security.

IT Security

In the last years, information more and more became a major factor of production. Information technology has vast benefits like increased quality, accuracy and speed, thus IT systems are used in almost every company. Since a variety of confidential data is generated and stored digitally, IT security has evolved to a critical problem. Therefore effective risk management could not be done without including IT security. (Tohidi 2011). For that reason, IT is an important component of ERM because on the one hand, it mitigates risks but on the other hand, it creates new ones. The latter is due to accidental or intentional misuse of equipment or data (Baracaldo/Joshi 2013), but also due to trends like mobile computing, outsourcing or cloud computing (Deprecency 2011). Companies are aware about this to a certain extent, like a survey on IT governance by ISACA in 2011[1] shows. 85 % of organizations with more than 500 FTEs have IT governance processes installed (ISACA 2011).

To provide an overview of potential hazards, the chapter deals with selected topics concerning important IT security issues.

Authorization systems

For IT security it is essential that only authorized persons can distribute and modify access privileges. Otherwise, malicious groups could change access rights to allow themselves and third persons or to deny authorized people to have access to sensitive data (Kortesniemi/Särelä 2014). One approach to challenge this task is to use an Access Control List (ACL). In this case, each resource needs a privilege for every user. It is obvious that with many users and data this attempt could no longer be handled in a meaningful manner (Kortesniemi/Särelä 2014).

Role-based access control (RBAC) which has evolved to the most used authorization mechanism in organizations eliminates this disadvantage. Permissions are assigned to roles, and roles are assigned to the software users, whereas roles represent task areas such as risk management, controlling or accounting (Nassr et al. 2012). The reason for the wide acceptance is that on the one hand the access rights become role based and thus reduce complexity. On the other hand, it simplifies authorizations so that it is understandable for non-technical users and becomes a link between business departments (Giblin et al. 2010). However, implementation of an RBAC System is very costly. Roles have to be defined and permissions assigned, furthermore a complete set of roles is needed. RBAC systems have to be dynamic and must be managed, maintained and adapted to changing business needs (Giblin et al. 2010). In order to reduce the administrative effort, hierarchical models could be used, so that permissions can be inherited (Kuhn et al. 2010).

In large organizations, the dynamic demand could lead into thousands of separate roles, therefore pure RBAC is not flexible enough (Kuhn et al. 2010). Attribute Based Access Control (ABAC) allows more dynamic access behaviour with increased system complexity, for example, it is possible to execute operations between 5 am and 5 pm, but not beyond this timespan. Combined design between RBAC and ABAC could lead to reduced complexity and increased flexibility (Kuhn et al. 2010).

USB devices

Digital devices are increasingly represented in everyday life. Mobile phones and USB memory sticks nowadays provide several to over a hundred gigabytes of storage capacity. USB devices go along with non-negligible risks for companies, who are still neglected by many. These devices could serve as a starting point for viruses or malware, which may lead companies in incidents or catastrophes. Since employees are hours and days busy with tasks in the company, they often have the opinion to possess a right to sensitive and protected documents. Due to the availability of USB memory sticks or hard disks and their storage capacity, it is very easy to copy large amounts of corporate data without permission. Furthermore, the best external firewall is useless when the attacker is inside the company (Verma/Singh 2012).

[1] The survey was covering 21 countries, 10 industries, 834 respondents

Data deletion and data encryption

Countless files are stored on hard disk drives (hdd’s). Those devices have to be changed sometimes, whether as a result of defects, for performance reasons or otherwise. Obvious that sensitive data is stored on hdd’s. With data trading an own division has developed in recent times. Carelessness or ignorance led not only individuals to sale or dispose used hard disk drives. A study of O&O in 2011 showed that in over 80% of all cases data could easily be restored (O&O Software, 2011).

For secure data deletion, there are basically two different variants, physical destruction, or override. Simple deletion of data is insufficient, because the data is not physically erased. The Department of Defense (DoD) prescribes various methods for secure physical destruction such as melt, crush and more. With a completely destroyed drive data, recovery is no longer possible. Destroying the hdd makes data recovery impossible, but destruction is not always desirable. For data overwriting, there are methods such as the DoD recommended 3 times of overwriting to an algorithm developed by Peter Gutmann. Most professional data recovery companies say that data recovery is impossible even if the data is overwritten only once, therefore a 3 times override could be regarded as relatively safe (Diesburg/Wang 2010).

In addition to but not replacing data deletion, data encryption can be considered. Data will be scrambled and could not be restored without the special key. Data is still readable, but accommodate only pointless information, which has no value without decrypting. Due to various options such as simply trying all possibilities (brute force), this method can be cracked, which is the reason that encryption could only supplement a safe erase of data (Diesburg/Wang 2010).

Mobile devices

Not only the private use of mobile devices, but also the use of these devices for business purposes is booming. Smartphones and tablets are used for the coordination of appointments, for e-mailing as well as for accessing internal corporate data or sharing data via cloud services. Time and cost savings can be named as a primary benefit of mobile devices along with the ease of use. However, this leads to a non-negligible number of new created risks. (Büllingen et al. 2009)

Due to the high popularity of using mobile devices, it is worthwhile for hackers to select them as potential targets for fraudulent tasks. As mentioned above, devices are most of the time used to retrieve sensitive internal corporate data. Employees are often not sensitized to the dangers that appear when downloading apps or connecting their mobile devices to public hotspots (Leavitt 2011). The traffic generated by mobile devices rose from 2012 to 2013 by more than 80% to 1.9 exabytes per month by 2019 18 exabytes per month can be predicted. With the number of mobile devices used an increase from 6.6 billion (2013) to 9.3 billion (2019) is expected (Ericsson 2013). This rather impressive number is possible because many people are using more than one mobile device (AT Kearney 2013). Those numbers indicate that mobile devices will become the focus of criminal organizations in the future even more.

Users of mobile devices have to look out for many dangers nowadays, phishing, malicious applications, viruses or spyware just to name a few (Leavitt 2011). Spyware can be used to hijack a device, so all data on the device and even phone calls can be monitored. The problem with Spyware is that the software is hidden in the background and the user has no option to discover the software. Even companies use this kind of programs to monitor their property (Leavitt 2011). Malicious software acts similar to spyware. In a program fraudulent code is hidden, which taps data such as passwords and forwards it to the hacker (Leavitt 2011). The focus on mobile devices must be on the use of secure applications. Applications, which use cryptographic mechanisms to protect corporate data, provide a good information security (Merz 2014). However, the trend towards a mixed private and business use of devices can be considered as problematic. Private devices are used professionally and professional equipment is used for private purposes. Serious mispricing of risks happens, therefore employees have to be sensitized about the risks involved necessarily in the consideration of IT security (Buck/Eymann 2014).

Recently, a trend towards the use of outsourced network storage can be recognized.

Through the use of so-called cloud services the processes of storage expansion or development of infrastructure can be outsourced and therefore they can be customized easily (Subashini/Kavitha 2011). Although cloud computing was one of the most promising innovations in recent years, it still brings a variety of issues and challenges for companies (Sabahi 2011). The following chapter will specifically concentrate on cloud computing and the challenges and risks related to this technology which have to be conducted by an efficient ERM system.

Cloud Computing

Cloud computing is a flexible, requirements oriented use of IT services, which are provided real time via high capacity rail networks and have to be paid based on usage (Terplan/Voigt 2011). Currently the literature distinguishes between three service models und four characteristic forms.

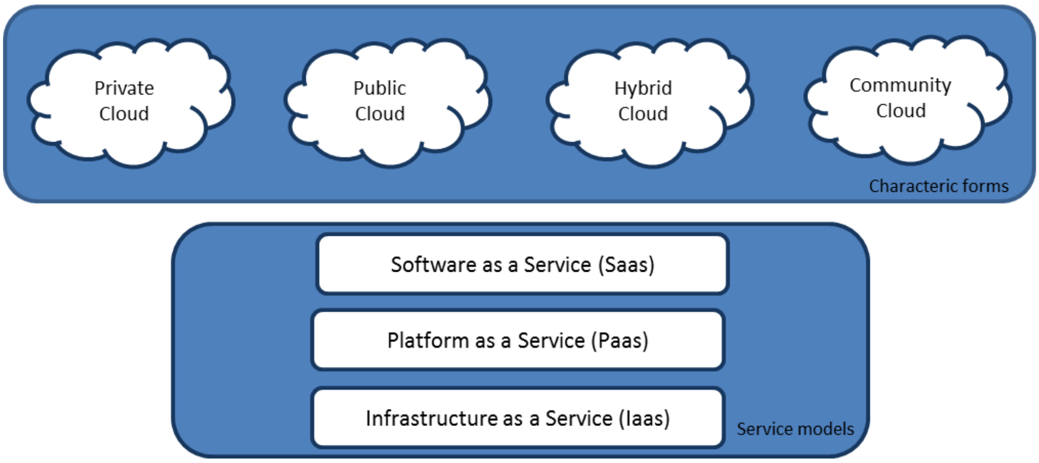
Private Cloud
Public Cloud
Hybrid Cloud
Community Cloud
Characteric forms
Software as a Service (Saas)
Platform as a Service (Paas)
Infrastructure as a Service (Iaas)
Service models

Figure 5: Cloud characteristics (source: authors, Grance/Mell 2011 p. 6-7)

Private Clouds are used only by one organization, community clouds by several organizations, whereas in a public cloud the service is used by a lot of users. The hybrid model is a mixture of the private and public form. The three service models build upon one another, whereas in case of SaaS the highest degree of abstraction is reached.

Current usage of Cloud services

The survey from ISACA investigated the current and planned use of cloud computing. Figure 6 shows that only 19.4% of the participants use cloud computing for non-mission-critical services. This value declines to 12% when talking about mission critical services. 40% of the respondents said that they plan to install cloud services for non-mission-critical services compared to 30% who want to use them for mission critical ones in the near future.

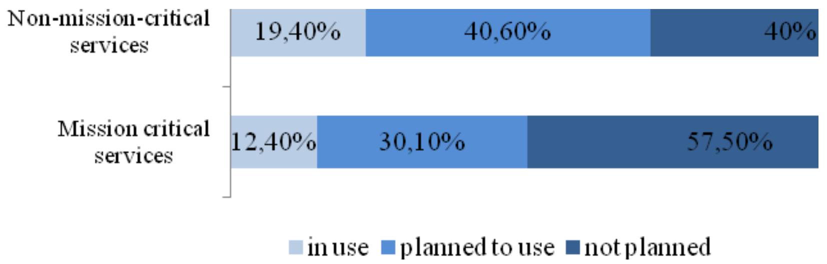

Figure 6: Use of cloud computing (source: authors, adapted from ISACA 2011 p. 37)

Among those who do not want to use cloud services data privacy, security and reliability issues are the driving factors.

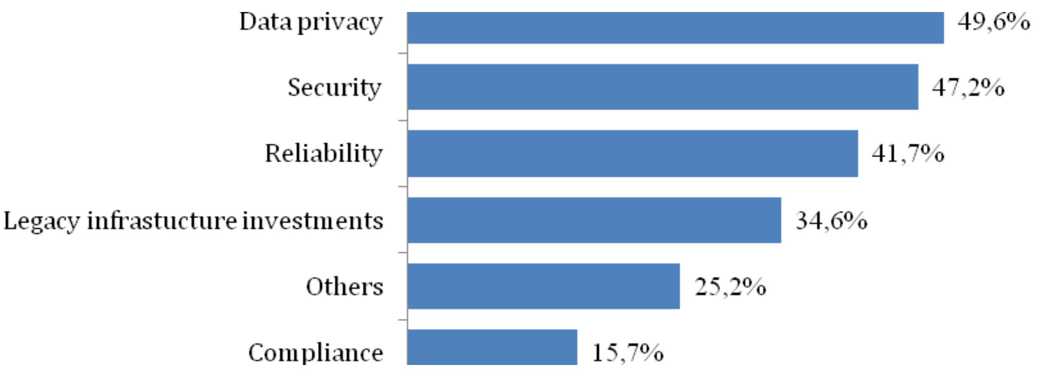

Figure 7: Reasons for not using cloud services (source: authors, adapted from ISACA 2011 p. 38)

Challenges and Risks of Cloud Computing

The reasons for not using Cloud services mentioned in the ISACA survey are quite similar to the ones discussed in current literature, although ´security´ can be seen as either an advantage or a disadvantage of cloud services.

Data privacy

The European data security law requires that the place, where individual personal data is stored, must be identifiable at any point of time. In case of cloud services, where the information is stored on several places all over the world this requirement can hardly be fulfilled (Christmann et al. 2010). The risks related to this point are manifold. When the storage location is unknown or shifts (without knowledge of the tenant) the applicable jurisdiction cannot be identified doubtlessly. Another potential risk for companies and their representatives is the one of being prosecuted because of uncompliant behaviour (Martens/Teuteberg 2011). Höllwarth points out in his guideline “Cloud Computing” that according to data protection law the tenant has to choose the Cloud Service Provider (CSP) carefully. The organisation has to assess the services defined in the contract before signing it and repeat this evaluation on a regular basis (Höllwarth 2011). When setting up a contract the tenant has to look if he has one or several Cloud providers. In case of several partner the contract contents have to be harmonised. The legal relationship becomes more complex and risky if the CSP is a so called general contractor. Although he is responsible for the subcontractors the problem of different legislation and data security intensifies (Juranek 2011). In the short term profits of the organization might be negatively influenced by costs for investigations and restitutions. In the long run reputational damage, loss of customer confidence and credibility can lead to big financial problems (Krutz/Vines 2010). To be compliant with the regulations and laws related to the place where the data is stored the use of private cloud services is the most secure one (Meir-Huber 2010 and Metzger et. al. 2011). CSPs face great risks in context with data privacy too. In case of Europe the member states have implemented the Data Protection Directive quite differently so the CSPs have to be aware being compliant to 27 different regulations. Additionally there are industry specific requirements that have to be fulfilled (Sunyaev/Schneider 2013).

Data security and reliability

A crucial aspect when switching to cloud services is the question of reliability and data security. Especially reliability is a major point of Service level agreement (SLAs) and can lead to high penalty payments for the vendor if the guaranteed figures – generally 99.9% - are not fulfilled. To ensure this high reliability as well as data security the CSPs store the data in several different data processing service centres. Smaller organisations can therefore improve their security standards when using the services of cloud providers, because the costs for multiple data backup would not be affordable for them. When using a public cloud service one always need the internet. Because it is unusual that the vendors provide VPN connections, a high level security standard does not exist. Instead there are open gateways which bear potential risks. It is up to both sides – the tenant and the vendor – to prohibit unauthorized use of these gateways. In case of the tenant by installing passwords that are not too easy to crack, in case of the vendor by a sophisticated security and risk management system (Meir-Huber 2010 and Metzger et al 2011). The redundant storage of the data goes along with problems. In case of different countries the jurisdictional question pops up again, which law has to be applied in case of a lawsuit (Martens/Teuteberg 2011).

Three measures can help companies to manage and remove uncertainty concerning these points. First a proper provider evaluation and selection process, second provider certificates so that tenants get some guidelines in this in other respects unclear market and third an effective risk and compliance management.

Risk and compliance management in the cloud

Martens and Teuteberg have developed a reference model for risk and compliance management in the Cloud.

The model, based on the ideas of GRC, has four perspectives (Figure 8) which influence each other to fulfil the requirements, whereat the KPI dimension plays a critical role because it enables the management to monitor and control. The limited space makes it necessary to focus on two of the elements of the model; further information can be read up in the article of Martens / Teuteberg.

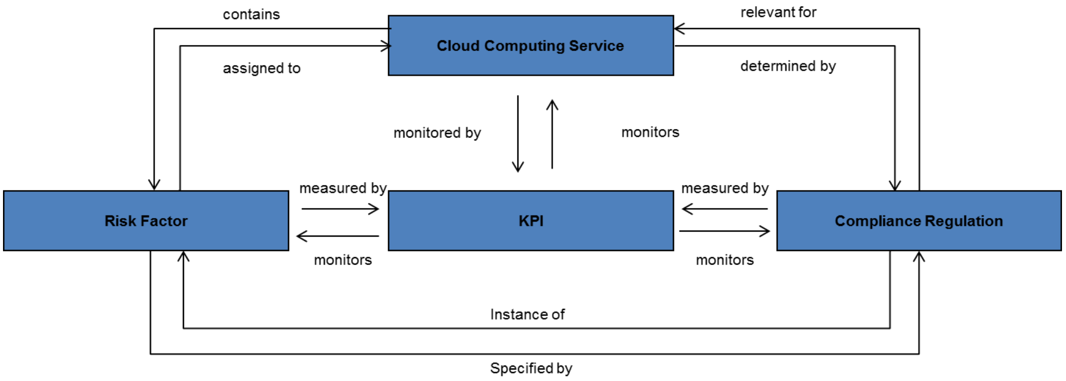

Figure 8: Meta-Reference Model for RC Management in the Cloud
(source: authors, adapted from Martens/Teuteberg 2011 p. 4)

In the cloud perspective issues like Cloud characteristics, SLAs and processes are discussed. Starting point are the Cloud characteristics. The choice of the service model – SaaS, IaaS, PaaS – depends on the risk appetite and boundaries the company sets. The question of the Cloud type is covered by this element too. In the SLA the negotiated service levels, costs, reliability targets and legal aspects are defined. The KPI perspective provides the necessary figures for monitoring these targets.

Certificates and Trust Management Systems for Cloud Services

SLAs are not sufficient to identify trustworthy Cloud providers. The decision to use or not use cloud services is mainly influenced by security and reliability topics. That is why certificates and Trust Management Systems (TMS) are necessary in this business.

Sunyaev et al. are convinced that independent certification institutes can be an appropriate answer for the existing lack of transparency, trust and acceptance especially among SMEs. The certification process must include an evaluation of the SLAs and provided services and an on-site audit of the data centre. To build up trust concerning data security the use of public key certificates as it is common practice in online banking could be an appropriate way. Additionally an assessment of the infrastructure security and the overall IT security management would complete a comprehensive view. For customers such certificates may be a useful guideline in the selection process but for CSPs it bears risks. Especially smaller ones might not be able to finance this certification process although it could be a good instrument for differentiation. So when installing a certification system for Cloud Services affordability on the one side and comprehensive, high quality assessment on the other side have to be ensured (Sunyaev et al. 2013)

TMS differs from trust and reputation systems. Whereas the latter one rely only on customers feedback a TMS works with numerous attributes relevant for evaluating Cloud services and get its information from different roots and sources (Figure 9). The computation of trust requires a powerful, high sophisticated system. To get a comprehensive picture quantitative and qualitative data, which might be contradictory in some cases, has to be incorporated. Because customers may assess the attributes differently the system has to be customizable so that each of them gets his own trust index. Another important aspect is resistance against manipulation. When TMS is an established relevant tool for CSP evaluation they will try to get high ratings and provide data that support this aim. An effective TMS has to identify and prohibit such attacks.

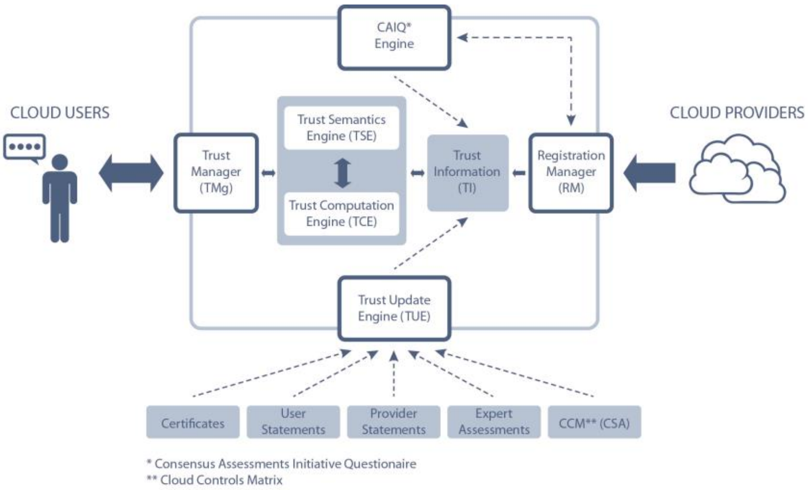

Figure 9: Architecture of a TMS (source: authors, adapted from Habib et al. 2011 p. 6)

Conclusion

Introduction of various regulations related to enterprise-wide risk management often brings corporations to their limits. Despite the increasing importance of risk management, it can be recognized that the majority of companies still deems traditional risk management approaches to be sufficient. Only a small proportion of companies already uses integrated ERM systems to manage their risks. Although decision-makers are well aware of traditional risk management's flaws, they shy away from implementation of integrated ERM systems due to expected high implementation costs, time and effort. On a short-term basis, these considerations may be correct. However, on long-term basis ERM systems will perform significantly better due to process improvements, automated risk evaluation et cetera. Besides these facts cross-departmental risk assessment will also lead to more reliable risk estimates. Furthermore, the applicability of traditional approaches for use in fast pace growing companies and very complex company constructs has to be questioned. For this reasons, the use of holistic ERM frameworks is highly recommended.

Even if information technology plays a crucial role in context to optimization of enterprise risk management, IT not only leads to minimization of risk but also creates new areas of risk to deal with. One key area of risk associated with IT use is the misuse of stored confidential data. Every day there are numerous cases of intentional data theft or accidental release of data due to the use of public networks. Although hacking with a percentage of 27.8 % is still the most used breach mechanism, data theft through portable devices with 18.4 % as well as insider threat with 16.7 % are often utilized breach methods. (Udoh/Adebayo 2014). In most cases, people are the weakest point and therefore they are the cause of miscellaneous activities to minimize IT risks like the implementation of complex authorization systems, the lock of various storage media like USB sticks or smart phones.

Another area of IT risks are new trends like mobile computing or cloud computing. Whereas mobile devices are mainly considered problematic due to the invocation of sensitive corporate data and frequent use of public networks, cloud computing defines a new type of data storage, which involves various new risks. The benefits seem overwhelming: flexibility of storage capacity according to actual requirements of the user is only one point to be mentioned. The use of cloud computing is currently still manageable, but numerous companies are planning to implement cloud solutions in the future. Reasons for abandonment of the numerous benefits are mostly risk topics like data privacy, security as well as reliability.

IT will always play a significant role in the support and further development of risk management. To ensure these functions, it is essential to identify potential risk areas concerning information technology at an early stage and to find appropriate solutions. ERM systems are valid tools to provide a holistic perspective on corporate risks and therefore enable rapid risk assessments and reactions in case of emergency.

References

AT Kearney (2013). The Mobile Economy 2013. http://www.atkearney.at/documents/3709812/3710624/BIP_The_Mobile_Economy_2013.pdf/1d78cea9-9e18-40ec-98d5-783dfbd86620 [downloaded 23.04.2014].

Baracaldo, N & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. Computer & Security, Vol. 39, 237-254.

Bayer M. (2013). IT-Risiko-Management ist gesetzliche Pflicht. Computerwoche, 42/2013. GBI-Genios Deutsche Wirtschaftsdatenbank.

Beugelaar, B. & Van Loon, W. (2011). Successful Governance, Risk and Compliance within reach. KPMG Compact IT Advisory, 11-20.

Buck, C. & Eymann, T. (2014). Risikofaktor Mensch in mobile Ökosystemen. HMD Praxis der Wirtschaftsinformatik, Vol. 51, 75-83.

Büllingen, F., Hillebrand, A. & Oczko, M. (2009). IT-Sicherheit als kritischer Erfolgsfaktor mobile Geschäftsanwendungen. DuD Datenschutz und Datensicherheit, 10/2009, 611-615.

Christmann, S., Hilpert, H., Hagenhoff, S. & Thöne, M. (2010). Datensicherheit und Datenschutz im Cloud Computing – Risiken und Kriterien zur Anbieterauswahl. HMD Praxis der Wirtschaftsinformatik, Vol. 47, 62-70.

Diesburg, S.M. & Wang, A. (2010). A Survey of Confidential Data Storage and Deletion Methods. ACM Computing Surveys, Vol. 43, No. 1, Article 2, 37 pages.

Debrecency, R.S. (2013). Research on IT Governance, Risk, and Value: Challenges and Opportunities. Journal of Information Systems, 1/2013, 129-135.

Deloitte (2012). Global risk management survey, eight edition. Setting a higher bar. http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/Us_fsi_aers_global_risk_management_survey_8thed_072913.pdf [downloaded 21.04.2014].

Ericsson (2013). Ericsson Mobility Report. On the Pulse of the Networked Society. http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf [downloaded 23.04.2014].

Giblin, C.,Graf, M., Karjoth, G., Wespi, A, Molloy, I., Lobo, J. & Calo, S. (2010). Towards an Integrated Approach to Role Engineering. Safe Config'10, 2010, 63-70.

Gleißner W. & Romeike F. (2005). Anforderungen an die Softwareunterstützung für das Risikomanagement. ZfCM Controlling &Management, 49. Jg. 2005, H.2, 154-164.

Götz B., Köhntopp F., Mayer B. & Wagner G. (2008). Einsatz einer ganzheitlichen GRC-Softwarelösung. HMD Praxis der Wirtschaftsinformatik, Band 45, Ausgabe 5, 89-98.

Grance, T. & Mell, P. (2011). The NIST Definition of Cloud Computing. *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf* [downloaded 16.4.2014].

Habib, S.M., Ries, S. & Mühlhäuser, M. (2011). Towards a Trust Management System for Cloud Computing. *http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6120922&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6120922* [downloaded 1.4.2014].

Haupt S. (2012). Mehrwert durch GRC-Software statt Overhead durch Excel - Sicherheit bei der Auswahl von GRC-Software. *Risk, Compliance & Audit*, Heft 03/2012, 17-23.

Hoffmann M. (2010). Governance, Risk and Compliance. *http://www.softwareag.com/at/solutions/banking/grc/overview/default.asp* [downloaded 14.04.2014].

Hoyt R. & Liebenberg A. (2011). The Value of Enterprise Risk Management. *The Journal of Risk and Insurance*, Vol. 78, No. 4, 795-822.

Höllwarth, T. (2011). Leitfaden Cloud Computing. Recht, Datenschutz und Compliance. *http://www.x-tech.at/download* [downloaded 15.04.2014].

ISACA (2011). Global Status Report on the Governance of Enterprise IT (GEIT). *http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/global-status-report-on-the-governance-of-enterprise-it-geit-2011.aspx* [downloaded 16.4.2014].

Joseph A., Arons A. & Crawford N. (2010). A Practical Approach to GRC Risk-Advisory and IT Collaboration. SAP Info GRC. *http://www.itelligencegroup.com/documents/SAP_Info_GRC_Byline.pdf* [downloaded 15.04.2014].

Juranek, J. (2011). Rechtliche Aspekte beim Cloud Computing. *http://www.zt-prentner-it.at/fileadmin/__UPLOADS/Diverses/cloud-loesungen/Praesentation_Dr._Juranek.pdf* [downloaded 10.04.2014].

Kortesniemi Y. & Särelä M. (2014). Survey of Certificate Usage in Distributed Access Control. *Computers & Security*, doi: 10.1016/j.cose.2014.03.013.

KPMG International & The Economist Intelligence Unit (2012). The Convergence Evolution - Global survey into the integration of governance, risk and compliance. *https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/convergence-evolution.pdf* [downloaded 13.04.2014].

Krutz, R.L. & Vines, R.D. (2010). Cloud Security. A comprehensive Guide to Secure Cloud Computing. Indianapolis. Wiley Publishing Inc.

Kuhn, D.R., Coyne, E.J. & Weil, T.R. (2010). Adding Attributes to Role-Based Access Control. *IEEE Computer*, Vol. 43, 79-81.

Leavitt, N. (2011). Mobile Security: Finally a Serious Problem? *IEEE Computer,* Vol. 44, 11-14.

Martens, B. & Teuteberg, F. (2011). Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. *http://www.uwi.uni-osnabrueck.de/martens/2011%20Martens%20Teuteberg%20Risk%20and%20Compliance%20Management%20for%20Cloud%20Computing%20Services%20Designing%20a%20Reference%20Model.pdf* [downloaded 02.04.2014]

Meir-Huber, M. (2010). Cloud Computing – Praxisratgeber und Einstiegsstrategien. Frankfurt. Entwickler. Press

Merz, P. (2014). Sichere mobile Unternehmensanwendungen. *HMD Praxis der Wirtschaftsinformatik,* Vol. 51, 45-55.

Metzger, C., Reitz, T. & Villar, J. (2011). Cloud Computing – Chancen und Risiken aus technischer und unternehmerischer Sicht. München. Hanser

Nassr, N., Aboudagga, N. & Steegmans, E. (2012). OSDM: An Organizational Supervised Delegation Model for RBAC. *Information Security*, Vol. 7483, 322-337.

O&O Software GmbH. (2011). Deutschland Deine Daten. *http://www.oo-software.com/de/studie-datenschutz-2011* [downloaded 21.04.2014].

SAP AG (2011). SAP Launches Next-Generation GRC, Enabling Unified View and Greater Control Over Risk. *PR Newswire US* 03/23/2011.

Sabahi, F. (2011). Cloud Computing Security Threats and Responses. *3rd International Conference on Communication Software and Networks*, 245-249.

Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, Vol. 34, 1-11

Sunyaev, A. & Schneider S. (2013). Cloud Services Certification. How to address the lack of transparency, trust, and acceptance in cloud services. *Communication of the ACM* 2/56/2013. 33-38.

Terplan, K. & Voigt, C. (2011). Cloud Computing. Heidelberg, mitp

Teubner A. & Feller T. (2008). Informationstechnologie, Governance und Compliance. *Wirtschaftsinformatik,* 5/2008. 400-407.

Tohidi, H (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science,* 3/2011, 881-887.

Udoh, I. & Adebayo, A. (2014). Breach Data Feedback towards Apt Security Measures. *Information and Knowledge Management,* Vol. 3, 83-91.