Journal of Risk and Financial Management

MDPI

Article

A Risk Management Framework for Cloud Migration Decision Support

Shareeful Islam [1,*], Stefan Fenz [2], Edgar Weippl [2] and Haralambos Mouratidis [3]

[1] School of Architecture, Computing and Engineering, University of East London, London E162RD, UK
[2] Secure Business Austria, Sommerpalais Harrach, Favoritenstrasse 16, 1040 Wien, Austria; SFenz@sba-research.org (S.F.); eweippl@sba-research.org (E.W.)
[3] School of Computing, Engineering, and Mathematics, University of Brighton, Brighton BN2 4GJ, UK; H.Mouratidis@brighton.ac.uk
* Correspondence: shareeful@uel.ac.uk; Tel.: +44-208-2237-273

Academic Editor: Xiao-Guang Yue
Received: 22 February 2017; Accepted: 10 April 2017; Published: 22 April 2017

Abstract: Managing risks is of paramount importance for enabling a widespread adoption of cloud computing. Users need to understand the risks associated with the process of migrating applications and data, so that appropriate mechanisms can be taken into consideration. However, risk management in cloud computing differs from risk management in a traditional computing environment due to the unique characteristics of the cloud and the users' dependency on the cloud service provider for risk control. This paper presents a risk management framework to support users with cloud migration decisions. In particular, the framework enables users to identify risks, based on the relative importance of the migration goals and analyzed the risks with a semi-quantitative approach. This allows users to make accurate cloud migration decisions, based on specific migration scenarios. Our framework follows basic risk management principles and proposes a novel and structured process and a well-defined method for managing risks and making migration decisions. A practical migration use case about collaborative application such as e-mail and document migration is considered to demonstrate the applicability of our work. The results from the studied context show that risks in cloud computing mainly depend on the specific migration scenario and organization context. A cloud service provider is not alone responsible for mitigating all the risks; hence, depending on the type of risk, the cloud user is also responsible for risk mitigation.

Keywords: risk management framework; risk assessment; cloud migration; security; analytic hierarchy process (AHP); business value

1. Introduction

Cloud computing provides many benefits for organization; specifically, cost saving, accessibility, and low maintenance overhead are well documented. There are risks associated with all aspects of cloud computing that are viewed as significant barriers for its widespread adoption [1,2]. Apart from the existing risks of computing infrastructure in general, the paradigm has new threats and risks that result from the unique characteristics of cloud computing and which need to be analyzed and controlled. The risks of the cloud, such as data leakage, lock-in, noncompliance with enterprise policies, and migration difficulties, could lead to a loss for business continuity that outweighs the expected benefits of using the cloud [3–6]. Moreover, risk varies depending on the cloud models and thus need to be addressed differently in different cases. The risk mitigation plan is also challenging even for the risks that are similar to other computing platforms and must be performed at service, data and infrastructure layers. This is because users have no control over or even any knowledge of the data once it has been migrated into the cloud infrastructure. Risk

management is one of the biggest concerns in cloud computing. It can outweigh the expected potential benefits of using the cloud and critical for businesses to stay functional and competitive. However, traditional risk management approaches need customization for supporting risk assessment in the cloud due to the variation of threats, cloud models, lack of users' control over the implementation of the risk control measures.

Existing efforts in the literature, which identify and analyze the risks for the cloud-based context, mostly consider security and privacy perspectives [7–9]. A limited number of works considers a systematic process for assessing and managing risks and making users aware of the issues that need adequate attention before considering the adoption of a cloud service. The novel contribution of this paper is a framework that supports (i) consideration of risk management from a holistic view of business, organizational and technical perspectives; (ii) a systematic process for assessing and managing risks based on the users' cloud migration context and relative importance of the migration goals; and (iii) supporting the users in making their cloud migration decision based on the assurance of existence risk control measures. Risk management in cloud computing is challenging comparing to traditional computing environment due to unique cloud characteristics such as multi tenancy and elasticity, which bring risks. Furthermore, risk control actions are not always under the control of the user, hence depending on the type of risks cloud service provider is also responsible for managing the risks. Our approach focuses on all these issues and contributes for assessing and managing the risks before any migration decision is taken. We consider six main migration goals—business value, organization function, confidentiality, integrity, availability and transparency—and determine the relative importance of the goals using an analytic hierarchical process based on the specific user's organizational context. The prioritized goals are used to assess the risks using a semi-quantitative approach to determine the risk level. Risk control actions are then identified based on the risk levels. Finally, the migration decision is taken based on the assurance that the potential cloud providers offers the necessary control measures for the risks that are out of users' control. The reason for considering the migration goals for risk management is that risk is defined as a negation of a goal. Organizations that intend to migrate their data into the cloud have certain number goals or objectives that they want to achieve with the migration decision, and risks certainly obstruct these goals. To demonstrate the applicability of our work, we consider a real migration use case from the SBA Research institute. The use case is about migrating collaborating applications which are critical for the business acceleration, improved productivity and decision making of SBA. The main goal is to evaluate the usefulness of the framework to identify the risks and to support for making the migration decision. We combine a case study method with action research, so that identified risks, controls and assurance of control measures can support SBA in making the migration decision.

The paper is structured as follows: The next section provides a detailed description of related work for risk management in the cloud computing context. The subsequent section describes the framework including the conceptual view and process, followed by the evaluation section, which demonstrates the applicability of our proposed approach with a case study. The final section concludes the paper and presents directions for future work.

2. Related Work

There are several publications that focus on risk management methods, migration decision support and on identifying risks for the cloud. This section reviews existing works in the area of risk management, security and privacy risks, which are related to our work.

2.1. Risk Management Framework and Migration Decision Support in the Cloud

A risk management framework should provide a comprehensive guideline for assessing and managing the identified risks. In [4], Islam et al. propose a goal-driven approach to analyze security and privacy risks of cloud-based systems. In [7], Saripalli and Walters propose a QUIRC security risk management framework based on six central cloud-specific security criteria, i.e., confidentiality, integrity, availability, multiparty trust, mutual auditability and usability, to identify and assess the security risks. In [8], Samad et al. consider a quantitative risk model for dynamic mobile cloud

environments. Risks in such systems are related to connectivity, limited resources, security, and limited power supply at the system level. In [9], Zhang et al. propose a security risk management framework for the cloud computing environment by following the ISO/IEC 27001:2005 standard. The process starts with the identification of critical areas, strategy and planning, followed by risk analysis and control. The framework is very generic and can be applied to any context. It does not provide any guidelines for determining the risk levels. There are standards such as ISO 31000:2009, which provides guideline risk management activities and considers risk management an integral part of the overall organizational processes, including strategic planning and all project and change management processes [10]. Fit'o et al. consider business level objective-driven semi-quantitative cloud risk assessment [11]. The risk level is estimated for each business level objective based on the probability of occurrence and impact. Five different risk levels are defined: critical, unacceptable, negligible, profitable and high profitable. Such an approach helps to determine profit maximization as a business level objective. However, the work is at a very early stage with a very brief description of the risk level estimation that makes it difficult to understand. Fit'o et al. in [12] also propose a Business-Driven IT Management (BDIM) model and optimization loop which aims to fulfill cloud service provider's business strategies. It includes three different levels of BDIM and links the levels with cloud environment and policy management framework. The optimization loop mainly considers fulfillment of business level objectives by looking IT event consequences on business results.

There are also works that focus on the understanding of the risks associated with the specific cloud migration scenario and demonstrate the real benefits of cloud migration decision support. Gadia presents a case study of a software development company which intended to migrate into the IaaS based solution instead of existing SaaS using cloud risk assessment [13]. There are several audit findings that provide gaps by the CSP to achieve the security objectives such as provider contract does not address the users security and privacy requirements, multi-factor authentication was missing, and sensitive data is exchange without secure a channel. ENISA analyzes three use-case scenarios, i.e., SME perspective, service resilience, and e-health, for the purpose of risk assessment [14]. The results identified a list of high level risk such as lock-in, malicious insider loss of governance, compliance challenges and isolation failure, and medium ranked risks are such as loss of business reputation, service failure, cloud provider acquisition, and supply chain failure. The risks impacts are varying depending on the type of cloud model. The security transparency framework to address the risks relating to violation of service level agreement is proposed by [15]. Microsoft proposes a cloud risk decision framework by following the overall process of ISO 31000 standard so that the right decision about the viability of cloud migration proposal can be obtained [16]. The COSO enterprise risk management for cloud computing emphasize on the higher level of inherent risk due to less direct control of enterprise assets migrated into cloud [17]. Therefore, there could be small investment for cloud migration as one of the well-known benefits but it could incur a big impact. The decision should consider the enterprise business process that the cloud could support, service and deployment model, and the nature of provider's risks and control environment.

2.2. Risks in the Cloud

Risks are the potential negative consequences that could outweigh the benefits of the cloud adoption. Lemos identified five main negative aspects of cloud computing: less legal protection, hardware ownership, policy, untrustworthy machine instances and individual assumptions [18]. In a European Network and Information Security Agency report, Catteddu and Hogbun pointed out legal risks besides security and privacy risks in the cloud from an organizational perspective [19]. Similar to the traditional computing environment, attacks like man-in-the middle, cryptographic, and Trojan attacks are also potentially applicable in cloud computing [20]. There are several works that demonstrate successful attacks on cloud service provider (CSP) infrastructure. In [21], islam et al identify the goals and risk of cloud migration. In [22], Theoharidou et al. examined the privacy risks migrating data, applications or services into the cloud by following privacy impact assessment with ten fundamental privacy principles such as accountability, clear purpose, and consent. Vimercati et

al. review the privacy risks and existing solutions for managing and accessing data in the cloud [23]. The risks are related to data dissemination and sharing, external storage of data, collaborative query execution, and anonymous communication for access data and storing it into the cloud. Pearson identified several privacy risks for cloud computing for users, organizations, cloud platform implementers, and providers. In particular, the main risks are disclosure of personal information, noncompliance with enterprise policies, loss of reputation [24]. In [25], Khosravani et al. present a case study about managing the risk of cloud adoption associated with highly sensitive data on children and sexual abuse cases of a charity. The case study is evaluated through a framework that analyzes the trust and controls for mitigating the risk of cloud adoption. Khajeh-Hosseini et al. identified potential benefits and risks for migrating into the cloud in a case study of an oil and gas industry SME in the UK [26]. The results showed that there are definite cost-saving system infrastructure advantages, i.e., a 37% reduction in costs over 5 years on EC2 as well as a 21% reduction in support calls. The study concluded that despite the advantages there are socio-technical issues that must be taken into consideration for cloud migration.

To summarize, all the works mentioned above justify the necessity and importance of considering risk management for cloud computing. We have identified several observations that demonstrate a number of limitations of the existing works. There is no comprehensive risk management framework that supports an organization by identifying potential risks before considering cloud adoption. Most of the risk management frameworks emphasize more on security and privacy risks rather than looking at other areas of the existing organizational context. Furthermore, there is a limited effort in the existing work to consider estimation of accurate risks level. Every organization intends to migrate into cloud certainly expects several benefits for using cloud and these benefits are the goals. Therefore, it is necessary to analyze these goals before taking any migration decision. Our work intends to fill these gaps and hence improves the existing risk management practice for the cloud computing domain. In particular, the novel contribution of our work is a risk management framework that supports the users with cloud migration decision looking at the migration goals, inherent risks and existing controls. The risks are considered from a holistic perspective of technical and non technical dimensions. The framework considers six generic migration goals and determines the net level of identified risks based on the relative importance of the migration goals. This helps user to understand as an early warning what could go wrong if the migration decision is taken place so that an informed decision can be taken for cloud migration.

3. Risk Management Framework

The proposed framework provides a comprehensive view of the risks to support an organization in making the cloud migration decision and balances the benefits with the potential risks. The scope of the risk management framework is to support the cloud migration decision and to monitor the risks during the operation. The framework includes risk management areas, conceptual view and a process for this purpose.

3.1. Conceptual View

Figure 1 shows an abstract view of the risk management framework. It includes several concepts such as migration goal, migration profile, risk, control, and assurance. We follow the existing risks management approaches, cloud computing, and goal modeling language to identify these concepts. Goals are the objective and expectation to support the organization due to the cloud migration. Risks are derived from the risk management areas and migration profiles. The risks obstruct the migration goals and need appropriate assessment. We follow the semi-quantitative risk assessment approach based on the risk event likelihood, impact, and prioritized migration goals. The assessment shows which risks need to be controlled based on the organizational context and migration profile. Risks are controlled by following different control strategies such as prevention, reduction or avoidance. The cloud user needs to ensure that appropriate measures are in place for controlling the risks. Therefore, assurance is necessary to confirm that the relevant control measure is complete. The user's migration decision depends on the results of this assurance and information within the migrated

entities. If the migration decision is taken, it is necessary to monitor the evolution of key risks and development of new risks and take appropriate actions to control the evolved and new risks.

The concepts are linked with each other through the activities to support tasks for the purpose of risk identification, assessment, mitigation and migration decision. The concepts are used within the task for transformation of output from input and assign different values. For instance, identify and categorize risks activity identifies the possible risk as a concept and causes as factors for the concept due to the cloud migration within the existing business context based on a specific migration profile. These risks are then assessed by using the relative importance of the migration goal and likelihood and impact properties of risk through the risk analyse and control activity. The task migration decision is triggered based on the level of completeness of assurance concept for the risk mitigation and supports an informative migration decision. Once the decision is taken, it is necessary to monitor the existing risks and identify any new risks due to the evolution of cloud platforms, changing of user needs, requirements or amendments to the CSP's terms and conditions. The task monitor risks in operation uses monitor concept to check the net risk level before and after the migration and identify any new risk that needs adequate attention.

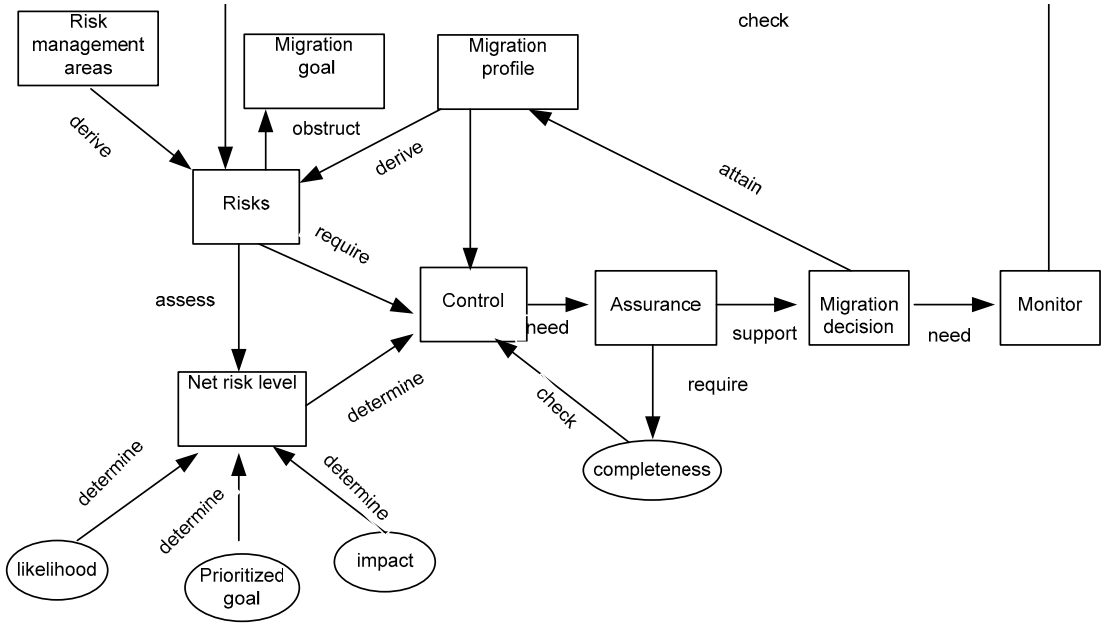

Figure 1. Conceptual view of risk management framework.

3.2. Risk Management Process

The process comprises of four sequential systematic collections of activities 2. Each of these activities has specific inputs and results in specific output artefacts. We follow the guidelines of the existing risk management standards ISO31000 and ISMS standard ISO27001:2013 to define the process [27]. A brief description of the activities is given below.

Activity 1: Initialize Risk Management

This is the first activity, which establishes the risk management context by following the cloud migration profile and formally approves the risk management activities within the organization. This requires active involvement of the management representatives and risk manager for planning the risk management activities focusing on the migration goals. This activity includes two tasks: defining the migration profile and planning risk management.

Task 1A: Define Migration Profile

The migration profile analyzes the existing organizational context and rationalizes the migration needs. This phase identifies the migration goals, organizational strengths and weaknesses, migration type, and potential migrated assets profile. It is also necessary to identify the key operational responsibilities to support the migration activities. Goals play a key role for risk management. These goals are the benefits and expectations of the cloud migration and have a potential impact on the organization. We consider six main migration goals, as given below:

- Business Value (BV): This goal includes the main business gain in terms of financial profit, maintenance benefits, service delivery, business growth—specifically in new markets—and competitive advantages due to cloud migration.
- Organization Function (OF): The organization function goal considers key operations for successfully running the business, including internal process improvement, customer services, human resources, collaboration with internal units and business partners, business continuity and disaster recovery, and efficient IT usage and IT availability.
- Confidentiality (C): This goal deals with not disclosing data to unauthorized users, including cloud users, CSP-internal users, and malicious attackers. The goal also includes secure deletion and transfer of data between authorized parties to prevent the data leakage.
- Integrity (I): Integrity refers to the trustworthiness of the migrated resources. In particular, the data migrated into the cloud must only be modifiable by authorized users.
- Availability (A): Availability refers to the migrated resources, such as data or applications, being accessible when needed and the cloud service being available as per the agreement.
- Transparency (T): Transparency refers to the dissemination of information about access to and usage of user data, security incidents and audit reports by the cloud service provider. It also considers real-time monitoring of virtual machines and SLAs. Transparency is critical for the mutual trust between the user and the CSP.

Task 1B: Plan Risk Management

This task initiates the implementation of risk management by determining the risk management scope, schedule and resources, risk treatment and monitoring strategy (if applicable) based on the migration profile. Risk management for the cloud entails supporting complex migration decisions; therefore, the plan should consider a proactive approach for risk control. The plan also determines the riskiness of the potential migrated project, in particular, how risky the cloud migration would be in terms of cost, schedule, risk control and business continuity. There are three levels of riskiness: high, medium and low. Generally, if an in-house application needs major amendment, employees lack the skill needed for the migration to the new technology, security controls and CSP support are poor, or the plan is to migrate highly sensitive data, the level of riskiness of the migration project could be high. There are various assets involved in the migration, and the functionalities of these assets change over time. The plan also identifies use cases/applications (if any) that are inappropriate for the cloud based on the risk levels and existing countermeasures. This helps isolate the assets involved and how they change over time to identify the vulnerabilities of the cloud environment. This activity mainly outputs the risk management plan and riskiness level of the overall migration project.

Activity 2: Identify and Categorize Risks

Once the risk management context and migration profile has been defined, the next activity is to identify all possible risks that could have an impact on the cloud migration. The input for this activity is the risk management and migration context identified by the previous activity and output produced by the activity is the risks list and associated category. This activity consists of two tasks.

Task 2A: Identify Risks

This task identifies all the possible risks and associated factors that could have an impact on the cloud migration project. Risk factors are the main causes of any risk, and controlling these factors is the initial concern of risk management. We need to identify as many risk factors as possible so that the organization is aware of the possible problems that could occur if the migration is undertaken. All risk factors and risk have unique name. One factor can influence more than one risk. Several techniques are employed for risk identification, such as reviewing the migration profile, criticality of the data, and interviewing the experienced organizational staff. Applications that are candidates for cloud migration, existing risk details from other projects of the organization, users' organizational environment and technical expertise with cloud technology, and risks from literature relating to cloud migration should be taken into consideration while identifying the risks. Risks focus on the major threats to the cloud models that could hinder the achieving of the migration goals during the cloud deployment and operation of the migrated entities. Risks like loss of revenue and data leakage are common in the context of cloud attack surfaces. In the case of the cloud, risk could be exploited by a malicious application as well as internal organizational users, CSP employees, and other tenants.

Task 2B: Categorize Risks

The identified risks should be categorized based on their impact on the organization's overall business continuity and ability to fulfill its mission and day-to-day tasks. We categorize risks into three groups: business, organizational, and technical. A brief overview of given below:

- Business risks: These risks directly obstruct the achieving of the user's main business goals. Business risks reduce the financial benefits and brand value and incur financial loss for the overall business continuity.
- Organizational risks: Such risks mainly focus on issues relating to the user's and cloud provider's overall organizational operational context. For instance, a cloud user organization's employee's inadequate experience with cloud technology and maintenance difficulties could lead to a severe business disruption while migrating and operating in the cloud. It is hard to predict and control human factors relating to human error and behaviors that pose a risk in the cloud context.
- Technical risks: These risks include underlying technical issues such as the cloud platform being affected by malicious code, hypervisor-level attacks, data leakage due to the multi-tenancy architecture, system malfunctions, or unauthorized transmission, which are more probable in a cloud-based context. Security and privacy issues play a critical role for the technical risks. In particular, the loss of confidentiality, integrity and availability as well as lack of transparency would certainly disrupt the business mission.

Activity 3: Analyze and Control Risks

Risk analysis helps creating a preliminary assessment to protect various assets and prevent certain threats from happening. This activity assesses the risks to determine the net risk value and identifies the necessary control action for mitigating the risks. Therefore, risk assessment plays a critical role in this activity. Using the full quantitative risk assessment method is challenging in the cloud computing domain due to the difficulty of obtaining precise risk probability and impact values based on historic data. It is also time consuming and costly. However, such an approach provides an accurate measurement of risk magnitude. Qualitative approach instead does not require precise values for calculating the risk probability and impact. However, such approach does not provide a precise value of risk. We follow semi-quantitative approach for determining the risk level. Hence, our goal is to provide a simple and straightforward estimation process for usable risk management. This activity consists of two tasks:

Task 3A: Assess Risks

Once the risks and risk factors have been identified in the previous activity, we need to calculate the net risk value. This task calculates the net risk value based on the relative importance of the affected migration goal. We follow a semi-quantitative assessment approach for determining the net risk level. This task consists of two steps.

Step 1: Relative Importance of Migration Goals

In our case, the net risk calculation depends on the relative importance of the migration goals. We use the analytic hierarchy process (AHP) for this purpose [28]. Each goal is compared with the other goals based on its importance level within the organizational context for the cloud migration. The importance levels follow the AHP scales, i.e., 1–9 as shown in Table 1, where 1 denotes equal importance and 9 is the extreme importance of one goal compared to another. The relative importance is the weight factor of the normalized principal Eigen vector value of the migration goal. Once the importance level has been obtained, the comparison matrix CM values are normalized to identify the relative weight of each goal. The sum of the weight values should be 1. Generally, the experienced staffs of a migration project need to agree on values for the importance levels. It is necessary to check the consistency of weight values by following Equation (1) according to AHP to avoid any inconsistency of the ranking values. If the consistency ratio is more than 10%, the assumptions for the relative importance are inconsistent and we need to redefine the values.

Let,

CR: Consistency ratio
CI: Consistency index
RI: Random consistency index
CM = Comparison matrix value
BV = Business Value, OF = Organization Function, C = Confidentiality,
I = Integrity, A = availability, T = Transparency

$$CM_{ij}= \begin{array}{c|cccccc} & \mathbf{BV} & \mathbf{OF} & \mathbf{C} & \mathbf{I} & \mathbf{A} & \mathbf{T} \\ \mathbf{Bv} & \mathbf{CM_{i,j}} & - & - & - & - & \mathbf{CM_{i,6}} \\ \mathbf{OF} & \mathbf{CM_{i+1,j}} & - & - & - & - & \mathbf{CM_{i+1,6}} \\ \mathbf{C} & \mathbf{CM_{i+2,j}} & - & - & - & - & \mathbf{CM_{i+2,6}} \\ \mathbf{I} & \mathbf{CM_{i+3,j}} & - & - & - & - & \mathbf{CM_{i+3,6}} \\ \mathbf{A} & \mathbf{CM_{i+4,j}} & - & - & - & - & \mathbf{CM_{i+4,6}} \\ \mathbf{T} & \mathbf{CM_{6,j}} & - & - & - & - & \mathbf{CM_{6,6}} \end{array}$$

Table 1. Comparison matrix scale.

Importance Level	Definition
1	Equal importance of two compared goals
3	Moderate importance/one goal slightly favored over the other
5	Strong importance/one goal strongly favored over the other
7	Very importance/one goal very strongly favored over to the other
9	Extreme importance/one goal extremely favored over the other
2,4,6,8	Intermediate values

$$(CR) = \frac{CI}{RI} \quad (1)$$

Step 2: Net Risk Calculation

The net risk calculation depends on the associated risk factor values. Therefore, we need to determine the risk factor values for the net risk calculation. Each risk factor value is estimated through the product of its probability and impact of overall risk as shown in Equation (2). As stated previously, it is difficult to obtain historic data for risk factor probability and overall risk impact in the cloud environment. We use subjective judgment depending on individual perception for defining probability and impact values. We also consider a rule of thumb with the following three rules to support the estimation:

- Rule 1: Risk impact depends on the affected migration goals. If a risk affects important migration goals, impact is certainly high.
- Rule 2: If the risk factors may be, at least partially, beyond the control of a user's organization and mainly posed by the CSP, the overall risk impact can be higher.
- Rule 3: Individual judgment is always useful for net risk calculation. However, individual perception should be closely mapped with reality, otherwise we may overestimate or underestimate risk value.

The risk value is obtained by averaging the risk factors' values as shown in Equation (3). Finally, the net risk level is the sum product of risk level and relative importance of affected migration goal as shown in Equation (4). This allows us to determine the risk level accurately through its influence to the migration goals. We follow the same scales for probability, impact and net risk value to make a simple estimation process.

Let,

r_i: Individual risk factor value
r_{i1}.....r_{in}: n influential risk factors of a risk R_i
$P(r_i)$: Probability of a risk factor r_i
Probability scales = unlikely (less than 0.30), likely (0.30–0.59), certain/expected (above 0.60).
I: Impact of overall risk R_i
Impact scales = low (less than 0.30), medium (0.30–0.59), high (above 0.60)
R_i: Value of a risk R_i
R_{net}: Net risk of R_i
W_e: Relative weight of the affected migration goal [BV, OF, C, I, A, T] by R_i
Risk level scales: low risk (less than 0.30), critical risk (0.30–0.59), highly critical risk (above 0.60)

$$r_i = P(ri) \times I \quad (2)$$

$$R_i = \frac{1}{n} \sum \{r_{i1}, r_{i2}, r_{i3}, \ldots\ldots\ldots\ldots, r_{in}\} \quad (3)$$

$$R_{net} = \sum We \times R_i \quad (4)$$

Risk levels

- Low risk (less than 0.30) implies that it is recommended to develop a corrective measure and contingency plan.
- Critical risk (between 0.30 and 0.59) implies the risk has an adverse affect on the organization and corrective actions are needed and a contingency plan should be developed if necessary. A plan should be developed for the execution of the control measure within a specific period of time.
- Highly critical risk (above 0.60) implies the identified control measures for the risk mitigation need to be implemented immediately within a short time frame with a plan. The risk level is highly critical if both the probability of the risk event and its impact are high or one is medium and another high.

Task 3B: Identify Potential Risk Control Measures

This task identifies the possible control measures that could mitigate and eliminate the identified risks to the cloud environment. Figure 2 shows a possible risk control strategy for managing identified risks relating to cloud migration. In the context of cloud based systems, prevention measures should avoid or deter the occurrence of any event that can potentially have a negative consequence. We advocate a prevention strategy for the cloud migration decision that includes realistic preventative actions such as clear assignment of roles and responsibilities to support the adaptation actions during the migration, strong access control mechanisms, and a business continuity plan. These measures are effective in controlling risks during migration. No-control action strategy mainly does not follow an immediate control action for a risk, rather reviews and monitors the risk further by gathering information after migration. Such measures are necessary in cloud-based systems for collecting evidence to support the audit. For instance, audit trials, provenance, monitoring suspicious activities, complete deletion of data, and security incident reports are detective measures. Users should be able to customize the monitoring of resource use to support the detective measure, as application performance after migration is necessary to support the business. Once the potential control measures have been identified, it is necessary to determine who is responsible for implementing the control measures. Depending on the nature of the risk and control measure, both the user organization and CSP may be responsible for managing the risks. Furthermore, we also need to review the risk factors to determine whether the identified control measures are able to eliminate or reduce the risk factors and to improve the situation caused by the risk factors. At the end of this activity, the risk register is updated with all identified risks from the previous activity, risk level, possible risks control strategy and suitable control measures for the risk control.

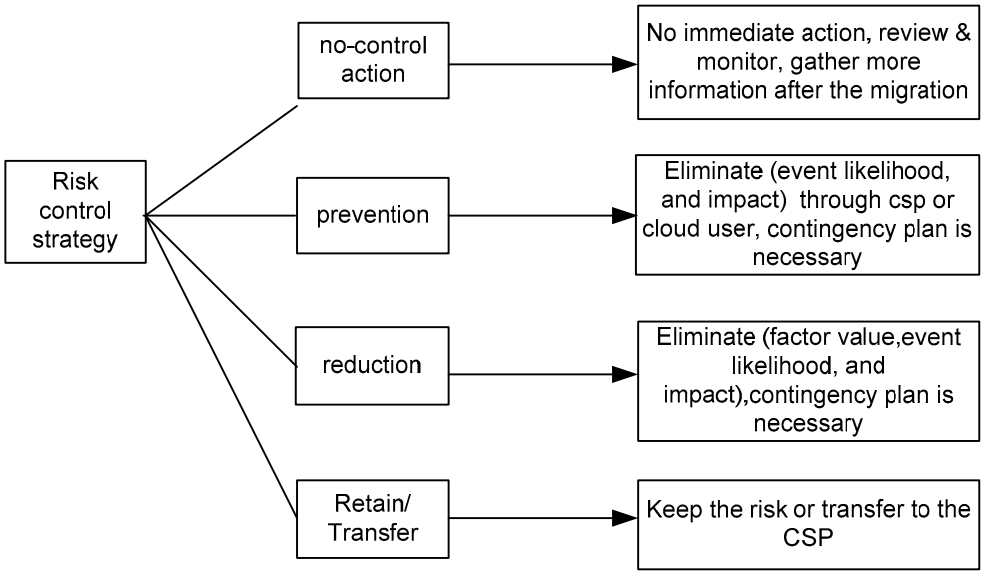

Figure 2. Risk treatment strategy in cloud computing.

Activity 4: Migration Decision and Risk Monitoring

This final activity makes the migration decision based on the assurance of control measures and monitors the risks if the migration decision is undertaken. Therefore, the complete risk register from the previous activities is a necessary input for this activity. The output from the activity mainly supports the migration decision by looking at the existing chosen cloud service provider offerings and monitoring the risk on certain interval. This activity consists of three tasks.

Task 4A: Assurance of Control Measures

A risk management framework to support cloud migration decision depends upon the effectiveness and completeness of control measures for risk mitigation. This step checks the CSP's capabilities to fulfill the identified control measures for the risks that are CSP responsibilities. The user should ask the potential CSPs to provide details about their existing controls or means by which they to mitigate the identified risks. A comparison can be made among the chosen potential CSPs on this occasion and chose the most appropriate one which has higher level of completion. Note that information can also be collected from the CSP's website and social commentary. Assurance checks the completion of control measures and assigns one of three levels:

- Level 1 No completion: There is zero or minimum evidence for the assurance of control measure attributes for managing the risks.
- Level 2 Partial completion: There is some evidence for the assurance of control measure attributes for managing the risks.
- Level 3 Full completion: There is adequate evidence for the assurance of control measure attributes for managing the risks.

Task 4B: Migration Decision

Our work advocates making the cloud migration decision based on the evidence for availability of risk control. This task considers how the cloud could support an organization in terms of risk control if the migration decision is taken. Full completion means adequate control measures for risk mitigation and adequate disclosure of security incident and policies. In such a case, the decision should be in favor of migration. In case of partial completion, the user should further analyze how to fulfill the necessary control measures for risk mitigation. In case of partial completion or no completion, the migration decision is not straightforward. In particular, further review with the key personnel of CSP service and SLA are necessary. Once the migration decision has been taken, it is necessary to define the migration strategy. The cloud migration strategy includes several parameters, such as migration size, hosting type, number of servers and license and bandwidth, candidate CSP, risk monitor, and roles and responsibilities.

Task 4C: Monitor Risks in Operation

This task monitors the existing risks to ensure that the risks are under control and identifies new risks upon completion of cloud deployment. New risk factors can emerge or the probability of existing factors can vary due to the evolution of cloud platforms, user requirements or amendments to the CSP's terms and conditions. User-migrated entities are in the operational phase throughout the risk monitoring. As shown in the procedure below, the probability of each risk factor is determined by its occurrence per monitored time. The monitored risk net value R_{netm} is then calculated similarly to the net risk calculation presented above. If R_{netm} is higher than R_{net}, we need to immediately revise the control strategy, otherwise further review is recommended for the next monitoring phase. It is a continuous task that monitors the status of the identified risks and control actions at regular intervals.

Risk monitoring procedure:

R_i = the identified risks
r_{i1} = risk factor
R_{netm} = monitored risk net value

For each identified risk R_i to be monitored R_{im}
Monitor the occurrence of related risk factors $r_{i1}, r_{i2}, \ldots\ldots r_{in}$
For each r_i,
$P(r_i)$ = no of occurrence/monitored time,
If ($R_{netm} \geq R_{net}$) then
Revise the existing control strategy with immediate action
If ($R_{netm} < R_{net}$) then no immediate action is required

4. The Risk Management Tool

We are currently developing a tool to support the automation of the presented risks management process. The aim is to reduce the human intervention, while performing the risk management activities through the tool support. Therefore, the tool provides a work flow to guide the users with the individual risk management activity, starting with defining migration profile through risk assessment to finishing migration decision and strategy. The tool can simultaneously be accessed and used by multiple users and produces output in Excel or PDF format from the individual activity. This section demonstrates the up to dated version of the tool.

4.1. Application Design

The entire application is written in Java 8 with a Web-based front end compatible to standard browser. The application user interface consists of a number of web pages which are associated with the relevant functionality to perform some task for managing the related information. Figure 4 shows the snapshot of application layout. Left hand side of the layout shows the four different activities of the process and Figure 3 also includes the migration profile information of the define migration profiles of the first activity. The users can also navigate in the workflow sequentially using pointed navigation buttons in the top right corner. The Web page content is presented in the centre of the screen with buttons for content related actions positioned on the right hand side. By clicking on "My profile" in the top left corner, the user can also access the profile information and messages associate with the user.

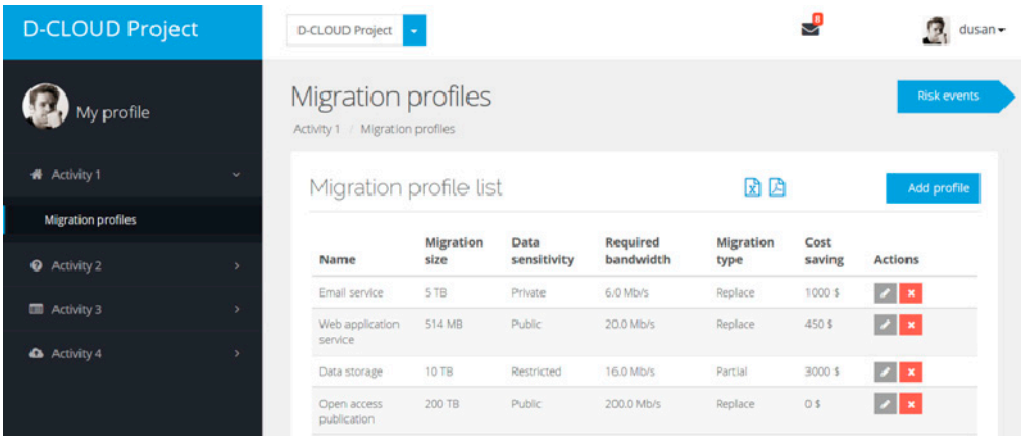

Figure 3. Application layout.

4.2. User Interface

There are several interfaces to support specific task within the activity of the process. Figure 4 shows the migration profile interface which allows the user to add the attributes' values for the profile. The user can also display the current migration profile list, update the information, and export the list into a PDF or Excel format.

Figure 5 shows interface that calculates the relative importance of the migration goal. The upper part of the Figure shows the comparison matrix table where user need to select the relative importance of a migration goal considering another goal with a scale 1–9 through the drop down list based on the migration context. Once the user presses the calculate weights button then the relative weight of individual goal is calculated and presented at bottom part of the interface. It also calculates the consistency ratio so that user can revise the comparison matrix value if the consistency ratio value is above the threshold.

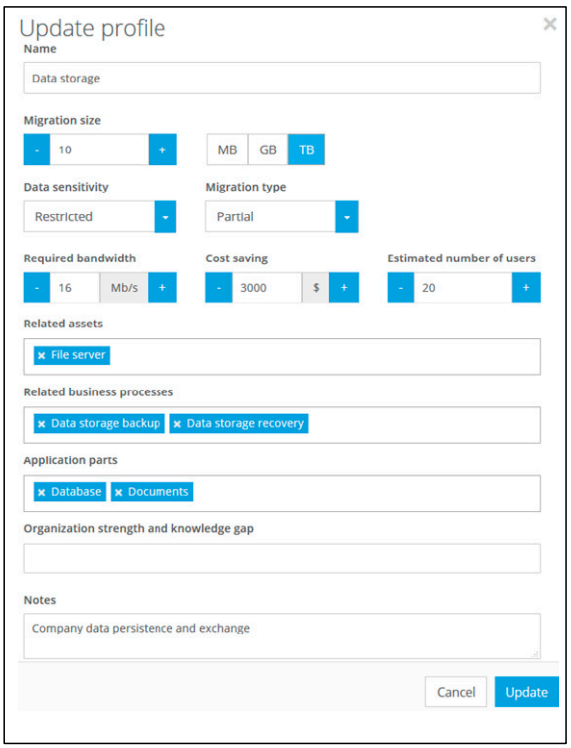

Figure 4. Migration profile interface.

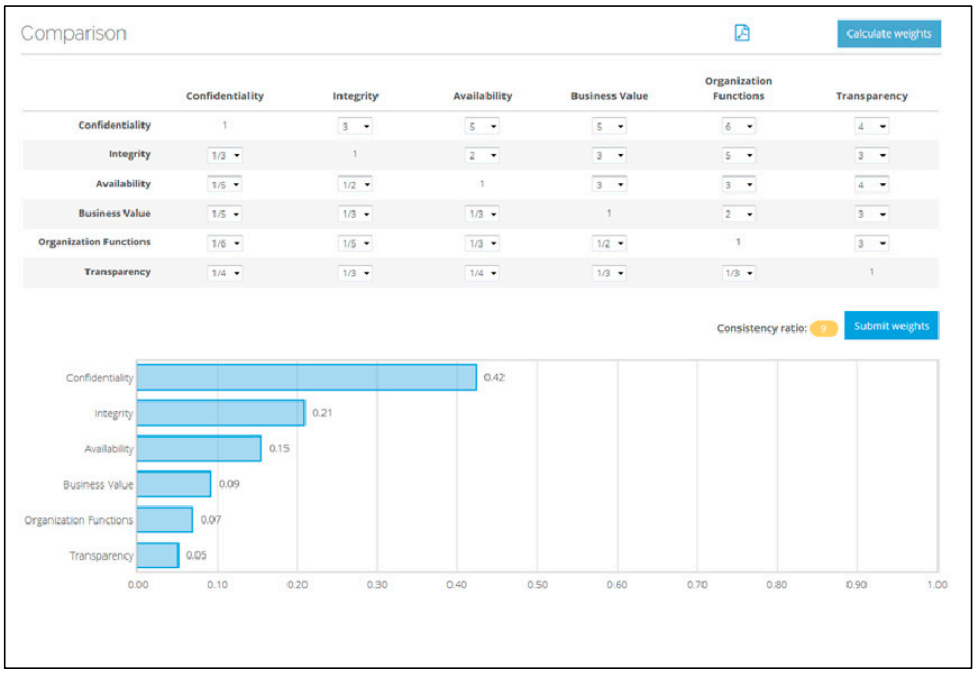

Figure 5. Relative importance of migration goal interface.

5. Evaluation

5.1. Study Design

We employed the proposed framework in a real-world example at Secure Business Austria (SBA) to demonstrate its applicability. We integrated the case study method with action research to demonstrate the applicability of the approach. However, selecting an appropriate research method for any empirical evaluation depends on several factors, such as availability of resources and

questions relating to the method and study context. We confirmed these factors before performing the study. Our case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context [29]. Action research makes an effort to provide practical value for real subject problems while simultaneously contributing to the acquisition of new theoretical knowledge [30]. Action research is particularly useful for this study as it contributes to understanding the risks involved in the cloud migration and supports SBA in making an informed migration decision. In this case, action research helps to solve a real problem. Figure 6 depicts the combined case study and action research design components. The research design considers typical design components such as study construct, data collection techniques and analysis, observation, action and conclusion. We perform an in-depth investigation of the SBA context by implementing the proposed risk management framework using the methods of case study and action research. The study concludes with observations, an informed migration decision, a comparison, and feedback for the fine-tuning of the framework.

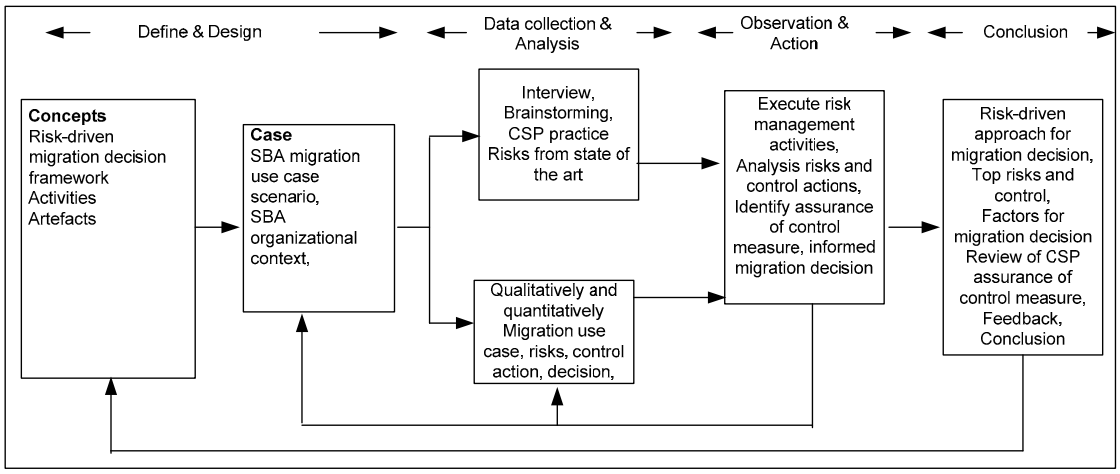

Figure 6. Study design details.

Study Construct and Data Collection

The goal of the study is to

- understand the usefulness of the risk management framework in supporting SBA in the migration decision;
- understand the risks associated with migrating the use-case scenario into the cloud;
- identify suitable CSPs that could address the risks and support the user in making the migration decision.

Data Collection and Analysis

The data collection began with a migration use case from SBA, followed by workshops and interviews with 10 key SBA users. The data was collected and carefully analyzed with a sequential explanatory strategy. The data collection began with a review of start-of-the-art works, use-case extraction, and a kick-off workshop, followed by the implementation of the risk management activities and artefacts generated from the activities. Finally, we obtained feedback about the proposed method from the key users through a list of open questions. The units of analysis mainly considered in the study were the risk management framework, the cloud migration decision and risk control actions. The collected data was analyzed both qualitatively and quantitatively based on the units of analysis. Quantitative analysis considered variables such as number of risk factors and risk events, complexity of determining net risk level, the number of control actions, migration decision, no of completion for the assurance measure by the CSP and risk monitoring. The qualitative analysis considered issues such as applicability of the risk-driven approach for the migration decision,

complexity of risk level, adequacy of the activities and artefacts, and comparison of risk factors with other studies.

Migration Use Case for the Study Context

SBA is a medium-size IT security research institute in Vienna [31]. The organization has a large number projects though collaboration with academic and industry partners focusing on various domains of IT security. It has more than 120 active researchers and 20 admin and IT staff to support achieving mission objectives. An enormous amount of storage is necessary to archive data and research outputs. The main partners of SBA are academic institutions such as universities in EU and non-EU countries, research institutions, private companies, and funding agencies. The migration use case is based on the data and infrastructure support. SBA's management is interested in reviewing this use case for possible cloud adoption. A brief description of the migration use case is given below.

Migration Use Case

SBA has an enormous amount of data related to various projects, which it also shares with partners. Collaborative work environments are quickly moving into the cloud environment for effective document exchange support. Currently, there are around 250 Windows-based virtual servers supporting the overall IT infrastructure of SBA. E-mail runs on an exchange server. The huge storage contains research data about previous and current projects, research proposals, penetration testing results of industry partners, audit data, and financial details. There is sensitive as well as public information in the overall storage. Data is the most critical asset for SBA's business, with a total effective storage of around 15 TB. The system infrastructure is deployed in the SBA main office located in Vienna. The existing Internet connection has a bandwidth of about 16Mbps and there is a secondary connection with 150 Mbps. There are 2 full time and 1 part time staffs working for overall IT support. Around 150 users use this network simultaneously for various purposes, mainly relating to their roles and responsibilities, locally and remotely. The total IT infrastructure maintenance cost for five years is € 50,000, and data size will triple from the current size, i.e., to 45 TB. SBA's strategic plan is to reduce the long term operational expense. In particular, the migration type focuses on migrating the existing collaborative applications such as Email, and document storage and sharing to cloud.

5.2. Introduction of Risk Management Process

Activity 1: Initialize Risk Management

The risk management team performed a kick-off workshop with the key SBA staff to initialize the risk management process. The first step of this activity was to define the migration profile by analyzing the migration scenario with the top SBA management. The risk management (RM) team had three members, one external, one internal and one management member. The team agreed that the six identified migration goals are important for any migration context. More specifically, SBA expects cost reduction, accessibility, and security as the top benefits of migration. The main user groups are internal and external researchers, office admins, management, IT and partner institutions' nominated staff. The migration use case is considered project of medium risk for the following reasons:

- There is no major amendment of applications involved in the migration profile;
- SBA staff has sound technical expertise; most have adequate security knowledge, and adequate in-house security controls are already implemented;
- Medium-sensitive organization data such as research data and research proposals are considered for the migration profile;
- Cost reduction, accessibility and secrecy of data are the most prioritized areas if the migration decision is taken.

The scope of risk management was considered by proactively controlled the identified risks or by obtaining accurate information relating to risk control actions before the migration decision is taken. The risk management schedule was considered in the migration decision and it was decided that risk monitoring would be a continuous activity if the decision was taken for the cloud migration.

Activity 2: Analyze and Control Risks

This activity assessed the identified risks from the previous activity so that appropriate control actions could be identified. The RM team members mainly used their experience to determine the likelihood and impact of the risks and associated factors. The team also agreed on the relative importance of the migration goals. Table 2 shows the results of comparison matrix. Each goal is compared with another goal based on its importance within the organizational cloud migration context. The higher the weight value of a goal implies it is more important than the other comparing goal. The scale of the comparison matrix is between 1 and 9. If two goals are equally importance then the value should be 1, otherwise value should be 3, 5, 7, 9 if the goal is moderate, strong, very strong, and extreme importance comparing to the other goal. There are intermediate values such 2,4,6,8, within these scales. For instance, Business Value (BV) is more importance than Integrity, which is why the BV value is assigned to 5. Once all comparison matrix values are obtained then it is added together and normalized to determine the relative importance of individual goal. The RM team compared and agreed the comparison matrix values as shown in Table 2. Business value obtained highest importance (0.32) for this migration context followed by confidentiality and organization function. This is because cost saving is the main motivation for this cloud migration context. Research outputs are the main data that are considered to be migrated hence confidentiality is considered the second prioritized goal. We also need to calculate the consistency ratio for identified comparison matrix values to confirm that the values are consistent for the context. In our case, the identified consistency ratio is 3.45%, which is less than 10%. Therefore, the assumptions for the relative importance of the migration are relevant for the context. After obtaining the relative weight, we had to calculate the net risk value. We show the calculation for risk R1; the net values for the other risks were calculated analogously.

Table 2. Comparison matrix.

	BV	**OF**	**C**	**I**	**A**	**T**
BV	1	3	1	5	3	5
OF	$\frac{1}{3}$	1	1	3	3	5
C	1	1	1	3	3	3
I	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{3}$	1	$\frac{1}{3}$	1
A	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	3	1	1
T	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{3}$	1	1	1
Sum	3.06	5.9	4	16	11.3	16

- Relative Weight of BV $= \frac{1}{6}\sum BV = 0.32$
- Relative Weight of OF $= \frac{1}{6}\sum OF = 0.22$
- Relative Weight of C $= \frac{1}{6}\sum C = 0.25$
- Relative Weight of I $= \frac{1}{6}\sum I = 0.06$
- Relative Weight of A $= \frac{1}{6}\sum A = 0.09$
- Relative Weight of T $= \frac{1}{6}\sum T = 0.06$

Consistency Ratio(CR) = 0.0345

Activity 3: Identify and Categorize Risks

This activity included the interviews with the selected eight SBA staff members and two staff members of partner organizations. The responses to the interview provided a raw list of risk factors that was refined further. Furthermore, SBA's existing risks from other projects were also taken into consideration. The risks were from all categories, including organization, technical and business risks. Data protection is one of the main concerns for SBA. Migration difficulties are not a risk for SBA as the internal staff has adequate expertise in cloud technology and adaption actions. The risks were then linked with the associated risk factors as shown in Table 3.

Net Risk R1 (Leakage of Research Data) Calculation

$P(r_1$ = long-standing access by CSP-internal employee) = 0.8
$P(r_2$ = malicious attack by impersonating to misuse and modify service instance) = 0.7
$P(r_3$ = VM vulnerabilities) = 0.2
$P(r_4$ = misuse by SBA-internal user) = 0.1
Impact of R1 = 0.8

Affected migration goals = BV, OF, C, I, T

$r_1 = 0.8 \times 0.8 = 0.64$
$r_2 = 0.7 \times 0.8 = 0.56$
$r_3 = .2 \times 0.8 = 0.16$
$r_4 = 0.1 \times 0.8 = 0.08$
$R_1 = \frac{1}{4}\ (0.64 + 0.56 + 0.16 + 0.08) = \frac{1}{4}\ (1.44) = 0.36$
Net risk $R_1 = 0.32 \times 0.36 + 0.22 \times 0.36 + 0.25 \times 0.36 + 0.06 \times 0.36 + 0.06 \times 0.36 = 0.327$

Table 3. Risk details.

Risk Factors	Risk	Category	Affected Goals	Net Risk
Long-standing access by CSP-internal employee, malicious attack by impersonating to misuse and modify service instance, VM vulnerabilities, misuse by SBA-internal users	R_1 = Leakage of research data (research output/research proposals)	Organization, Technical	BV, OF, C, I,T	0.33 (Critical risk)
Inaccurate usage estimation, uncertainty of cloud billing due to price change, poor SBA reputation due to cloud migration	R_2 = Financial loss	Business	BV,OF	0.32 (Critical risk)
CSP instability and lack of customer support, unavailability of data, lack of disaster recovery and business continuity plan by SBA/CSP, inconsistencies between SBA and CSP policies	R_3 = Interruption of organizational functionalities	Organization	BV,OF,A,T	0.60 (Highly critical risk)
Lack of audit support by CSP, poor transparency of SBA data access, unclear SBA policies for controlling data in the CSP infrastructure, attacker gains control over the SBA's service instance	R_4 = Loss of control /CSP dependency for the business continuity	Organization	BV,OF,C,I,A,T	0.287 (Low risk)
Poor flexibility of data access, resource exhaustion, availability reduction.	R_5 = Data unavailability	Organization, Technical	BV,OF,A	0.30 (Critical risk)

Identify Potential Risk Controls

The RM team agreed that it was necessary to control the identified risks and associated factors or to at least obtain evidence on how the CSPs handle such risks. The interruption of organizational functionalities was one of the highly critical risks for SBA. Therefore, selection of a stable CSP is essential so that appropriate service can be obtained from the provider. Some of the control actions are outside SBA's control and depend on the CSP for the implementation, such as physical security of the data center, data loss/leakage prevention, and audit report. SBA also needed to review the existing disaster recovery and business continuity plan. The list of control actions and associated responsibilities is given below:

- C1 (Data leakage prevention): encryption of data at rest and in transit, restricted standing access, monitor privileged data access; CSP
- C2 (Physical security): physical security of CSP's data center; CSP
- C3 (Data loss prevention): data loss prevention mechanism; CSP
- C4 (Data transparency): appropriate dissemination of information about data access specifically by the CSP's internal staff; CSP
- C5 (Stable CSP): cloud vendor should not go out of business; CSP
- C6 (Audit program and report): appropriate governance and audit management program, CSP audit report; CSP
- C7 (Security incident report): CSP security incident report; CSP
- C8 (Policy): access control with privileged access, disaster recovery and business continuity plan by CSP; CSP
- C9 (Customer service): real-time customer support service; CSP
- C10 (Penetration testing): SBA should perform penetration testing with the knowledge of the CSP; SBA
- C11 (Policy amendment): extend SBA's existing access control, disaster recovery and business continuity to adjust to cloud-based dependencies; SBA
- C12 (Usage estimation): accurate usage estimation based on the existing and future need of SBA; SBA
- C13 (Usage monitor): tools to monitor usage; SBA
- C14 (Testing): necessary testing to confirm that the service, control process, and VM are functioning and protected from risks; SBA

Activity 4: Migration Decision and Risk Monitor

The previous activity identified 14 control actions. This activity identified the potential CSPs that match the SBA migration profile so that completeness can be checked for risk control. The feasible solution for SBA's migration profile is IaaS. There are several CSPs who can support this migration context and we compare their offering in terms of the identified control measures. Two CSPs are chosen which are better offerings than others and more reputable. However, there is also the possibility of choosing free cloud storage infrastructure. However, such a service does not have a dedicated customer support service. If there is any interruption of service, it would be difficult to solve the problem in real time. Therefore, such a service is not suitable for SBA users for reasons of business continuity.

Assurance of Control Measures

This step identifies the assurance of control measures from the two potential CSPs by collecting evidence from the relevant sources as shown in Table 4.

Table 4. Assurance of controls for the two CSPs.

Control Measure	CSP A	CSP B
C1	Data encryption at rest and in transit using BitLocker and SSL/TLS encryption; CSP partner could access the data only by obtaining consent from the user; Admin access is strictly controlled Standing access is strictly checked before authentication.	Users have complete control of the instance and virtual networking environment; Encrypted IPsec VPN connectivity besides HTTPs using secure socket layer through API end points; Protection against traditional network security issues such as DDoS, MITM, spoofing; Encrypted data storage using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys. There are several security flaws relating to data leakage identified by different research
C2	Physical access control is in place but no details available	Physical access control is strictly implemented at the perimeter; security staff utilizing video surveillance, intrusion detection systems, and other electronic means; Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.
C3	DLP prevention features are included while users are sending sensitive data; Data encryption at rest and in transit using BitLocker and SSL/TLS encryption; CSP partner could access the data only by obtaining consent from the user; Admin access is strictly controlled; Isolation between tenants; But no clear evidences on what technologies are really used for leakage prevention.	Users have complete control of the instance and virtual networking environment; Encrypted IPsec VPN connectivity besides HTTPs using secure socket layer through API end points; Protection against traditional network security issues such as DDoS, MITM, spoofing; Encrypted data storage using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
C4	Discloses the location of data and who is accessing the data	AWS audit trial provides log of user activities
C5	CSP B is a reputable institution	CSP A is a reputable institution
C6	Third-party audit is performed to comply with ISO27001 certification, NIST 800-53, HIPAA BAA and SSAE16 SOC1 Type II	CSP A compliance program provides evidence of robust security and complies with ISO 27001 certification, SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), PCI DSS Level 1, FIPS 140-2; Users can also deploy solutions that comply with HIPAA or Cloud Security Alliance (CSA)
C7	No evidence	No evidence but CSP B claims that it will notify publically if applicable
C8	Strong access control using RBAC and lockbox and physical security, several back up of users' data in different locations; No evidence of disaster recovery and business continuity plan	High-level availability of data in various global locations; industry-standard diagnostic procedures to drive resolution of incidents
C9	Dedicated real-time customer support service	Dedicated real-time customer support service
C10	No evidence	Permits users to perform penetration testing of its resource through an official procedure

Migration Decision

Based on the assurance of control measures after reviewing two CSPs, we summarized several evidences based on the controls. In general, both CSPs have integrated possible mechanisms for controlling the identified risks. There is adequate evidence for protection against data leakage, but there are findings in recent research relating to possible vulnerabilities for data leakage of CSP B. Most of the risk factors for the highly critical risk, i.e., interruption of organizational functionalities, are ranked as partial completions. This is due to the fact that there is a lack of evidence for the business continuity plan and it is difficult to match SBA and CSP policies due to a lack of information. However, these factors could be resolved in the course of the migration through an appropriate service-level agreement. CSP A does not have any evidence that it allows users to perform penetration testing or provides security incident reports. CSP B claims that, if applicable, a vulnerability report will be published, however, there are no clear statements on this issue. Therefore, CSP A has no completion for C7 and C10, partial completion for C3, and full completion evidences for C1, C2, C4, C5, C6, C8, C9. In case of CSP B, there is no completion for C7 and partial completion for C3. However, as mentioned previously, several security flaws have been discovered in CSP B's infrastructure. The RM team recommended CSP A as a suitable CSP considering the SBA context.

The recommendation makes sense to the SBA management, however they would also like to understand the risks and associates control support the fulfillment of the top prioritized goals, i.e., business value and confidentiality. Interruption of organizational functionalities and leakage of research data are the top ranked risk. Therefore, it is necessary to understand whether the assurance of in-house and CSP controls sufficiently reduce the likelihood of the risks and impacts to be materialized. There are several controls identified for the risk mitigation such as data leakage prevention, data loss prevention, policy amendment, stable CSP and customer support. Some of these controls are already given full assurance from the cloud service provider. However, policy amendment is under the SBA responsibility. Therefore, the management final decision follows the RM team recommendation for the cloud migration.

Risk Monitoring

As the decision is taken for migration, monitoring activity should initially take into consideration the risk factors that do not have adequate evidence of control, such as transparency of security incident reports, mapping SBA and CSP policy, mechanisms for data leakage prevention and penetration testing. Furthermore, it should be mentioned that once the migration has taken place, SBA users' new requirements should be taken into consideration. SBA users should not ignore their individual IT responsibilities even though their data is managed by the selected CSP. Mitigating risk factors relating to financial loss is mainly a responsibility of SBA rather than of the CSP. Therefore, appropriate controls are necessary to monitor the usage and SBA's IT team should forecast the accurate usage once the cloud is deployed. Finally, SBA should also revise the existing policies to match the CSP policies.

6. Discussion

The risk management framework was helpful to SBA in assessing the risks and making an informed cloud migration decision. It provides a comprehensive analysis of risks from various dimensions relevant to the studied context. Several observations can be made based on the studied evaluation:

6.1. Applicability of the Framework

Risk-driven approach for cloud migration decision: The integration of the risk management approach into the cloud migration decision provides an early warning of the possible risks that could outweigh the expected migration benefits. There is a strong dependency between risks and the migration decision. Therefore, our approach makes the stakeholders aware that necessary actions need to be considered for controlling all the risks. The process is systematic and covers all areas from

a holistic perspective for the risk identification. In particular, it evaluates the impact of cloud-related risks on business values, organization functions and other technical areas. A semi-quantitative risk analysis technique is followed to determine the net risk value. The study results show that it is a reasonably applicable technique and can effectively support the cloud migration decision.

Risk management process: Based on the responses to the interview, the underlying activities of the process are operational and adequate. The process begins with a migration profile, so risk management plan and risk identification should be clearly linked to the migration profile. The risk assessment technique follows the prioritized migration goals so that net risk values are influenced by the relative importance of migration goals. The artefacts produced by the activities are mainly textual; however, they provide a clear view of the migration profile, risk details and assurance of control measures. Therefore, the process is systematic and the artefacts are reasonably applicable to any context to support the risk management and migration decision.

Influential factors for the migration decision: Our study observed that migration goals, risks and their control are influential factors for cloud migration. The identified six migration goals are generally applicable to any context but the relative importance of these goals is important and necessary for the migration context. Risks are the obstruction of these goals and net risk values are influenced by these goals. From the studied context, the goals and their relative importance make it easy to rationalize the motivation for migration. It is critical to identify, analyze and control the risks relating to cloud migration before any migration decision is taken. These risks directly obstruct the fulfilment of the migration goals. For instance, in the studied project, interruption of organizational functionalities and data leakage are two critical or highly critical risks that obstruct goals like business value, organization function and confidentiality. SBA would not make any migration decision until there is an adequate assurance of control actions for risk mitigation.

6.2. Comparison with Other Study Results

We compare the results of our study and framework with other study results from the literature. The proposed risk-driven framework for cloud migration decision is a comprehensive approach compared to the other works. For instance, in [7], Saripali and Walters propose a QUIRC security risk management framework, which only focuses on the risks, but it is not clear how the risks need to be identified and assessed. Fit´o et al.'s business level objective-driven semi-quantitative cloud risk assessment approach only considers the business level objective and lacks consideration of technical and non-technical risks [11]. None of the work provides a systematic risk management process and links the risk assessment with the migration goals. Our work identifies and compares the existing CSP offers for risk mitigation, hence allowing user to perform an in-depth analysis for the migration decision.

In terms of identified risks, our results and those discussed in existing literature have one thing in common at least in part. Khajeh-Hosseini et al. identified dependency on a third party and deterioration of customer care and service quality as the top risks [26]. Khosravani et al. are also concerned about the loss of control over sensitive data, lack of customer support and skill, and lock-in [25]. These results are fully or partially similar to our findings. However, risks such as resource exhaustion, service unavailability and portability, as identified by Samad et al. in [8] in a cloud based e-health application context, decrease in satisfying work, and department downsizing identified as by Khajeh-Hosseini et al. in [26] are not similar to our studied context. We also identified some unique risk factors such as inconsistencies between SBA and CSP policies, lack of disaster recovery and business continuity plan by SBA, potential poor reputation of SBA due to cloud migration, lack of audit support by CSP, and poor transparency of SBA data access that were not mentioned by the other studies. Organization functionality is the top risk in our context, which also does not match any other work.

Most of the risks are due to the fact that users do not have control over the CSP's infrastructure. For instance, standing access to data by CSP-internal users for administrative reasons is a critical risk factor in a cloud environment unless the CSP explicitly declares how it restricts admin user access. Based on the case study, there are also factors that are influenced by the cloud user's context, for

instance usage estimation, keeping track of overall usage, and extension of the policies to adjust to the cloud-based dependencies. Therefore, managing some of the risks is the joint responsibility of both CSP and user. Furthermore, these responsibilities vary depending on the type of deployment model chosen. We concluded that risks in cloud computing mainly depend on the specific migration scenario and organization context. Furthermore, users must not ignore their own IT responsibilities despite cloud migration.

6.3. Limitations of the Framework

We have identified three main limitations based on the studied context regarding the framework. Firstly, risk assessment is influenced by six main migration goals in our example; however, if the number of goals were to increase, the net risk level estimation would be more complex. However, we advocate considering only the highly prioritized goals, if the number of goal increase. Secondly, the studied project compares two CSP offers; however, it is not easy to make the final choice, as both CSPs' offer could be suitable for the SBA context. The active involvement and consensus of key staff is necessary in this case, in addition to a service-level agreement. Finally, in the studied project, the risk monitoring activity was not performed, as the decision for the CSP had not been made yet when the study was performed. Without looking at the monitoring activity, it is difficult to analyze the identified risks and their evolution.

6.4. Study Validity

We tried to reduce the expectation bias on the case study result. As the principal investigator is an external researcher, it helps to reduce the bias of the studied results. The studied context is from a single case, therefore there is a possibility of expectation bias and the identified results cannot be generalized. To overcome the generalization limitation, the study results were compared with other results from the literature. The comparisons confirmed several commonalities of risks as well as unique factors found in the studied context. In terms of construct validity, the interviewed staff have adequate IT and security knowledge due to their domain expertise. Furthermore, we also conducted a kick-off workshop to provide the details of the proposed framework. Therefore, all participants clearly understood the terms being used.

7. Conclusions

Cloud computing brings new opportunities, but at the same time there are many challenges involved that could pose various risks. It is not unexpected that we are seeing new risks for cloud-based systems. Risk management is certainly critical for analyzing the risks and offers realistic plans for risk control and business continuity. An effective risk management process should be an integral part of the cloud migration decision and protects the stakeholder from financial loss due to cloud adaption. Our work contributes to filling the gap in the existing literature by providing a comprehensive and well-structured risk management framework. We propose a risk-driven approach for supporting the cloud migration decision. Results from risk management support the migration decision and protect users' migrated resources from threats. To demonstrate the applicability of the work, we applied the framework to a real migration use case with very promising results. The results show that the risk-driven approach provides early warning about the issues that need adequate attention before making the migration decision. The framework considers six main migration goals and prioritizes the goals based on the migration context. Risks are analyzed using a semi-quantitative approach and influenced by the migration goals to provide accurate risk levels. The results of the risk management activities were directly incorporated into the studied context. We have noted the experience and insights gained and lessons learned as well as limitations of the case study. We also compare the identified risk factors from the study with other study results to generalize our findings. However, a single case study is not an adequate basis for generalization and determining the framework's applicability. More case studies are necessary to validate the framework. We are currently working on defining a guideline for risk management activities along

with a checklist so that the framework could provide better hands-on support to potential cloud users. We are also planning to develop migration goals and a risk taxonomy and integrate it with the guidelines. Our future direction will be dedicated to these aims.

Acknowledgments: This work is financed by the Austrian Science Fund (FWF) project no. P26289-N23. The authors would like to thank the SBA staff for support with the evaluation part.

Author Contributions: Shareeful Islam carried out the background work and developed the risk management method based on the review of the state-of-the-art works. He also initial drafted the manuscript with Stefan Fenz. Stefan Fenz supported the initial draft and with the evaluation part. Edgar Weippl contributed with the evaluation part and review of the risk management method. Haralambos Mouratidis contributed by reviewing the whole paper and finalizing the conclusion and abstract. All authors contributed to the write up and review and have approved the paper manuscript.

Conflicts of Interest: The authors declare that there is no conflict of interest.

References

1. Kalloniatis Christos, Haralambos Mouratidis, Manousakis Vassilisc, Shareeful Islam, Stefanos Gritzalis, and Evangelia Kavaklif. "Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts." In *Computer Standards & Interfaces*; Elsevier, Amsterdam, Netherlands, 2014.
2. Mouratidis Haralambos, Shareeful Islam, Christos Kalloniatis, and Stefanos Gritzalis. A framework to support selection of cloud providers based on security and privacy requirements. *Journal of Systems and Software* 86 (2013): 2276–93.
3. Gruschka Nils, and Luigi Lo Iacono Vulnerable Cloud: SOAP Message Security Validation Revisited. Paper presented at the IEEE International Conference on Web Services, Los Angeles, CA, USA, 6–10 July 2009.
4. Shareeful Islam, Haralambos Mouratidis, Edgar Weippl. A Goal-driven Risk Management Approach to Support Security and Privacy Analyzes of Cloud-based System. In *Security Engineering for Cloud Computing: Approaches and Tools*; IGI Global Publication, Hershey, PA, USA, 2012.
5. Kalloniatis Christos, Haralambos Mouratidis, and Shareeful Islam. "Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements." In *Requirements Engineering Journal (REJ)*. Springer-Verlag, Berlin, Germany, 2013, vol. 18, pp. 299–319.
6. Ristenpart Thomas, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. Paper presented at the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
7. Saripalli Prasad, and Ben Walters. Quirc: A quantitative impact and risk assessment framework for cloud security. Paper presented at the IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5–10 July 2010.
8. Samad Javeria, Seng W. Loke, and Karl Reed. Quantitative Risk Analysis for Mobile Cloud Computing: A Preliminary Approach and a Health Application Case Study. Paper presented at the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Melbourne, Australia, 16–18 July 2013.
9. Zhang Xuan, Wuwong Nattapong, Li Hao, and Zhang Xuejie. Information security risk management framework for the cloud computing environments. Paper presented at the 10th IEEE International Conference on Computer and Information Technology (CIT), Cork, Ireland, 29 June–1 July 2010.
10. *ISO 31000:2009 Risk Management Principles and Guidelines*. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Geneva, Switzerland, 2009.
11. Fitó J. Oriol, Mario Macías, and Jordi Guitart. Toward Business-driven Risk Management for Cloud Computing. Paper presented at the IEEE international conference on Network and Service Management (CNSM), Niagara Falls, ON, Canada, 25–29 October 2012.
12. Fitó, J. Oriol, Mario Macías, Ferran Julia, and Jordi Guitart. Business-Driven IT Management for Cloud Computing Providers. Paper presented at the IEEE 4th International Conference on Cloud Computing Technology and Science, Taipei, Taiwan, 3–6 December 2012.
13. Sailesh Gadia, Cloud Computing Risk Assessment a Case Study. *ISACA Journal* 4 (2011): 2011.

14. ENISA_Survey. "A SME Perspective on Cloud Computing Survey, The European Network and Information Security Agency. 2009." Available online: https:/www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-sme-survey (accessed on 24 March 2016).
15. Umar Ismail, Shareeful Islam, Moussa Ouedraogo, Edgar Weippl , A Framework for Security Transparency in Cloud Computing, *Journal of Future Internet* 8 (1), 2016.
16. Greg Stone, Pierrre Noel, Cloud Risk Decision Framework, Microsoft. Available online: download.microsoft.com/documents/australia/ .../smic1545_pdf_v7_pdf (accessed on 01 April 2016).
17. Warren Chan, Eugene Leung, and Heidi Pili. *Enterprise Risk Management for Cloud Computing*, https://www.coso.org/Documents/Cloud-Computing-Thought-Paper.pdf, 2012 (accessed on 01 April 2016).
18. Robert Lemos. "5 Lessons from Dark Side of Cloud Computing. CIO. 2009." Available online: http://www.cio.com.au/article/314110/5_lessons_from_dark_side_clo ud_computing?eid=-156 (accessed on 26 February 2016).
19. Catteddu Daniele. "Cloud15 Computing: Benefits, Risks and Recommendations for Information Security. 2009." Available online: http//www.enisa.europa.eu/act/rm/files/deliverables/cloud.../at.../fullReport (accessed on 24 January 2016).
20. Michael Gregg. "10 Security Concerns for Cloud Computing, Global Knowledge Training LLC. 2010." Available online: http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf (accessed on 23 March 2016).
21. Shareeful Islam, Stefan Fenz, Edgar Weippl, and Christos Kalloniatis. Migration Goals and Risk Management in Cloud Computing: A Review of State of the Art and Survey Results on Practitioners. *International Journal of Secure Software Engineering (IJSSE)* 7 (2016): 44–73.
22. Marianthi Theoharidou, Nick Papanikolaou, Siani Pearson, and Dimitris Gritzalis. Privacy Risk, Security, Accountability in the Cloud. Paper presented at the IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), Bristol, UK, 2–5 December 2013.
23. Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Over-encryption: Management of access control evolution on outsourced data. Paper presented at the 33rd international conference on Very large databases, Vienna, Austria, 23–27 September 2007.
24. Siani Pearson. Taking account of privacy when designing cloud computing services. Paper presented at the ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, BC, Canada, 23 May 2009.
25. Amir Khosravani, Brian Nicholson, and Trevor Wood-Harper. A case study analysis of risk, trust and control in cloud computing. Paper presented at the IEEE Science and Information Conference, London, UK, 7–9 October 2013.
26. Ali Khajeh-Hosseini, David Greenwood, and Ian Sommerville. Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. Paper presented at the IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5–10 July 2010.
27. *ISO 27001:2013 Information Technology—Security Techniques—Information Security Management Systems—Requirements*. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Geneva, Switzerland: 2013.
28. Thomas L. Saaty. Decision making with the analytic hierarchy process. *International Journal of Services Sciences (IJSSCI)* 1 (2008): 83–98.
29. Robert K. Yin. *Case Study Research: Design and Methods*. SAGE Publications Inc., Oaks, CA, USA, 2003.
30. Davison, R.M.; Martinsons, M.G.; Kock, N. Principles of canonical action research. *Information Systems Journal* 14 (2004): 65–86.
31. SBA. "Secure Business Austria. 2015." Available online: http://www.sba-research.org/research/ (accessed on 01 April 2016).