Rahman, Alifah Aida Lope Abdul; Islam, Shareeful; Kalloniatis, Christos; Gritzalis, Stefanos

Article

A risk management approach for a sustainable cloud migration

Journal of Risk and Financial Management

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Rahman, Alifah Aida Lope Abdul; Islam, Shareeful; Kalloniatis, Christos; Gritzalis, Stefanos (2017) : A risk management approach for a sustainable cloud migration, Journal of Risk and Financial Management, ISSN 1911-8074, MDPI, Basel, Vol. 10, Iss. 4, pp. 1-19,
https://doi.org/10.3390/jrfm10040020

This Version is available at:
https://hdl.handle.net/10419/238845

Journal of
Risk and Financial Management

MDPI

Article

A Risk Management Approach for a Sustainable Cloud Migration

Alifah Aida Lope Abdul Rahman [1,*], Shareeful Islam [2,*], Christos Kalloniatis [3] and Stefanos Gritzalis [3]

[1] National Audit Department, Persiaran Timur 3, 71760 Bandar Baru Enstek, Negeri Sembilan, Malaysia
[2] School of Architecture, Computing and Engineering, University of East London, London E16 2RD, UK
[3] Department of Information and Communication Systems Engineering, University of the Aegean, Mytilene 81100, Greece; chkallon@aegean.gr (C.K.); sgritz@aegean.gr (S.G.)
* Correspondence: aida@audit.gov.my (A.A.L.A.R.); shareeful@uel.ac.uk (S.I.); Tel.: +60-388-899035 (A.A.L.A.R.); +44-208-2237273 (S.I.)

Received: 26 September 2017; Accepted: 30 October 2017; Published: 9 November 2017

Abstract: Cloud computing is not just about resource sharing, cost savings and optimisation of business performance; it also involves fundamental concerns on how businesses need to respond on the risks and challenges upon migration. Managing risks is critical for a sustainable cloud adoption. It includes several dimensions such as cost, practising the concept of green IT, data quality, continuity of services to users and clients, guarantee tangible benefits. This paper presents a risk management approach for a sustainable cloud migration. We consider four dimensions of sustainability, i.e., economic, environmental, social and technology to determine the viability of cloud for the business context. The risks are systematically identified and analysed based on the existing in house controls and the cloud service provider offerings. We use Dempster Shafer (D-S) theory to measure the adequacy of controls and apply semi-quantitative approach to perform risk analysis based on the theory of belief. The risk exposure for each sustainability dimension allows us to determine the viability of cloud migration. A practical migration use case is considered to determine the applicability of our work. The results identify the risk exposure and recommended control for the risk mitigation. We conclude that risks depend on specific migration case and both Cloud Service Provider (CSP) and users are responsible for the risk mitigation. Inherent risks can evolve due to the cloud migration.

Keywords: sustainability; cloud migration; risk analysis; degree of belief; risk exposure; and Dempster-Shafer (D-S) theory

1. Introduction

The benefits for using cloud computing services are already well documented and are mostly related to resources sharing, on-demand self-services, rapid scalability, improved economies of scale and collaboration (Kalloniatis et al. 2013; Khajeh-Hosseini et al. 2011). Despite of several benefits, there are risks that could outweigh the expected benefits of cloud migration. In particular, customers are concerned about the control of data, hidden and migration cost undisclosed incidents and continuity of service. When migrating to cloud, potential cloud users are expecting that cost for migration is reasonable level with no hidden cost, service and maintenance from third party should be at an expected level. In reality, decision for cloud migration is influenced by several factors that contribute for or against it such as financial support, security, continuity of services, data leakage efficiency and maintenance (Mastroeni and Naldi 2011; Islam et al. 2016, 2017). Therefore, it is necessary to understand whether cloud is a sustainable or non-sustainable solution for the business. Sustainability has become strategic important for the Information System (IS) and cloud domain due to focus on resource and energy savings and to address the needs of internal and external stakeholders through the balancing

economic, environmental and social aspects (Müller et al. 2011). In the scope of sustainable cloud computing, Müller et al. (2011) emphasised that sustainability should include quality criteria, adequate protection for organisation's data, and flexibility of a disaster management. Due to these aspects, sustainability can be used as additional support to the existing controls provided by the management.

The novel contribution of this paper is a risk management approach that systematically assesses and manages risks to support users with a sustainable cloud migration. There are uncertainties involved from all aspects of cloud and risks posed by these uncertainties need appropriate assessment (Wang et al. 2014; Sunyaev and Schneider 2013; Puthal et al. 2015). Our work contributes to develop a risk management approach for sustainable cloud migration. This paper is an extension of our previous work that focused on sustainability issues for cloud migration (Rahman and Islam 2015). The risks are identified based on four sustainable dimensions and analysed using Dempster-Shafer (D-S) theory. The reason for considering D-S theory is that it deals with uncertainty or incomplete information and combines multiple evidences for determining degree of belief. Furthermore, it is hard to obtain historic data in cloud computing to determine risk event probability. Therefore, individual belief is important on this occasion to determine the probability and impact of risk. To demonstrate the applicability of our work, we consider a real migration use case from the Malaysia Ministry of Health. The main goal is to validate the proposed approach and evaluate its effectiveness on supporting potential users for undertaking a cloud migration decision of selected services.

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 sustainable dimensions 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

This section presents a number of research efforts related to the proposed approach. Specifically it presents respective works that focus on sustainability issues for information system and risks management in cloud computing.

2.1. Sustainable Information System (IS) and Cloud

Sustainable IS has been discussed within several areas; IS projects (Silvius et al. 2009), development of IT strategic plan (Harmon and Demirkan 2011) and cloud computing (Müller et al. 2011). These studies imply that sustainability is mainly involved in the long-term strategy of an IS for creating innovation, improve operational activities, improve quality of information and service. In this sense, the incorporation of sustainability into business process becomes important to accomplish the changing demand from the key users and also for decision-making purposes (Asif et al. 2013). In (Yi et al. 2012) authors claim that from the cloud computing perspective sustainability is achieved as long as the system is able to perform according to specific computational quality characteristics such as disaster management flexibility, service availability, adequacy of specific security features and in parallel connectivity stability among cloud distribution in order to enhance specific performance goals. It is also suggested that in order to achieve proper cloud design, deployment, migration and services, organisations may apply the Cloud Computing Business Framework for measuring cloud business performance as well as for improving specific business functions (Chang et al. 2011).

2.2. Risks Management in Cloud Computing

In practice, control mechanisms are provided by the organisation to ensure that migrating to cloud is secured, timely and meet user's requirements. Therefore, organisation needs to consider the internal and external risks that the cloud migration potentially exposed to. A number of researches have discussed risk management in cloud computing including areas such as security, cloud architecture, regulatory compliance, data location, disaster recovery and provider lock in

(Silvius et al. 2009). Zhang et al. in (Zhang et al. 2010) developed a risk management framework for cloud computing covering all cloud service models and cloud deployment models (Zhang et al. 2010). The authors emphasised on enterprise security risk, which include incident management, application security, identity and access management, portability and interoperability. Alternatively, in (Madria and Sen 2015) authors proposed an off-line risk assessment framework for cloud service providers (CSP). They developed an off-line risk assessment framework to evaluate the security of CSP according to the threats presented when specific applications are migrated to the cloud. The proposed framework consists of three modules; mission oriented risk assessment, cloud service provider risk assessment and cloud adoption strategies. In conjunction with CSP, in (Morin et al. 2012) authors proposed to conduct Service Level Agreement (SLA) risk management as a basis to improve governance, risk and compliance in cloud computing environments. Risk may be partially transferred to the CSP (via SLA) but the residual risk still needs to be assessed (Theoharidou et al. 2013). This requires the organisation to develop new risk profile and to consider other threats that may be posed by the CSP. In relation to cloud risk assessment, ENISA in (ENISA 2009) provides guidance on the assessment of cloud risks and benefits for potential and existing users of cloud computing which include audit and SLA assessment. Basically, the role of risk management in cloud migration is performed in order to identify the most important risks associated to a specific organisation, to provide information to a decision maker and as a strategy to highlight the implication of cloud migration to organisation in terms of change in procedures, process and resources due to cloud computing (Khajeh-Hosseini et al. 2011; Brender and Markov 2013). From the organisational perspective, risk factors on cloud migration are derived from four key areas; enterprise, technical, legal and common risk. In relation to these four areas, the organisation needs to consider several aspects such as business economic, security, availability, quality of services, uncertainty with implemented new technologies and outsourcing (Brender and Markov 2013). Cloud migration decisions involve alternative of buying or leasing resources in long term. In this view, the Different Net Present Value is proposed to evaluate risk for long-term cloud migration decisions since it includes an alternative way for buying and managing storage facilities in house, disk failures and prices (Mastroeni and Naldi 2011). There are also works that demonstrate successfully attacks to the CSP infrastructure. Specifically, Amazon EC2 is vulnerable of Signature Wrapping attack, which poses to any DoS attack within the EC2 infrastructure (Gruschka and Iacono 2009). EC2 is also susceptible to side-channel-attacks that allow attackers to obtain sensitive data about the user (Ristenpart et al. 2009).

To summarize, most of the aforementioned works relating to risk management focus on the organisational and management issues in the cloud and lack of focus for a sustainable cloud migration. The risk factors identified from different perspectives include management competency, service level, security, and cost effectiveness. Less discussion is made on relevant controls suitable for mitigating the identified risks. For a sustainable cloud migration, it is necessary to understand risks from a more holistic perspective and risk analysis should be conducted based on the existing CSP offerings. Our work contributes towards this direction.

3. Sustainable Cloud Migration

In general, sustainability is considered to be economic, social, and environmental progress for both current and future context of the organisation. Sustainable cloud migration also focuses on these dimensions but emphasizes on the continuity of service, adequate training and support for administrators and IT professionals and ease of use (Behrend et al. 2011). While, Bash et al. (2011) emphasised on economic, ecological and social aspects for assessing the overall sustainability of data centres and cloud. Different organisations may have their own objectives and motivations for cloud migration towards increasing productivity and reducing costs, ensuring business continuity, minimizing carbon risk and improving energy efficiency. In our work, we defined sustainable cloud migration as:

The ability of cloud services to satisfy internal and external users' value, economic value, business continuity, flexibility and agility of the system and environmental value.

3.1. Sustainable Dimensions

We considered sustainability in four dimensions, i.e., economic, environmental, social and technological (Schmidt et al. 2009). These four dimensions need to be analysed to address the challenges of cloud migration such as the growth of technologies, user competency, hidden cost, security and green IT requirements. Each sustainability dimension has specific objectives and sub-dimensions. Detail of sustainability dimension and its sub-dimensions are shown in Figure 1.

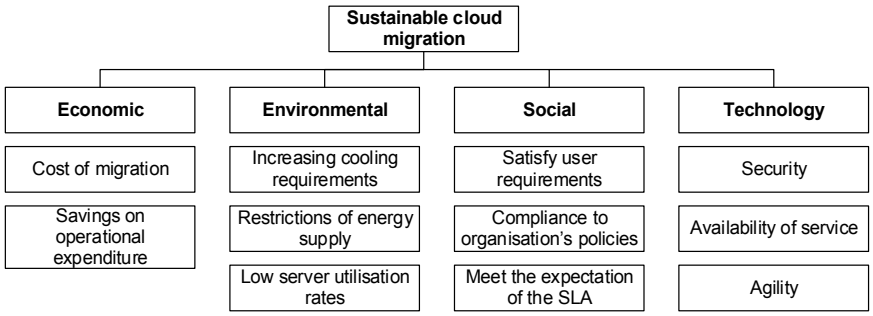

Figure 1. Sustainability dimension.

3.1.1. Economic Dimension

Sustainable cloud migration concerns on understanding the exact cost of outsourcing infrastructure or service and performs cost analysis in order to decide whether cloud migration would be economically worthy for the organisation (Rana 2014). Economic evaluation plays an essential role in analysing the estimation of cost provided by the Cloud Service Provider such as cost of infrastructure, maintenance, testing and other related operational costs. In reality, the stability of economic factor is influenced by external environment such as changes in government policy, government transformation plan or emergence of new technology. Under this view, the economic situation is exposed to a number of threats or risks such as inadequate budget estimation, changes in legal policy and lack of continuous monitoring, so the main concern of organisation is to ensure there is sufficient budget allocation to support the cost of outsourcing, a continuous monitoring activities to make certain that there is no cost overrun, schedule overrun, or any additional cost to adopt with a new technology.

3.1.2. Environmental Dimension

It focuses on the eco-friendly cloud settings as part of the social responsibility. To determine green settings, the selected configuration must support the requirements of multiple applications and minimise energy consumption. It is difficult to identify the optimal configuration that can meet a required response time from several applications. In addition, different hardware consumes variable power, so it is hard to determine the level of energy consumption and energy savings. The availability of resources such as cost, IS infrastructure, governance and skills are the key components to achieve the objective of green cloud. While energy savings in cloud computing is seen as advantage for many organisations, there are risks associated with the green cloud implementation. The sustainability risk includes sufficient knowledge and skills to identify what type of configurations can meet a required response time and is not affecting the quality of services. Cost optimisation is also a risk since it is a challenge to define the operating cost taking into account that different hardware use different energy. The structure and functionality of green cloud can be a challenge to organisation especially regarding the way to define an optimal response time, promote energy savings without adversely impacting quality of service.

3.1.3. Social Dimension

The social dimension for a sustainable cloud migration is to ensure the migration process meet requirements from users, organisation, public and other relevant stakeholders. It is perceived that cloud computing will be continuously performed, has scalable storage, available for delivering services, apply elasticity to prevent denial of service attack and compliance to rules and regulations. Of this features, cloud computing is actually highly dependent on third party services, so it is essential to consider risk associated to cloud service provider in relation to service level, transfer of knowledge, compliance to organisation's policies and standards, incident management and licensing.

3.1.4. Technology Dimension

The technology dimension aims to ensure that cloud migration is secured, scalable, available, and maintainable. Among the main advantages of cloud computing are sharing of resources and infrastructure to multiple clients, thus promoting economies of scale. The distribution of cost and resources to several locations generates potential sustainability risks related to system performance, security and privacy in cloud computing. These include falsification of messages, hardware interception, information leaks, traffic redirection (Brender and Markov 2013).

3.2. Principles and Characteristics for a Sustainable Cloud Migration

A number of concepts for a sustainable cloud computing have been proposed and can be classified into resource savings oriented (Accenture 2010; Harmon et al. 2010), architecture oriented (Bash et al. 2011; Hessami et al. 2009) and control oriented (Müller et al. 2011; Perrini and Tencati 2006). In view of these concepts of sustainable cloud computing, an ideal approach to assist user in achieving a sustainable cloud migration decision can be outlined as depicted in Table 1.

Table 1. Characteristic of sustainable cloud migration.

Process Level of Cloud Migration	Objective	Economic Controls	Environmental Controls	Social Controls	Technological Controls
Planning stage	No hidden cost, Timely Service and maintenance at expected level, Comply with organisation's rules and policies.	Cost benefit analysis Measure cost effectiveness of each related cost to cloud migration.	Check for certification Check for Eco labels	Suppliers audit, Reliable clause of SLA, User requirements, Examine ethical policy, compare economic costs and benefits related to social activities and policies).	Software and hardware selection, Check user requirements.
Execution stage	Lower energy cost, Data center efficiency, Effectively outsourcing, Shared IS infrastructures, Shared application systems	Cost effectiveness	Increase cooling, Energy savings Low server utilization rates, Use dynamic provisioning, shared infrastructure, operate servers at higher utilisation rates, use advanced data centre infrastructure, power conditioning.	Business continuity, Satisfy user requirements, Check user's competency, Compliance to data privacy and security.	Ease of use Flexibility of the systems, Agility of the systems.
Follow up	Effectively and timely maintain	Cost effective	Green IS compliance	Meet user's objective	Availability of service

The purpose of sustainable cloud migration is to contribute to the overall strategy of cloud, to enhance accountability of the organisation to internal and external users and, also the environmental and technological aspects. Sustainable cloud migration achieves these targets by applying indicator that is relevant to each sustainability dimensions. An example of indicator to measure cloud migration is depicted in Table 2. To derive a sustainable cloud migration, the D-S theory is used to compute probability of risk, to identify the impact of risk and the risk exposure level.

Table 2. Sustainability indicator.

Criteria	Sub-Criteria	Indicator
ECONOMIC	Cost benefit analysis Procurement process effectiveness	Satisfaction assessment on compliance with financial rules and regulations
ENVIRONMENT	Green IT configuration Paperless Energy savings	Percentage savings for paperless environment, recycling, energy savings, reduction of general waste No of IT equipment shared Availability of green oriented disposal policy
SOCIAL	Compliance to rules and regulation Outsourcing Key performance indicator IS strategic plan Knowledge transfer User's satisfaction Continuous monitoring	Satisfaction assessment on compliance with rules and regulation, control policies and procedure for application/third party provider, (percentage of objective attained) Percentage of employees who know the system's functions(responsiveness, user friendly) Percentage of employees who can perform system maintenance procedures Satisfaction assessment for KPI achievement
TECHNOLOGY	Availability of service, service delivery flexibility Security	No of system incident reported Average time for system failure Percentage of accurate and reliable information/output produced by IS average time for generated output, application processing No of interaction for continuity of operation (availability of backup plan, storage facility) Satisfaction assessment of system flexibility Average time for network connectivity No of report produced by audit trails Average recovery time after service is down Average time to restore the data Ability to add, modify and remove any software , hardware or data components from IS infrastructure Availability of destruction procedure

4. Demspter Shafer Theory (D-S Theory) of Evidence

The Dempster-Shafer theory of evidence was developed by Dempster and later extended by Shafer (Dempster 1967, 1968; Shafer 1976) and has been widely applied for business decision, auditing, sustainability evaluation and risk assessment (Beynon et al. 2011; Awasthi and Chauhan 2011). The D-S theory uses the concept of 'degree of belief' for modelling and reasoning under uncertainty and incomplete information. The D-S theory consists of three basic functions; basic probability assignment functions or m-values, belief functions and plausibility functions. The description is as follows:

4.1. Basic Probability Assignment (bpa) or m-Values

The basic different between m-values and probabilities is that probabilities are assigned to individual elements or states of a frame (θ). Frame of discernment is a set and mutually exclusive. The sum of all probabilities is one. The m-values in the belief functions represent the uncertainties assigned to individual elements or states and to a set containing of any two elements, three elements, and so on to the entire frame. Similar to probabilities, all these m-values add to one:

$$\sum_{A \in \theta} m(A) = 1,$$

where A represents a proper subset of the frame (θ), and the m-value for the empty set is 0, i.e., $m(\varnothing) = 0$.

4.2. Belief Functions

Given a bpa, we can compute the total belief provided by the body of evidence. The belief in a subset of a frame (θ), say A, is equal to the sum of all m-values for the individual elements in the subset A:

$$\mathrm{Bel}(\mathrm{A}) \sum_{\mathrm{B}\in\mathrm{A}} \mathrm{m}(\mathrm{B})$$

Bel (A) is the total belief committed to A, that is the bpa of A itself plus the bpa attached to all subsets of A.

Plausibility functions

The Plausibility (Pl) function is to provide complementary value of belief. The plausibility in a subset of a frame (θ), say A, represent the maximum uncertainty that could be assigned to A if all future evidence supported A. This is defined as:

$$\mathrm{Pl}(\mathrm{A}) \sum_{\mathrm{A}\cap\mathrm{B}\neq 0} \mathrm{m}(\mathrm{B}) = 1 - \mathrm{Bel}(\sim \mathrm{A})$$

The ambiguity in A is measured as Pl (A) − Bel (A).

We combine and propagate the belief masses (m-values) from several controls to their related risk factor. The combined belief masses (m-values) for a subset A of the frame (θ) using Dempster's rule are given as follows:

$$\mathrm{m}(\mathrm{A}) = (1 \div \mathrm{K}) \sum \{\mathrm{m1}(\mathrm{B1})\mathrm{m2}(\mathrm{B2}) | \mathrm{B1} \cap \mathrm{B2} = \mathrm{A}, \mathrm{A} \in (\varnothing)\}$$

where K is the 'renormalisation' constant given by:

$$\mathrm{K} = 1 - \sum \{\mathrm{m1}(\mathrm{B1})\mathrm{m2}(\mathrm{B2}) | \mathrm{B1} \cap \mathrm{B2} = \varnothing\}$$

K is often interpreted as a normalisation factor which measures the conflict between the pieces of evidence. The larger the K, the more the sources are conflicting and the lesser in the sense of combination. If K = 0, this shows complete compatibility and if 0 < K < 1, it shows partial compatibility. If K = 1, the orthogonal sum does not exist and the sources are totally contradictory.

We combine the evidence and propagate the m-values of controls to their related risks by using equations below.

We use the Dempster's rule as simplified by (Dempster 1967, 1968; Shafer 1976) combine multiple items of evidence for a risk factor. For example:

Control 1: mC1 (a), mC1 (~a), mC1 ({a,~a})
Control 2: mC2 (a), mC2 (~a), mC2 ({a,~a})
Control n: mCn (a), m Cn (~a), mCn ({a,~a})

We combine and propagate the belief masses (m-values) from several controls to their related risk factor. We use (Dempster 1967, 1968; Shafer 1976) to derive m-value for risk through 'AND' relational node. The value of K is written as follows:

$$\mathrm{K} = \sum_{\mathrm{i}=1-\mathrm{n}} (1 - \mathrm{mC1}\ldots\mathrm{n}(\mathrm{a})) + 1 - \sum_{\mathrm{i}=1-\mathrm{n}} (1 - \mathrm{m\ C1}\ldots\mathrm{n}(\sim \mathrm{a})) - \sum_{\mathrm{i}=1-\mathrm{n}} (\mathrm{m\ C1}\ldots\mathrm{n}(\{\mathrm{a},\ \sim \mathrm{a}\})) \quad (1)$$

and the m-values are:

$$\mathrm{mC1}(\mathrm{a}) = 1 - \sum_{\mathrm{i}=1-\mathrm{n}} (1 - \mathrm{mC1}(\mathrm{a}))/\mathrm{K} \quad (2)$$

$$\mathrm{mC1}(\sim \mathrm{a}) = 1 - \sum_{\mathrm{i}=1-\mathrm{n}} (1 - \mathrm{mC1}(\sim \mathrm{a}))/\mathrm{K} \quad (3)$$

$$mC1(\{a, \sim a\}) = \sum_{i=1-n} (mC1(a, \sim a))/K \quad (4)$$

The belief and plausibility functions are given below:

$$\begin{gathered} Bel = Bel(a), \\ Pl(a) = 1 - Bel(\sim a) = 1 - (\sim a) = \sum_{i=1-n} (1 - mC1(\sim a))/K \end{gathered} \quad (5)$$

$$Pl(\sim a) = 1 - Bel(a) = 1 - m(a) = \sum_{i=1-n} (1 - mC1(a))/K \quad (6)$$

5. Risk Management Approach

The proposed risk management approach is based on the degree of belief measured by the potential cloud user perspective. The process consists of three sequential systematic collections of activities and each one of these activities has specific inputs and results in specific outputs artefacts. Figure 2 specifies the process of the risk management approach.

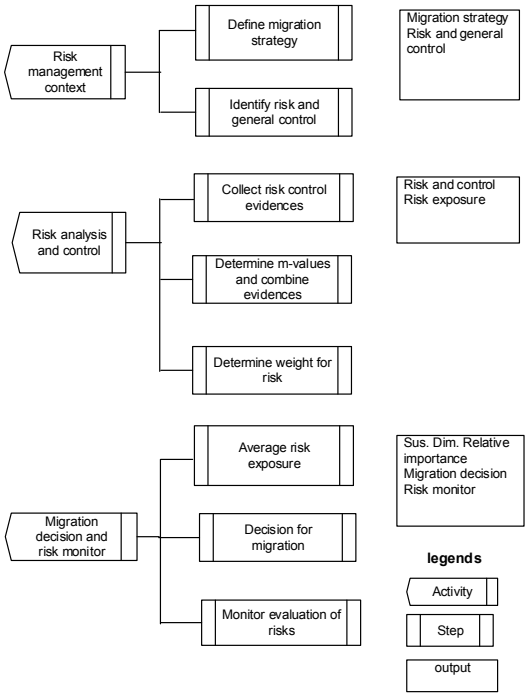

Figure 2. Risk Management Process.

5.1. Activity 1: Risk Management Context

This is the first activity that establishes the scope of risk management through the cloud migration strategy. The cloud migration strategy analyses the existing organisation context and rationalizes the migration needs. This activity includes two steps, i.e., define migration strategy, identify risks and general controls.

Step 1.1 Define migration strategy

This step analyses the existing organisational context to justify the migration needs. Therefore, it is necessary to involve the key organisational people through brainstorming workshop(s) to identify key migration needs that could support the existing business context. It is essential for organisation to analyse and consider business and technical requirements along with guidance and strategies to ensure successful migration to cloud computing. Assessing business requirements include

evaluation of financial capability, data governance, security consideration and overall organisation readiness for using cloud computing. In relation to technical requirements, it includes technology considerations such as migration type, service model, security and integration. This step identifies relevant information for the migration strategy.

- Migration type: Type I: Replace, Type II: Partially migrate, Type III: Migrate the whole software stack Type IV: Cloudify.
- Service model: suitable service model, i.e., IaaS, SaaS, PaaS.
- Deployment model: suitable deployment model, i.e., public, private, community and hybrid
- Security assessment: include access controls, data governance, change management, business continuity, incident handling, third party management, compliance to rules and regulations, auditability of virtual records, data retention policies and physical security.
- Migration size: migration size depends on the relevant application and data properties. The application properties include inherent application components, storage, integration point, business logic. Data include type, registry, size, format, sources, and dependency with the application. Furthermore, it is also necessary to identify the sensitivity of the migrated data so that appropriate protection requirements can be identified. User data migrates into the cloud can be different categories, i.e., Personal Identifying Information (PII), depersonalized information and anonymised information.
- Financial assessment: evaluation on cost savings or return on investment includes cloud deployment, timing of the migration, application and data requirements, and platform storage. The bigger the migration, the higher expected migration costs and complexity.

Step 1.2 Identify risks and general controls

The step identifies the risk and general controls based on the migration strategy of step 1.1. It is necessary to identify all possible risks so that users can be aware of early possible warning that could potentially damage the migration context. Organisational previous list of risks list should also be taken into consideration for this step. Risks focus on the major threats to the cloud models that could obstruct to achieve the benefits of migration during the deployment of cloud and operation of the migrated entities. Risk should categorize based on the four sustainable dimensions. This step also includes identification of general controls that are necessary to mitigate the risks. We need to follow the existence literature, industry practice and standard to identify the general controls.

5.2. Activity 2: Risks Analysis and Control

Once the risks and general controls are identified, it is necessary to calculate the risk exposure in order to determine its severity. The risk analysis is a challenging task within the risk management process due to the difficulties of obtaining data in cloud computing domain to precisely estimate the risk exposure. We follow subjective judgement depending on individual perception as a semi-quantitative assessment for determining the risk exposure value. In particular, we use D-S theory for this purpose to identify the degree of belief that the existing controls are adequate to mitigate the identified risks.

Step 2.1 Collect risks control evidences

For cloud migration purposes, the sources of information about the controls for migrating are derived from the existing organisation practice and CSP offerings. Data relating to control of evidence can be obtained from primary and secondary sources such as existing organisation implemented controls, publicly available information- annual reports and CSP website. If necessary, this step also advocates collecting evidences by interviewing the key organisational personnel to obtain information about the control and adequacy of controls. Table 3 shows risk and general controls for sustainable dimensions.

Table 3. Risk and general controls for sustainable dimensions.

Risk	General Controls
Economic a. Budget overrun b. Schedule overrun c. Excessive contract variation d. Maintenance more frequent than expected. e. Business disruption f. Financial loss g. Service costs are not being competitive over the period of contract h. Obsolescence of hardware due to delay in IS development	a. Establish budget document as accordance to relevant laws and regulations. b. Review budget performance on a scheduler basis. c. Budget is approved and authorised by a steering committee. d. Variance is notified in a timely manner. e. Overall costs are considered for cloud migration such as license, maintenance, services, re-design, deployment and testing, integration and human resources implications. f. Implement continuous monitoring to ensure payment are made based on percentage of work completion. g. Any changes to budget plan is approved and authorised and also being supported with concrete justification.
Environmental a. Energy waste b. Resource waste c. Ineffective green IS implementation	a. Establish policy for green IS implementation such as paperless office, green IS disposal. b. Provide environmental control such as ventilation, air conditioning, temperature control. c. Provide energy savings techniques such as sleep scheduling and virtualisation of computing resources in cloud computing centres.
Social a. Failure to meet performance criteria b. Shortfall in service quality c. Violation of legal compliance d. Loss of controle. Business disruption e. Loss of trust and confidence f. Loss of reputation	a. Establish service level agreement (SLA) to define expected service such as response time. b. Implement short term contracts. c. Providing provisions for making changes in SLA or contract. d. Establish a scheduler review on the response time, scalability of storage, resolution time and etc. e. Identify capabilities to manage change include availability of resources, reason for change and competency of staff (knowledge transfer). f. Checks compliance procedures for IT Governance. g. Providing software escrow provisions.
Technology a. Equipment failure b. Data loss c. Data leakage d. Damage to structure e. Loss of control over IS f. Loss of infrastructure support g. Fraud and theft h. Malicious code	a. Establish policy for business continuity, incident handling, and security. b. Provide audit trail to provide documentary evidence of the activity, time, operation, procedure or event. c. Provide Access Control List to register user and its activities on the system. d. Provide authenticity procedures. e. Provide antivirus, firewall, encryption, and related security parameters. f. Establish network security policies.

Step 2.2: Estimate risk probability and impact

This step estimates the risks event probability based on the belief of existing controls for the risk mitigation. Therefore, we need to collect evidence to support the belief from both the in-house and potential CSPs relating to the controls. Evidences are gathered pertaining to a particular assertions and are measured to determine the overall belief and plausibility whether the assertion is adequate, partially adequate or inadequate. We use the following scales to measure the evidence:

- Adequate (A): Control is adequate to mitigate a risk
- Not adequate (N): Control is not adequate to mitigate a risk
- Partial adequate (P): Control is either adequate or inadequate to mitigate a risk

There can be values between 1 and 0, depending on the degree of belief about the control that could mitigate the risks. If there are multiple controls for a specific risk then the m-value is assigned

to each control and combined using Equations (1)–(5) to determine belief and plausibility functions. The plausibility function obtained from this step measures the maximum amount of probability that can be distributed in the element in Control (mC1.n). Using the D-S theory of belief functions, risk can be modelled by applying the notion of the plausibility (i.e., risk) of a negative outcome (Dempster 1967). The plausibility function is also representing material errors that exist in the evidence and can be applied to measure a risk (Brender and Markov 2013). So the estimation of probability value of risk follows either equation 5 or 6 and probability scales are shown in Table 4.

Table 4. Probability scale.

Score	Likelihood	Likelihood of Occurrence
5	Expected	More than 90% chance of occurrence
4	High	64–89% chance of occurrence
3	Moderate	35–63% chance of occurrence
2	Low	10–34% chance of occurrence
1	Not likely	Less than 10% chance of occurrence

Step 2.3 Determine risk exposure

The final step of the activity determines the risk exposure for each sustainability dimension. The risk exposure value is the multiplication of risk event probability and impact as shown in equation below. Finally, the risk exposure values are mapped to the qualitative scales as shown in Table 5 to determine the acceptable level of risk for cloud migration decision

$$\mathrm{RE(ri)} = \mathrm{P} \times \mathrm{I} \tag{7}$$

where

ri: Individual risk of any category, i.e., economic, environmental, social and technology
i = 1 ... n
RE: Exposure of risk ri
P: Probability of risk ri
I: Impact of risk ri

Table 5. Risk exposure scale.

Risk Exposure Level	Score	Risk Exposure Description
Extreme	0.81–1.0	Economic: Budget deficit, cloud migration is suspended. Environmental: Unable to comply with green IS strategy and cost optimisation. Social: Incapable to monitor service performance from the supplier and managing change. Technological: Incompetent to handle IS incidents, to accomplish IS control objectives or to provide security for IS or for cloud migration.
High	0.61–0.8	Economic: Budget deficit, cloud migration is reschedule at a later date. Environmental: Able to comply with green IS strategy but incur additional cost. Social: Incapable of monitoring service performance from the supplier and managing change. Technological: Business continuity, crisis management plan and IS strategic plan are not established.
Medium	0.41–0.6	Economic: Limited budget estimate, cloud migration is possible. Environmental: Only some equipment is green IS compliant due to limited budget. Social: Capable of defining service level and managing change. Technological: Business continuity, crisis management plan and IS strategic plan are established and but not tested.

Table 5. *Cont.*

Risk Exposure Level	Score	Risk Exposure Description
Low	0.21–0.4	Economic: Reasonable budget estimate, adequate resource for cloud migration. Environmental: Equipment is green IS compliant. Social: Capable of defining service level and managing change. Technology: Business continuity plan, crisis management plan and disaster recovery plan are available and tested.
Very Low	0.0–0.2	Economic: Moderate budget estimate, adequate resource for cloud migration. Environmental: Equipment is green IS compliant. Social: Capable of defining service level, provides adequate IS controls, storage and managing change. Technology: Business continuity plan, crisis management plan and disaster recovery plan are available, tested and sufficient.

5.3. Activity 3: Migration Decision and Risk Monitor

This final activity undertakes the decision whether cloud migration is feasible after taking into account sustainability risk and its related controls. In a context of decision making under risk, we defined total risk exposure as a basis for cloud migration. This activity consists of three steps.

Step 3.1 Determine the overall sustainable risk

Once the risk exposure values are obtained from sustainable dimensions, the overall sustainable risk value are averaged and can be written as follows. Similar equations are applied to environmental, social and technological dimensions. IS auditors derive conclusions based on the value of risk exposure which is used a basis to conclude the level of IS sustainability.

$$\text{Rsustainable(Economic)} = \frac{RE1 + RE2 + \ldots\ldots RE n}{n}$$

where,

Rsustainable (Economic) = Total sustainable risk exposure for economic

Ren = n number of risk exposure for economic.

Step 3.2 Decision for migration

Once the overall sustainable risk exposure value is determined then it is necessary to undertake the migration decision. The evidence from the D-S theory support judgement from users' perspective. These findings lead on finding a solution for a feasible migration subjected to the following conditions:

Type 1: Possible to migrate

A possible to migrate is applicable when the level of risk exposure is between very Low to Low and the value of risk exposure is between 0.51 and 1.0. This judgement is concluded based on the following criteria:

(a) The number of sustainability dimensions that linked to a high risk exposure should be less than three.
(b) Risk exposure is insignificant and can be mitigated by the existing controls.
(c) The controls are adequate and have been designed in accordance with relevant legislations, regulations or best practices for the sustainability dimension which is deemed to be important.
(d) There is adequate justification and documentation relevant to the cloud migration procedures and practised.
(e) The cloud migration is for noncomplex application systems or the migration size is small.

Type 2: Reasonable to migrate

A reasonable to migrate is described when the risk exposure is at medium level. This judgement is concluded when the following circumstances exist:

(a) The number of sustainability dimensions that linked to a high risk exposure should be less than two.
(b) There are evidence that threats or risk are manageable.
(c) There is adequate justification and documentation relevant to the cloud migration procedures and practised.
(d) The migration is intended for core systems of the organisation and the existing controls are effective and efficient to mitigate risks. Appropriate control measures are designed to minimise risk for each sustainability dimensions.

Type 3: Unlikely to migrate

An unlikely to migrate condition is applicable when three or four of sustainability dimensions have high risk exposures. This judgment is issued when the following circumstances exist:

(a) The controls are not adequate to mitigate risks.
(b) The controls have not been designed in accordance with relevant legislations, regulations or best practises.

Step 3.3 Monitor the risk

This step supports the risk monitoring activities by evaluating the existing risks and identifies new risks upon completion of cloud deployment. Cloud platforms can evolve by nature and changes could occur within the control domain. It is likely that new risks can emerge and/or probability of existing risks can be changed. Risk monitoring is essential for the process. Following the sensitivity analysis we advocate to investigate the impact if belief values of the information sources change. For example, cloud migration may need functional flexibility to support business activities and processes or the business may need to respond to new rules or to meet requirements of the new system during the cloud implementation. For this analysis, assume that one item control needs to be added due to the replacement functions of the IT system. We determine the degree of belief of this control and evaluate the changes based on D-S theory. The result will show the level of adequacy of the new control and varies with the changes in input belief. It is important to pay more attention on the items of control at higher levels because they have greater impacts on the overall risk evaluation than the items of control at the lower assertion levels.

6. Evaluation

For evaluation purposes, we employ the approach into a real-world scenario in collaboration with the Malaysian Ministry of Health (MoH). Public hospitals in Malaysia are categorised into two types; regional/state and district hospital. The provision of healthcare services, number of bed and number of medical specialist are factors that determined the type of hospital. The MoH is a public organisation and its operations are located at the Head Quarters in Putrajaya. To date, there are 139 branches of MOH that provide public healthcare services nationwide. The goal of the study is to Support MoH with cloud-migration decision:

- Identify risk and possible control for making a viable sustainable decision;
- Examine the applicability of using sustainable dimension and risk for the cloud migration decision.

6.1. Migration Use Case

The Ministry of Health (MoH) is a very large organisation. To date, there are more than 70,000 employees in the MoH and email service is the main medium for communication among

employees from all locations. The ministry follows paperless communication strategy. Therefore, MoH has a huge amount of email transactions that are operating under the Internet connectivity of 32 Mbs in the head office. All emails are maintained on the mail server for legal/audit/documentary purposes and are archived for a period of 180 days. An allocation of 500 MB email storage is provided for individual employee and the email storage varies according to their roles and responsibilities. The total five years IT infrastructure maintenance cost for managing the email service is £20,000–£40,000 and data size will increase triple of the existing size, i.e., 45 TB.

6.2. Introduction of Risk Management Process

6.2.1. Activity 1: Risk Management Context

The risk management team consists of one of the co-authors and two MoH internal staffs (IT and HR). The team performed a kick–off workshop with the key MoH staffs to initialize the risk management process. First step of this activity defines the migration profiles by analysing the migration scenario with the top MoH management. Cost reduction is one of the main goals that the management intends to achieve through cloud migration. However, it is also necessary to safeguard all e-mails through cloud.

Step 1.1 Define migration strategy

The management of the MoH has developed migration strategy for the email services to be migrated into the cloud. The strategy began with the basic requirements prior to migration as stated below:

- Migration type: Type II: Partially migrate due to not considering the whole MoH.
- Service model: SaaS
- Deployment model: public
- Security assessment: access controls, data governance, change management, business continuity, incident handling, third party management, compliance to rules and regulations, auditability of virtual records, data retention policies and physical security.
- Migration size: The application and data requirements are identified. The application requirements include components, storage, integration point, business logic. Data requirements include files, registry information, size of data, sources and storage. The category of data and its sensitivity are also taken into consideration.

Step 1.2 Identify risks and general controls

During this step an interview with the key MoH staffs is performed in order to identify the possible risks. These risks are then consolidated with general controls to mitigate the risks. Table 3 already showed the general controls.

6.2.2. Activity 2: Risks Analysis and Control

In this step the goal is to obtain evidences of existing controls from the MoH infrastructure by interviewing eight (8) key IT staffs. About 22 questionnaires were distributed to the staff of MoH. The respondents were from operational to senior level of management and had a minimum of five (5) years' experience working with the MoH.

Step 2.1 Collect risk control evidences

Based on the questionnaires, respondents are required to provide their belief on the adequacy of controls provided by the organisation. From the assessment, Economic risk (R1) has three types of controls to mitigate risk related to budget estimation, monitoring and changes in policies. Environmental has two type of controls, Social has three types of controls and Technology has four type of controls.

Step 2.2 Estimate risk probability and impact

This step determines the risk event probability and impact based on the identified risks and evidence of controls. The probability mainly focuses on the belief by following the existing control. From this analysis, it was observed that mitigating controls for economic risks are provided by the organisation and there has been less commitment from the CSP to be involved in budget or financial arrangement for cloud migration. Under this context, the degree of belief considers that the existing risk can be mitigated. Here we obtained the value for C1 is 0.6, partially mitigate (P) is 0.3 and not mitigate (N) is 0.1. Note that, the result shows risk from the economic dimension and we can continue the calculation for the other dimensions as well.

K values for R1 are as follows:

$$\mathrm{K} = \prod \mathrm{i} = 1 - 5(1 - mR1(A)) + \prod \mathrm{i} = 1 - 5(1 - mR1(p)) - \prod \mathrm{i} = 1 - 5(1 - \mathrm{mR1(I)} = 0.4 \times 0.5 \times 0.4 \times 0.4 \times 0.3 + 0.7 \times 0.5 \times 0.7 \times 0.7 \times 0.7 - 0.1 \times 0 \times 0.1 \times 0.1 \times 0.1 = 0.12965$$

and the m-values are:

m(A) = 0.9259

m(P) = 0.0740

m (N) = 0.00000

Then, we determine the overall beliefs and plausibility that the assertion is adequate or partially adequate.

$$\text{Bel (A)} = 0.9259, \text{Bel (P)} = 0.0740$$

$$\mathrm{Pl(A)} = 1 - Bel(P) = 1 - m(P) = \prod \mathrm{i} = 1 - 5(1 - mi(P)) \div K = 0.9259$$

$$\mathrm{Pl(P)} = 1 - Bel(A) = 1 - m(A) = \prod \mathrm{i} = 1 - 5(1 - mi(P)) \div K = 0.0740$$

Step 2.3 Determine risk exposure

For decision making purposes, it is necessary to evaluate all risk factors and understand all the relevant issues. The summary of the complete assessment of overall m-values and risk exposure are depicted in Table 6.

Table 6. The overall m-values and risk exposures.

Sustainable Dimensions	m-Values			Weight Factor (Impact)	Probability Value	Risk Exposure
	Mitigate	Inbetween	Not Mitigate			
Economic						
R1	0.9259	0.07404	0	0.673	0.0741	0.0498693
R2	0.6666	0.25	0	0.256	0.3334	0.053504
R3	0.9795	0.0204	0	0.07	0.0205	0.001435
						Total 0.1366547
Environment						
R4	0.7222	0.2222	0.0555	0.6333	0.2778	0.1759307
R5	0.8378	0.1351	0.027	0.2667	0.1622	0.0432587
						Total 0.2191895
Social						
R6	0.8974	0.0769	0.0256	0.2179	0.1026	0.0223565
R7	0.8591	0.1126	0.0281	0.4676	0.1409	0.0658848
R8	0.9523	0.0357	0.0119	0.3143	0.0477	0.0149921
						Total 0.1032335
Technology						
R9	0.9692	0.0307	0	0.2554	0.0308	0.0078663
R10	0.875	0.1111	0.138	0.1129	0.125	0.0141125
R11	0.918	0.0819	0	0.5861	0.082	0.0480602
R12	0.922	0.0649	0.0129	0.454	0.078	0.355412
						Total 0.105451
						Overall 0.1411322

6.2.3. Activity 3. Migration Decision and Risk Monitor

Step 3.1 Determine the overall sustainable risk

In order to assess the feasibility of the cloud migration, it is necessary to incorporate the overall sustainability risks. The overall sustainability risk for this case study is 0.1411. As stated previous section we consider five different risk scales for sustainability. The overall risk value is very low for the study context. This value justifies based on the migration context and its low complexity.

Step 3.2 Decision for migration

From the overall sustainability risk, it could be concluded that Type I of decision making can be applied as it has low score and migrating to cloud is possible as overall controls are adequate to mitigate economic risk, environmental risk, social risk and technology risk.

Step 3.3 Risk Evaluation Monitor

As the decision for migration is taken, initially monitoring activity should be taken into consideration the risk factors that do not have adequate evidence of control such as environmental, technology, and social. Furthermore, it is worth mentioning that once the migration is taken in place, the MoH user new requirements need to be addressed. For example, if the management plans to expand the network capacity of cloud system, this decision may involve additional cost relating to integration, installation and maintenance. To show the changes in overall belief when estimation of cost is changes, the above arithmetic measures are used to identify new degree of belief, m-values as well as risk exposure within economic dimension. If the changes vary in significant values and may increase the probability for risk exposure, the organisation may reconsider to pay more attention on the budget estimation, which include hidden cost, monitoring and contingency plan.

6.3. Discussion

The risk driven sustainable cloud migration decision support is certainly assisted MoH for making their migration decision and considering cloud into their existing business process. The approach supports analysing all potential risks from the four sustainable dimensions, so that MoH can determine the viability of cloud migration.

6.3.1. Applicability of the Sustainable Cloud Migration Approach

We have made several observations. The underlying activities within the process are operational and adequate. The only issue is with understanding D-S theory by the MoH users. However, if we can automate the activities then users do not need to be aware of the complex calculations for risk analysis.

6.3.2. Sustainability Risk Driven Approach for Sustainable Cloud Migration

The integration of sustainable risk driven approach for cloud migration supports users understand the possible risks before considering cloud migration. Our work considers risks from four different sustainability dimensions which ease to understand the potential negative consequences if the migration decision is taken by the management. Organisations are considering changes for day-to-day business environment, therefore decision should be sustainable for the overall business continuity and continuous improvement (Dempster 1968). In particular, there is always external pressure to MoH for providing cost saving services and internal operations. Therefore, migration to cloud could be a viable option but it is necessary to know what could go wrong if the migration decision is taken. Our work effectively supports towards this direction.

6.3.3. Evaluation Inherent Risks for Cloud Migration

Migrating into cloud presents new challenges and these challenges pose any potential risks specifically relating to technology and economic. There are also risks based on the existing computing context. Therefore, it is necessary to consider all these inherent risks if the cloud computing is considered to support the business. In this paper, we discussed how organisation can manage inherent risks for cloud migration by linking it with sustainability. These risks are already existed within the organisation and due to the cloud migration it is necessary to further evaluate the risks. The identified general control from both in house and CSP allows to evaluate the likelihood of risks depending on the degree of belief for the risk mitigation. The sustainability risks that make up our work are derived from the potential negative impacts that have emerged as important within organisation.

6.3.4. Risk Management Process and Artefacts

The MoH employees agreed that the underlying activities for the sustainability risk driven process are adequate to identify and analysing the possible risks. The process initiates with the migration profile that helps to understand what the organisation would like to migration within existing context so that possible risks from the sustainable can be identified. Risks analysis activities depend on individual degree of belief of the existing control for the risk mitigation using the D-S theory so that risk exposure can be determined accurately. This aims to support the informed migration decision. The artefacts produced by the activities are mainly textual tabular format and provide a reasonable clear view of risks.

6.3.5. Limitations of the Framework and Study Validity

Our main observation with the approach is that it is difficult for the MoH employees to understand the risk exposure calculation due to the complexity of determining the probability values. However, we are planning to automate the calculation so that user intervention can be reduced for the risk estimation. We also do not follow risk monitor activity as the decision for migration approved and there is an internal time frame for execution. Therefore, it is difficult at this stage to analyse the evolution of risks. The studied context is from a single case, there is a possibility of expectation bias and the identified results cannot be fully generalized. The MoH interviewed employees have adequate technical knowledge and it helps us to validate the work and reduce from any lack of knowledge to understand the approach and terminology.

7. Conclusions

There are many challenges in cloud computing despite of significant benefits. These challenges can pose any potential risk that could outweigh the expected benefits. Risk management is certainly critical for analysing these challenges and offers realistic plan for the risk control and business continuity. We advocate integrating an effective risk management practice during the cloud migration decision so that organisation can forecast the sustainability of cloud to support business needs. The proposed sustainable risk-driven approach for supporting cloud migration decision is based on the evidential reasoning approach using D-S theory of belief functions. The proposed approach allows decision makers to justify the adequacy of controls provided by the organisation to mitigate the identified risks. The application of the approach to a real case study has been very promising specifically for providing early warning about the issues that need adequate attention. The results from the risk management activities have directly incorporated into the studied context in order to support them with their migration decision. We are currently working on defining a guideline for the risk management activities along with a proper checklist so as to provide better hands-on support to the potential cloud users. We are also planning to apply the approach into different context to generalize our findings.

Acknowledgments: This work is partly supported by the Public Service Department of Malaysia and the National Audit Department of Malaysia.

Author Contributions: Alifah Aida Lope Abdul Rahman carried out the background work and developed the risk management method based on the review of the state-of-the-art works. She also initial drafted the manuscript with Shareeful Islam. Shareeful Islam also supported the initial draft and with the evaluation part. Christos Kalloniatis contributed with the evaluation part and review of the risk management method. Stefanos Gritzalis 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 no conflict of interest.

References

Accenture. 2010. *Cloud Computing and Sustainability: The Environmental Benefits of Moving to the Cloud*. Hong Kong: Accenture, pp. 1–11.

Asif, Muhammad, Cory Searcy, Ambika Zutshi, and Olaf A. M. Fisscher. 2013. An integrated management systems approach to corporate social responsibility. *Journal of Cleaner Production* 56: 7–17. [CrossRef]

Awasthi, Anjali, and Satyaveer S. Chauhan. 2011. Using AHP and Dempster–Shafer theory for evaluating sustainable transport solutions. *Environmental Modelling & Software* 26: 787–96.

Bash, Cullen, Tahir Cader, Yuan Chen, Daniel Gmach, Richard Kaufman, Dejan Milojicic, and Puneet Sharma Shah. 2011. *Cloud Sustainability Dashboard, Dynamically Assessing Sustainability of Data Centers and Clouds*. Palo Alto: HP Laboratories, HPL-2011-148.

Behrend, Tara S., Eric N. Wiebe, Jennifer E. London, and Emily C. Johnson. 2011. Cloud computing adoption and usage in community colleges. *Behaviour & Information Technology* 30: 231–40.

Beynon, Malcom, Darren Cosker, and David Marshall. 2011. An expert system for multi-criteria decision making using Dempster Shafer theory. *Expert Systems with Applications* 20: 336–57. [CrossRef]

Brender, Nathalie, and Iliya Markov. 2013. Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management* 33: 726–33. [CrossRef]

Chang, Victor, David De Roure, Gary Wills, and Robert Walters. 2011. Case studies and organisational sustainability modelling presented by cloud computing business framework. *International Journal of Web Services Research* 8: 26–53. [CrossRef]

Dempster, Arthur P. 1967. Upper and lower probabilities induced by a multivalued mappings. *The Annals of Mathematical Statistics* 38: 325–39. [CrossRef]

Dempster, Arthur P. 1968. A generalization of Bayesian inference. *Journal of the Royal Statistical Society* 30: 205–47.

ENISA. 2009. Cloud Computing Benefits, Risks and Recommendations for Information Security. Available online: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications (accessed on 2 June 2017).

Gruschka, Nils, and Luigi Lo Iacono. 2009. Vulnerable Cloud: SOAP Message Security Validation Revisited. Paper presented at IEEE International Conference on Web Services, Los Angeles, CA, USA, July 5–10; pp. 625–31.

Harmon, Rober, and Haluk Demirkan. 2011. The Next Wave of Sustainable IT. *IEEE IT Professional* 13: 19–25. [CrossRef]

Harmon, Rober R., Tugrl Daim, and David Raffo. 2010. Roadmapping the Future of Sustainable IT. Paper presented at IEEE Conference on Technology Management for Global Economic Growth, Phuket, Thailand, July 18–22; pp. 1–10.

Hessami, Ali G., Feng Hsu, and Hamid Jahankhani. 2009. *A Systems Framework for Sustainability*. Berlin and Heidelberg: Springer, pp. 76–94.

Islam, Shareeful, Stefan Fenz, Edgar Weippl, and Christos Kalloniatis. 2016. 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* 7: 44–73. [CrossRef]

Islam, Sahreeful, Stefen Fenz, Edgar Weippl, and Haris Mouratidis. 2017. A Risk Management Framework for Cloud Migration Decision Support. *Journal of Risk and Financial Management* 10: 10. [CrossRef]

Kalloniatis, Christos, Haris Mouratidis, and Shareeful Islam. 2013. Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements. *Requirements Engineering* 18: 299–319. [CrossRef]

Khajeh-Hosseini, Ali, Ian Sommerville, Jurgen Bogaerts, and Pradeep Teregowda. 2011. Decision Support Tools for Cloud Migration in the Enterprise. Paper presented at IEEE 4th International Conference on Cloud Computing, Hangzhou, China, October 11–14; pp. 542–48.

Madria, Sanjay, and Amartya Sen. 2015. Off-Line Risk Assessment of Cloud Service Provider. Paper presented at IEEE Cloud Computing Conference, Anchorage, AK, USA, June 27–July 2; vol. 2, No. 3. pp. 50–57.

Mastroeni, Loretta, and Maurizio Naldi. 2011. Long-range Evaluation of Risk in the Migration to Cloud Storage. Paper presented at IEEE Conference on Commerce and Enterprise Computing, Luxembourg, September 5–7; pp. 260–66.

Morin, Jean-Henry, Jocelyn Aubert, and Benjamin Gateau. 2012. Towards Cloud Computing SLA Risk Management: Issues and Challenges. Paper presented at 45th Hawaii International Conference on System Science, Maui, HI, USA, January 4–7.

Müller, Gunter, Noboru Sonehara, Isao Echizen, and Sven Wohlgemuth. 2011. Sustainable Cloud Computing. *Business & Information Systems Engineering* 3: 129–31.

Perrini, Francesco, and Antonio Tencati. 2006. Sustainability and stakeholder management: The need for corporate performance evaluation and reporting systems. *Business Strategy and Environment* 15: 296–308. [CrossRef]

Puthal, Deepak, B. P. S. Sahoo, Sambit Mishra, and Satyabrata Swain. 2015. Cloud Computing Features, Issues, and Challenges: A Big Picture. Paper presented at Conference on Computational Intelligence & Networks, Bhubaneshwar, India, January 12–13.

Rahman, Alifah Aida Lope Abdul, and Shareeful Islam. 2015. Sustainability Forecast for Cloud Migration. Paper presented at IEEE International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Environments, Bremen, Germany, October 2.

Rana, Omer. 2014. The Costs of Cloud Migration. *IEEE Cloud Computing* 1: 62–65. [CrossRef]

Ristenpart, Thomas, Eran Tromer, Hovav Shacham, and Stefan Savage. 2009. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. Paper presented at 16th ACM Conference on Computer and Communications Security, New York, NY, USA, November 9–13; pp. 199–212.

Schmidt, Nils-Holger, Koray Erek, Lutz M Kolbe, and Rüdiger Zarnekow. 2009. Sustainable Information Systems Management. *Business & Information Systems Engineering* 5: 400–2.

Shafer, G. 1976. *A Mathematical Theory of Evidence, a Mathematical Theory of Evidence*. Princeton: Princeton University Press.

Silvius, A. J. Gilber, Jasper Van Den Brink, and Jacobus Smit. 2009. Sustainability in Information and Communications Technology (ICT) Projects. *Communications of the IIMA* 9: 33–44.

Sunyaev, Ali, and Stephen Schneider. 2013. Cloud services certificate. *Communications of the ACM* 56: 33–36. [CrossRef]

Theoharidou, Marianthi, Nick Papanikolaou, Siani Pearson, and Dimitris Gritzalis. 2013. Privacy Risk, Security, Accountability in the Cloud. Paper presented at IEEE Cloud Computing Technology and Science (CloudCom), Bristol, UK, December 2–5.

Wang, Chengen, Zhuming Bi, and Li Da Xu. 2014. IoT and Cloud Computing in Automation of Assembly Modeling Systems. *IEEE Transactions on Industrial Informatics* 10: 1426–34. [CrossRef]

Yi, Sangho, Artur Andrzejak, and Derrick Kondo. 2012. Monetary cost aware checkpointing and migration on Amazon cloud spot intances. *IEEE Transactions on Services Computing* 5: 512–24. [CrossRef]

Zhang, Xuan, Nattapong Wuwong, Hao Li, and Xuejie Zhang. 2010. Information Security Risk Management Framework for the Cloud Computing Environments. Paper presented at IEEE Computer and Information Technology, Bradford, UK, June 29–July 1.