future internet

MDPI

Article

ERMOCTAVE: A Risk Management Framework for IT Systems Which Adopt Cloud Computing

Masky Mackita [1], Soo-Young Shin [2] and Tae-Young Choe [3,*]

[1] ING Bank, B-1040 Brussels, Belgium; maskymackita@gmail.com
[2] Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea; wdragon@kumoh.ac.kr
[3] Department of Computer Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea
* Correspondence: choety@kumoh.ac.kr; Tel.: +82-54-478-7526

Received: 22 June 2019; Accepted: 3 September 2019; Published: 10 September 2019

Abstract: Many companies are adapting cloud computing technology because moving to the cloud has an array of benefits. During decision-making, having processed for adopting cloud computing, the importance of risk management is progressively recognized. However, traditional risk management methods cannot be applied directly to cloud computing when data are transmitted and processed by external providers. When they are directly applied, risk management processes can fail by ignoring the distributed nature of cloud computing and leaving numerous risks unidentified. In order to fix this backdrop, this paper introduces a new risk management method, Enterprise Risk Management for Operationally Critical Threat, Asset, and Vulnerability Evaluation (ERMOCTAVE), which combines Enterprise Risk Management and Operationally Critical Threat, Asset, and Vulnerability Evaluation for mitigating risks that can arise with cloud computing. ERMOCTAVE is composed of two risk management methods by combining each component with another processes for comprehensive perception of risks. In order to explain ERMOCTAVE in detail, a case study scenario is presented where an Internet seller migrates some modules to Microsoft Azure cloud. The functionality comparison with ENISA and Microsoft cloud risk assessment shows that ERMOCTAVE has additional features, such as key objectives and strategies, critical assets, and risk measurement criteria.

Keywords: risk management; ERM; OCTAVE; cloud computing; Microsoft Azure

1. Introduction

Cloud computing is a technology that uses virtualized resources to deliver IT services through the Internet. It can also be defined as a model that allows network access to a pool of computing resources such as servers, applications, storage, and services, which can be quickly offered by service providers [1]. One of properties of the cloud is its distributed nature [2]. Data in the cloud environments had become gradually distributed, moving from a centralized model to a distributed model. That distributed nature causes cloud computing actors to face problems like loss of data control, difficulties to demonstrate compliance, and additional legal risks as data migration from one legal jurisdiction to another. An example is Salesforce.com, which suffered a huge outage, locking more than 900,000 subscribers out of important resources needed for business transactions with customers [3].

The main cause of these incidences was poorly conducted risk identification during risk management process. Effective risk assess and being aware of different vulnerabilities are the best mechanism for

incidence prevention in cloud computing. Thus, a novel risk management framework is highly required to properly identify those risks and to provide an ultimate way of mitigating their occurrence. Our motivation comes from potential security risks of cloud computing due to their distributed nature and mainly the lack of dedicated risk management method. Many risk managers admit struggling to grasp the basics of how the cloud is deployed in their businesses, and how to manage risks linked to this new technology. Identifying risks and understanding them are the prime challenges. Risk management for cloud computing must discover some key risks, prioritize them, and formulate a mitigation plan. Due to the nature of cloud computing risks and the emergence of new risks, one-time risk assessment is not sufficient.

The aim of the paper is to introduce a new risk management method ERMOCTAVE for mitigating risks in cloud computing environment. As a method, we coalesce Enterprise Risk Management (ERM) framework and risk-based information security methodology Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). Although OCTAVE is prone to IT-related risks, ERM prioritizes risks and brings risk management to a more strategic level. As an example of ERMOCTAVE application, we suggest a case study scenario of an Internet seller who migrates a part of their web system to a cloud system, Microsoft Azure.

The remaining section is organized as follows. Section 2 explains terminologies and related works. Section 3 explains the proposed ERMOCTAVE method in detail. Section 4 helps understanding of ERMOCTAVE using a case study with Microsoft Azure cloud. Section 5 compares functionality of ERMOCTAVE and two existing methods. Finally, Section 6 finishes with conclusion.

2. Terminologies and Related Works

2.1. Terminologies

Cloud computing is a model for delivering data virtually on the Internet through web-based tools and applications, rather than a direct connection to a server. Resources are stored in servers. In the IT security environment, "risk" is the probability that a confidential information is exposed, data integrity is damaged, or information availability is interfered. Risk formula is the result of likelihood probability multiplied by the impact of the above events. Also, risk can be defined as result of identified vulnerability being exploited by a specific threat [4].

"IT risk management" is the process enabling the balance between operational cost and economic costs of protective controls in order to protect IT systems that support their organization's objectives. This process provides decision-making in all areas of our lives not only in IT environments. An effective risk management methodology helps managers determine appropriate actions for offering security capabilities [1].

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a strategic assessment method for risk-based security [5]. It uses people's knowledge of security practices to understand the current security posture of the organization. Unlike typical assessments, which only target technological risk, OCTAVE also considers organizational and strategic risks. Using OCTAVE, a small team of people from the operational units and the technology department together address the security requirements, balancing three key aspects: operational risk, security practices, and technology. The OCTAVE method has three phases in which processes are described below [5].

Phase 1 Build asset-based threat profiles: Phase 1 gathers information from the organization and defines threat profiles for critical assets.

Process 1 Identify senior management knowledge: Information about important assets, security requirements, threats, current strengths, and current vulnerabilities is collected from senior managers.

Process 2 Identify operational area knowledge: The information is collected from managers of selected operational areas.

Process 3 Identify staff knowledge: The information is collected from general staff and IT staff members.

Process 4 Create threat profiles: Critical information assets are selected and threat profiles for those assets are defined.

Phase 2 Identify infrastructure vulnerabilities: This phase evaluates key components of systems supporting the critical assets for technological vulnerabilities.

Process 5 Identify key components: This process identifies key components from the systems that support the critical assets.

Process 6 Evaluate selected components: Tools are run to evaluate the selected components, and the results are analyzed to refine the threat profiles.

Phase 3 Develop security strategy and plans: The primary purpose of this phase is to evaluate risks on critical assets and to develop a protection strategy and risk mitigation plans.

Process 7 Conduct risk analysis: A set of impact evaluation criteria is defined to elaborate the impact value (high, medium, or low).

Process 8 Develop protection strategy: The organization-wide protection strategy focuses on improving security practices and mitigation plans, which reduce the important risks on critical assets are developed.

Enterprise risk management (ERM) is a framework affected by the board of directors and the management of an entity. ERM aims to identify potential events that may affect the entity and to manage risks using its risk appetite. "Risk appetite" is the level of risk that the entity is prepared to accept in pursuit of its objectives. The level could be averse, minimal, cautious, open, or hungry. ERM offers assurance regarding the accomplishment of objectives set by the entity [6]. In ERM, uncertainty has both risk and opportunity. Risk can reduce value while an opportunity can enhance value. ERM components are described as follows.

- Internal environment: the internal environment provides basics on how risk and control are addressed.
- Objective setting: before the management identifies potential events, objectives of the entity are set. ERM makes sure that the objectives are consistent with the risk appetite.
- Event identification: potential events impacting the entity are identified. This process involves identification of events from internal or external sources which affect the accomplishment of objectives.
- Risk assessment: identified risks are analyzed and assessed on both inherent and residual basis considering risk likelihood and impact.
- Risk response: possible responses to risks are identified. They include avoiding, accepting, reducing, and sharing risks.
- Control activities: policies, procedures, and controls are established and implemented to sustain the risk response decisions.
- Information and communication: relevant information is captured and communicated enabling people to carry out their responsibilities.
- Monitoring: ERM is entirely monitored to react dynamically as changes are made.

2.2. Related Works

The advantages of cloud computing over traditional networks are well known and they include fast deployment. However, identification of the risks in cloud computing is more difficult because of the lack of a dedicated framework. Such risks make businesses feel difficulty when adopting cloud technology. Over the last few years, a lot of documents have been written about risks and guidelines regarding cloud computing adoption. These documents rank highly as a security concern, but rank low across risks where a dedicated risk management framework is required.

In that perspective, some organizations related with standardization frameworks have published risk management frameworks for cloud computing. The International Organization for Standardization (ISO/IEC JTC 1/SC 27) has developed a set of standards aiming to address risk management for cloud computing [7]. The standards are applied to new service models, such as Data as a Service (DaaS) and the cloud service brokers emergence, which offers intermediation, portability, governance, provisioning, and service integration, in addition to existing cloud services. However, the framework standards seem more like tools that enable understanding of the risks around cloud migration rather than an effective method to mitigate these risks.

The European Network and Information Security Agency (ENISA) identified 35 types of risks by 19 contributors and lists eight top security risks based on indicative likelihood and impact [8]. The 35 risks are ranked from the lowest to the highest. Risk analysis proposed by ENISA is based on a real-life case study of a small- and medium-sized enterprise (SME) using cloud computing [9]. However, any risk management framework for mitigating risks in cloud computing is not included.

Cloud Security Alliance (CSA) published "Top Threats to Cloud Computing V1.0", which includes the top seven threats as identified by its members [10]. The objective is to provide threat identification that can be updated, because dynamic and distributed properties are major natures of cloud computing [11]. The threat list roles more as managerial tool for higher strategic decisions in cloud adoption. Still, there is a lack of risk management framework in cloud computing.

National Institute of Standards and Technology (NIST) published two drafts titled "Cloud Computing Synopsis and Recommendations" [12] and "NIST Cloud Computing Standards Roadmap" [13]. The drafts introduce a cloud-adopted risk management framework for services moved to the cloud. This framework enables federal organizations to develop a computer security plan based on risk tolerance and the information sensitivity. The provided set of standards and guidelines supports risk response strategies. However, the framework only allows analysis of risks in cloud computing than a comprehensive method to assess them.

Information Systems Audit and Control Association (ISACA), published a document, "IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud", which introduces a guide to cloud controls taken from COBIT, Val IT, and Risk IT [14]. Its framework is not quite structured to identify and mitigate potential risks in cloud computing.

A cloud risk assessment framework based on the ISO 31000 standard was introduced by Microsoft [15]. It has six steps that evaluate risks for cloud service candidates and focuses on decision-making for cloud-based computing. The framework provides value to decision-making process. However, it lacks mitigation plan after a specific risk has been identified and assessed.

Since the above-mentioned risk management frameworks lack details on real application, ideas especially for risk assessment methods, have been proposed as follows. Fitó et al. proposed SEmi-quantitative BLO-driven Cloud Risk Assessment (SEBCRA) for the risk assessment process [16]. SEBCRA uses the impact of risk on a given business-level objective (BLO) and its probability to calculate its risk level estimation (RLE). Priority of a BLO is decided by the RLE and risks are treated based on the

priority. Since SEBCRA uses semiquantitative risk assessment, choosing the most critical risks and treating them is still left to experts.

Martens and Teuteberg proposed a decision-making method when choosing a cloud computing source among multiple providers using quantified cost including risk [17]. The method provides equations of component factors with parameters decided by experts and conditions. FICO Xpress Optimization is used to optimize the cost that satisfies the linear equations [18]. This method can be combined with any risk management framework when a decision-making is necessary.

Fan and Chen proposed a risk evaluation method that qualifies identified risks using pairwise comparisons matrices [19]. After evaluating each risk to two values, frequency and severity, the method locates the risks to a quadrant space in order to visualize the effect of each risk.

Above mentioned works demonstrate that there is no effective method for risk management on immigration to cloud computing. The works are just guidelines or reports on understanding cloud computing risks. If a researcher attempts to propose a framework on the immigration situation, the lack of important features required for proper risk management, such a mitigation plan, critical asset identification, or control activities, is evident.

3. ERMOCTAVE Method

3.1. Structure of ERMOCTAVE

Although OCTAVE and ERM are good frameworks for risk management in their objectives, they are not sufficient for an organization that immigrates to cloud computing. The major advantage of OCTAVE is that three levels, IT technological department, security department, and operational units work in the combined manner. ERM pays attention to uncertainty that holds risk and opportunity at the same time. Since cloud computing is a popular IT technology with uncertainly, we suggest a combination of OCTAVE and ERM with supplements like mitigation plan step.

Basically, ERMOCTAVE is constructed by distributing ERM components to OCTAVE phases as follows [20].

Phase 1: ERM components "Internal environment" and "Objective setting" are merged to OCTAVE phase 1 (Built asset based threat profiles). Such integration helps to make threat profiles in a viewpoint of the organization's objective.

Phase 2: ERM components "Event identification" and "Risk assessment" are merged to OCTAVE phase 2 (Identify infrastructure vulnerability). Since OCTAVE has component oriented viewpoints on assets, event and risk oriented viewpoints of ERM help correct identification of vulnerabilities.

Phase 3: ERM components "Risk response", "Control activities", "Information and communication", and "Monitoring" are merged to OCTAVE phase 3 (Develop protection strategies and mitigations plans.). The ERM components enrich protection and mitigation methods of OCTAVE.

3.2. ERMOCTAVE Phase 1

In the phase, threat profiles for critical assets are reported as a result. The profiles are used to identify vulnerabilities and risks. The phase proceeds in the following 8 processes.

P1.1 Objective setting: this process defines core objectives of the organization who uses cloud computing services. From the objectives, the reason to use the cloud computing services is derived.

P1.2 Internal environment: the main roles in the organization are described in detail to identify assets and vulnerabilities in the following processes.

P1.3 Identify assets: this process creates a list of assets. The following question should be answered.

- what are important assets?

P1.4 Identify current security practices: this process creates a list of security practices in use. The following question should be answered:

- Which cloud functionalities are used to protect the important assets?

P1.5 Identify critical assets: this process selects important assets critical to the objectives. The following questions should be answered.

- Which assets largely impact on the objectives if they are disclosed to unauthorized people?
- Which assets largely impact on the objectives if they are modified without authorization?
- Which assets largely impact on the objectives if they are lost or unavailable?

P1.6 Describe security requirements for critical assets: this process clarifies security properties of critical assets. The following questions should be answered.

- Is the critical asset proprietary or sensitive?
- What is the security requirement for the critical assets? Are confidentiality, integrity, or availability important for them?

P1.7 Identify current vulnerability of the organization: this process creates a list of vulnerabilities using the following question.

- Which damage on the assets injures the objectives?

P1.8 Create threat profiles for critical assets: the goal of this process is to identify threats that affect critical assets through the vulnerabilities; the following question should be answered.

- Which potential threats have a non-negligible possibility?

3.3. ERMOCTAVE Phase 2

In this phase, risks are identified and assessed by events and vulnerability identification. The phase is composed of the following 3 processes.

P2.1 Event identification: this process identifies events that can affect on the assets.

P2.2 Review of identified vulnerabilities: this process links each vulnerability presented on the assets to each potential risk. The following question should be answered.

- Which technological vulnerabilities are presented on the assets?

P2.3 Risk assessment: inherent and residual risks are identified. "Inherent risk" is a risk that has existed in the given organization, and "residual risk" is a risk that still exists even after all controls are applied.

3.4. ERMOCTAVE Phase 3

In this phase, risks on critical assets are evaluated, and protection strategies and mitigation plans are created. The phase is composed of the following 6 processes.

P3.1 Identify risks to critical assets: the goal of the process is to link each critical asset to an identified risk.

P3.2 Create risk evaluation criteria and evaluate risks: for each risk, the following question should be answered.

- Which degree of impact is imposed on the organization's impact area, e.g., reputation, productivity, and customer confidence?

Also, the process defines the risk evaluation criteria required to understand qualitative measures of the impacts. The following questions should be answered in order to design the risk evaluation criteria.

- What defines the degree of each impact such as high, medium, or low?
- What is the evaluation value of each degree of impact—high, medium, and low?

If the number of risks is large and the evaluation is difficult, even for experts, a methodology proposed by Fan and Chen can be used [19]. In the simple case, the risk score, RS_k, for risk k is defined as follows [21].

$$RS_k = \sum_{i=1}^{I} r_{ki} v_{ki} \quad (1)$$

where

- I: the number of impact areas
- r_{ki}: ranking of impact area i on risk k ($r_i = 1, 2, \cdots, I$), high ranking has high value of r_{ki} and rankings are different for each. That is, $r_{ki} \neq r_{kj}$ if $i \neq j$.
- v_{ki}: impact value of impact area i on risk k. The values are decided by experts, for example, low (1), medium (2), and high (3).

P3.3 Create risk response and protection strategy: risk response is identified for each identified risk. Four types of risk responses are used, as follows [22].

- Avoidance: provides activities to eliminate the risk.
- Reduction: implements control activities and takes actions to reduce the risk likelihood, risk impact, or both.
- Sharing: reduces risk likelihood by transferring to or by sharing a portion of the risk with other subjects or organizations.
- Acceptance: takes no action against the risk likelihood or impact.

After determining risk responses, the goal of this process is to develop a protection strategy. The following key questions can be used during this activity.

- Which training innovation could help the organization adopting cloud computing to improve its security posture?
- How to ensure that all staff in the organization using cloud computing understands their security roles and responsibilities?
- What can be done to improve protection of an organization when dealing with external partners?
- How to ensure that all staff are aware of business continuity and disaster recovery plans?

P3.4 Create risk mitigation plans: the goal of the process is to make a risk mitigation plan using the following questions.

- Which risk will be mitigated immediately?
- Which risk will be mitigated later?
- What actions could be taken to make the mitigation plan?

P3.5 Control activities: the mitigation plan composed of control activities is implemented in this process. The types of controls will be preventive, detective, manual, or automated.

P3.6 Identify next steps and monitoring: The senior managers must identify the next steps, which will be considered after implementing the mitigation plans though the following questions:

- Which security points should be reviewed?
- How can senior managers support the initiative of security improvement?

- What are the plans for ongoing security evaluation activities?

Management must continue to monitor the effectiveness of the entire ERMOCTAVE to verify that the program adequately addresses the relevant risks and facilitates achieving the cloud computing objectives.

4. Case Study with Microsoft Azure Cloud

Selecting a good cloud vendor is an important step during the decision-making process of immigration to cloud computing. Instead of including the step in the proposed infrastructure, we propose two papers: Baldwin et al. recommended cloud computing environments that work as stable ecosystems for better risk management [23], and Martens and Teuteberg proposed a decision model that computes cost for each cloud source and property of a company who tries to adopt cloud computing. Baldwin et al. insisted that a cloud computing system evolves by overcoming attacks from outside and by adopting new concepts and technologies if the system is constructed as an ecosystem with interacting customers, software vendors, and a cloud platform. The feature of Martens and Teuteberg's model is that it outputs costs as the decision background. Thus, it helps decision-making when selecting a cloud computing for immigration quite directly.

We borrow a scenario where an organization adopts cloud computing from a Microsoft Azure manual [24]. Since Microsoft Azure takes 15.2% market share in worldwide cloud infrastructure, it is a good choice with stable ecosystem especially for Microsoft Windows users [25]. The scenario involves a company who uses a web application called 'orders application' to sell products over the Internet, quite common situation for small company to immigration toward cloud computing. As an Internet-focused organization, it has partnered with external companies that provide services such as transport and delivery. The transport partner merely needs to be advised when an order is made and may also advise the company when delivery to the customer has been done.

Although the order is being used for the business interface, other on-premises applications are used for invoicing, supplier orders, planning management and more. However, this case study only deals with the order's application and its integration with other systems, such as the main management and monitoring applications on-premises.

The company adopts cloud computing to the web application using Microsoft Azure, which is used as a platform for new services and extended capabilities. The company aims to reduce on-premises office costs by exploiting new technologies such that the business offerings in the cloud. Although we are aware of the desire to keep the availability of existing applications to support an immense customer base, the company is willing to invest in the new services development and the change of existing services to enhance the profitability. This includes dealing ahead for concerns such as increased request for their services, offering better business information capabilities, enhancing application availability and performance, and dealing with complexity by, for example, adding external partners.

In our scenario, some vital functions like management/operations applications and some databases are not located in the cloud but on premises. Separated transport partners perform transport and delivery functions. They may use cloud-based services by themselves, but this does not affect the company's application design and implementation.

4.1. On-Premises Order Application

In the original implementation, all applications ran on premises and data was stored in a local database server, as shown on Figure 1. The orders application was created as two separate components: the order's application (the website and business logic) and the suite of management and reporting applications.

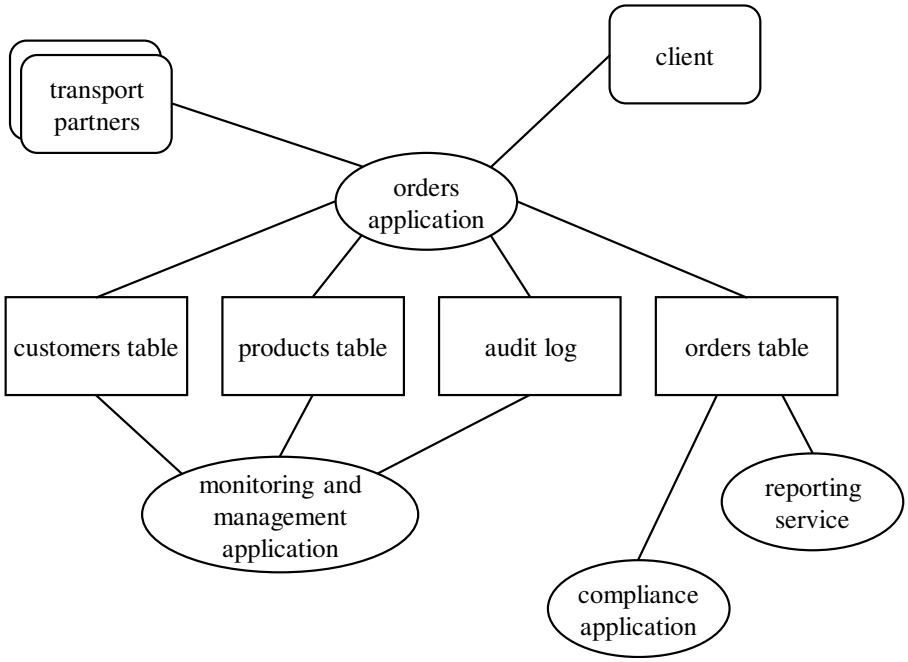

Figure 1. Applications running on premises.

Additionally, the order's application would require the ability of scaling to accommodate the expected growth on demand and to change over time, while the management and reporting applications would not require scaling ability to anything like the same extent.

4.2. Azure Hybrid Application

In the scenario, the company adopts an existing infrastructure into Azure hybrid cloud by migrating resources and applications to the cloud. Applications running across the cloud and on-premises use the Azure SQL platform in the same or different cloud data centers and resources on premises. Figure 2 shows the scenario architecture implemented for the hybrid application. In this figure, the orders application operates in much the same way as when it ran entirely on premises. Dashed undirected edges indicate control flows including small amount of data between entities. Dashed directed edges mean one way data flows especially for data replication. More details about the components and implementation of each part of the application are explained below.

- Orders application: it is a web application that allows visitors to make orders for products. It stores the data in Azure SQL which would distribute the data over different cloud data centers.
- Orders table: when a customer issues an order, the orders application receives the order and stores it into orders table. The orders table is updated whenever a customer makes an order, orders are shipped by the transport partners, and the product is delivered to the customers.
- Audit log: it is a database table for management and monitoring of the applications.
- Customers table: it contains client information.

- Products table: it contains product information. Products table and customers table are updated on premises in conjunction with the related on-premises processes. Since duplications exist in the tables located in each data center, a data synchronization mechanism should work.
- Reporting service: two types of reporting services are available using the Azure SQL service:
  - SQL server reporting service: it creates comprehensive reports of business intelligence from stored tables in the database.
  - Azure SQL reporting service: a service provided by Azure and generates a set of customized business intelligence reports.
- Azure SQL: Azure SQL is a database service that fully supports SQL-based operations. It is implemented by SQL server instances in cloud data center.
- Compliance application: it examines orders on compliance with export restrictions and government regulations for technical products.
- Monitoring and management application: it monitors daily operations, holds logging, and is used for audit on data accesses.
- Security manager: the security manager is responsible for monitoring the entire security operation by implementing security policies, regulations, rules, and ensuring that Azure cloud is securely deployed and used by employers and visitors. The security manager also delegates tasks and duties to staff. One of the security manager's main duties is to control customer accesses to the orders application.
- Social identity providers: Social identity refers to an identity managed by an established online identity provider. Social identity providers generate identifiers for users who connect servers that allow the identifiers. This can be achieved using an authentication system verifying a security token. As an example, Azure cloud enables users to log in with their Facebook credentials. In this case, Facebook is considered as a social identity provider.

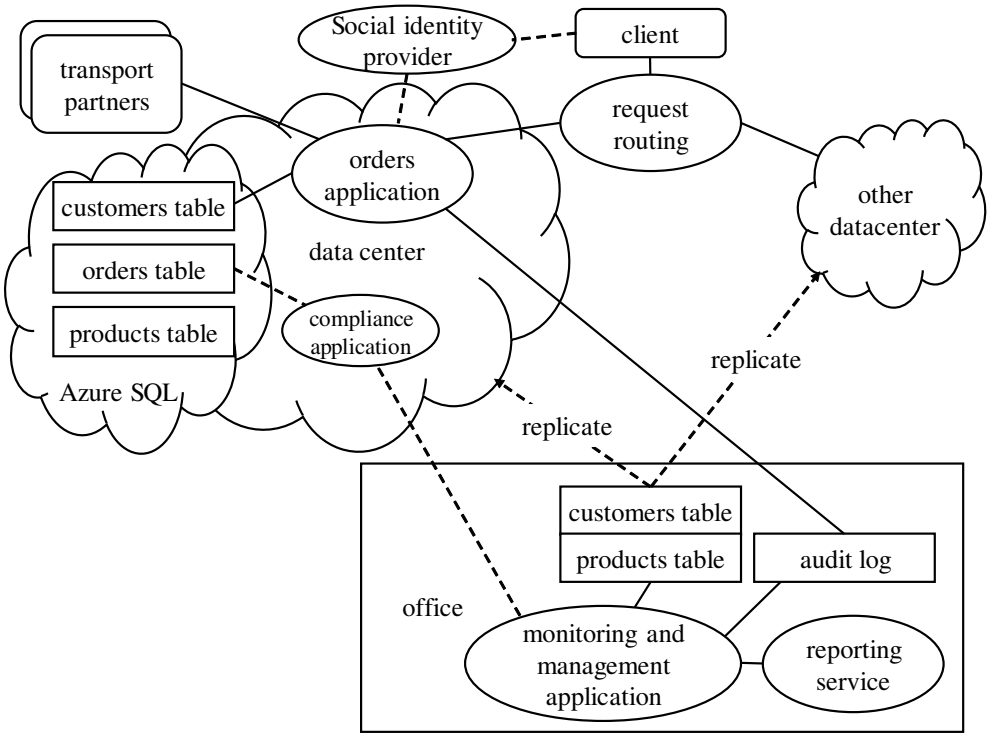

Figure 2. The example application running on cloud and on-premises.

After applications migrating to Microsoft Azure cloud infrastructure, the functionalities between modules are as follows.

- Every customer's request passes through Azure traffic manager which redirects it to the orders application running in the closest cloud data center.
- A social identity provider is used to authenticate customers.
- When a customer makes an order, the orders application stores the order details in the orders table, sends a message to an appropriate transport partner, and then sends any audit information to the monitoring and management application on premises.
- The compliance application continually validates the orders for checking their conformance with legal restrictions and notifies those requiring attention to the security manager. It also produces daily report to the monitoring and management application.
- When delivering the order to the customer, a transport partner sends a message to the orders application so the orders table can be updated.
- To obtain management information, the reporting service application on premises generates reports using the Azure SQL reporting service located in the cloud. These reports can be accessed by specific external users (e.g., remote partners and employees).

4.3. Applying ERMOCTAVE Phase 1

P1.1 Objective setting

- Objectives: In our scenario, the business of the company is to manufacture specialist electronic components for online sale. It aims to maximize capacity to process customer orders, which results in increased company profit. At the same time, its security capability should prevent any problem occuring from network security pitfalls.

P1.2 Internal environment

- Risk management philosophy: migration of existing on-premises applications to Azure cloud is not direct and it requires considerable effort and redesign to maintain reliability, performance, and security. Cloud services are relatively safe. Therefore, connection between cloud and the applications should be closely observed.
- Internal people: there are developers who know about various Microsoft products and technologies including Microsoft SQL Server, Microsoft Visual Studio, and Microsoft Azure cloud technology. The developers hope to use any of the available features that can help to ease their tasks. The security manager decides how the tasks are accomplished by assigning the tasks to the proper people. The transport and delivery functions are performed by separate transport partners which use their own IT services, but this has no impact on applications of the company's cloud infrastructure.

P1.3 Identify assets

Assets to protect

- Information: orders table, audit log, customers data, and product data.
- Systems: orders application, SQL reporting service, Azure SQL, compliance application, and monitoring and management application.
- Hardware: server on premise.
- People: developers and security manager.
- External: transport partners, external access to reports, and social identity providers.

Important assets

- Information
  - Orders table: orders table is an important asset because it is only located in the cloud data center, close to the orders application and it stores all details of orders made by customers.
  - Customers table: customers table is an important asset because it is needed in order to authenticate visitors and to accept orders from them. Also, customer data is used by a bidirectional synchronization mechanism to replicate information between on-premises network and all cloud data centers hosting the order's application.
- Systems
  - Orders application: it is an important asset because it receives all customer's orders.
  - Azure SQL: Azure SQL is an important asset because it provides data synchronization across cloud and on-premises databases using Azure data sync function.
- Hardware
  - Server on premises: server is an important asset because it monitors all data (orders, customers, products, and audit log) on premises and maintains all on-premises capabilities efficiently.
- External
  - Transport partners: through an automated monitoring, they proactively manage the life cycle of orders and shipments.
  - Social identity providers: they provide authentication mechanism enabling users to access the order application.

P1.4 (Identify current security practices) it deals with actual actions taken to protect important assets.

- Authentication for accessing the orders application uses Azure Access Control Service (ACS) which is a way of authenticating access to web applications and services (Microsoft owned cloud-based service) [24]. ACS can be configured to act as both the token issuer (STS) and the identity provider.
- Reliable messaging and communications are required when orders are passed to various transport partners for shipping and are stored for audit and compliance purposes. Such messaging and communication are implemented using Azure service bus, which is a cloud messaging system that connects everything (applications, devices, and services), wherever they are located on cloud, on-premises, or both.
- In order to make order processes by customers reliable and scalable, it must be stored and not be lost. Azure service bus topics and queues are provided in order to achieve the needs [26]. The orders applications run in more than one cloud data center. Each orders application owns its set of subscriptions with Azure service bus topics and queues. Each transport partner receives orders from a subscription in any of cloud data centers, and posts response messages back to the queue in the data center [24].
- Synchronization of data across cloud and on-premises locations is provided using Azure SQL data sync. It is a data synchronization service between data centers and services. Azure SQL data sync provides a lot of options such as unidirectional and bi-directional synchronization.
- Maximization of scalability and control of elasticity in the orders application is implemented using Azure autoscaling application block, which is a service that automatically scales Microsoft Azure applications based on defined rules [24]. We can choose a host location for a block between in Azure and on premises application. After that, Azure autoscaling application block provides the capabilities required.
- Maximization of performance in orders application requires efficient management of network latency and maximizing connectivity to the orders application. The ability is provided by Azure traffic manager which routes customer's requests. Azure traffic manager allows setting up

request routing and loads based on predefined policies and rules. It provides a way of routing requests to multiple deployments of Azure applications and services regardless of the cloud data center location. Azure caching service improves response time and contributes to the application performance.

- Maximization of availability in order applications is done by Azure autoscaling application block too.

P1.5 Identify current organizational vulnerabilities

- Unclear service-level agreement (SLA): A SLA is a standardized contract between a service provider and an end user where a service is formally defined [27]. In our scenario, SLA has not been documented and described against Azure cloud services. It is important to specify that in cloud computing, because SLA gathers information on all the contracted services and their agreed expected reliability in one document. It clearly specifies expectations, metrics and responsibilities so if there is any issue with the service, neither party can ignore it. SLA ensures that both sides have a common understanding of the requirements. Therefore, lacking an established SLA creates a huge vulnerability in our Azure cloud.
- User's authentication and authorization requests in the cloud: the orders application authenticates and authorizes visitors. Traditionally, authentication is carried out in local. Progressively users expect services to be enabled using universal credentials like Windows live, Google, or Facebook. It is called federated authentication, and it provides the opportunity to support single sign-on (SSO) function. With SSO, users sign in to one application using unique credentials (Windows Live ID for example) and can visit other sites that support the credential without authenticating again [28]. However, SSO has some weaknesses: lack of stronger authentication such as using smart cards. If the SSO fails out, users would lose access to all sites as single point of failure, or an intruder can access assets through a crack point.
- Unsafe on-premise assets: cloud storage remotely maintains, manages, and backs up data [29]. This service enables the users to save files online, so that they can access them from any location. However, for data stored on premises, if the premise catches on fire or the computer server gets stolen, we will not be able to retrieve data since there is no activated backup system. There is lack of backup processes and disaster recovery plan.

P1.6 Identify critical assets

Which assets will largely impact the organization if they are confidentiality disclosed to unauthorized people?

- Server on premises: if the local server is disclosed to unauthorized people, information for monitoring services, logging activity of the orders application, and reporting service would be wrongly exploited and be used for bad purposes. The audit log data which has sensitive information against public would be hijacked and may pollute reputation of the company.
- Orders table and customers table: it contains private information. Its exposure may affect reputation of the company.

Which assets will largely impact the organization if they are modified without authorization? (integrity)

- Order applications: if the order's application is modified without legal authorization, all orders made by customers may be wrongly directed and the result of delivery from transport partners would be a disaster.
- Azure SQL: it is a database service fully supporting SQL-based operations. If some changes are made without valid authorization, this would create malfunctions on orders table, customers table, and products table.

Which assets will largely impact the organization if access to them is interrupted? (availability)

- Orders table: the orders application reads the order table in order to display the current orders list and to send delivery information to users. If access to the order table is interrupted, orders cannot be consulted by orders application and customers would not receive what they ordered.
- Transport partners: if an access to transport partners is interrupted, delivery systems would not work.

P1.7 Describe security requirements for critical assets: from P1.6, critical assets are listed, and security requirements are enumerated as follows.

- Server on premises: confidentiality, integrity, and availability.
- Orders table: confidentiality and availability.
- Customers table: confidentiality.
- Order's application: integrity.
- Azure SQL: integrity.
- Transport partners: availability.

Integrity is not requirement for the tables because it is guaranteed by applications' integrity.

P1.8 Create threat profiles for critical assets: which potential threats can be non-negligible to the critical asset?

- Intruder willing to access the orders application.
- Insufficient quality of outsourcing services and transport partners.
- Unauthorized people physically intruding the server on premises.

4.4. Applying ERMOCTAVE Phase 2

P2.1 Event identification: events that can effect on the assets are identified.

- Excessive requests to the orders application including DDoS attacks.
- Malfunction of the server on premises.
- Intruders disclose or modify database tables or applications.
- Network failure.
- Services of partners are degraded or unavailable.

Since only the orders application is accessible in public, other component like server on premises is safe from the event. The DDoS attacks can be protected by Azure DDoS protection.

P2.2 Review of identified vulnerabilities: Which vulnerabilities are present on each evaluated cloud infrastructure component?

- Lack of SLA: applications and tables in cloud.
- Single Sign-on (SSO) as single point of failure, limited authentication mechanisms: applications and tables in cloud.
- Lack of backup processes and disaster recovery plan: applications and tables on premises.

P2.3 Risk assessment

Keeping in mind that risk is the result of a vulnerability being exploited by a threat [26], we can identify potential risks in our scenario as follows:

- Risk 1: if the vulnerability "Lack of Service Level Agreement (SLA)" is exploited by the threat "need of outsourcing services and additional transport partners", it would result in risk "impossibility of outsourcing and contracting with transport partners".
- Risk 2: if the vulnerability "Single Sign-on (SSO) as single point of failure" is exploited by the threat "Intruder willing to access orders application", it would result in risk "Azure cloud intrusion".

- Risk 3: if the vulnerability ”lack of back up processes and disaster recovery plan” is exploited by the threat ”breaking of physical controls”, it would result in risk ”data (customers, orders, products, and audit log) loss on premises”.

Inherent risks: the following is considered as an inherent risk because it is a risk caused by the absence of any action to control.

- Risk 1: ”impossibility of outsourcing and contracting with transport partners”.

Residual risks: the followings are considered residual risks because they will remain after mitigation is considered (risk after controls).

- Risk 2: “Azure cloud intrusion”.
- Risk 3: “Data loss on premises”.

4.5. Applying ERMOCTAVE Phase 3

P3.1 Identify risks to critical assets

We link each critical asset to a specific identified risk.

- Database Server on-premise (Risk 3: “Data loss on-premises”).
- Orders Application (Risk 2: “Azure cloud intrusion”).
- SQL Azure, order’s table/data, and transport partners (Risk 1: “Impossibility of outsourcing and contracting with transport partners”).

Which critical assets are targets of human threat actors?

- Database server on-premise.

What are the motives for each human threat actor that might use physical access to violate the security requirements of this critical asset?

- To see logging activity, customers sensitive information, and reporting service.

P3.2 Create risk evaluation criteria and evaluate risks

- Risk evaluation criteria: we review the risk evaluation criteria and focus on how to define high, medium, and low impact. We borrow the following impact areas from OCTAVE; reputation, customer confidence, productivity, and fines/legal penalties (the number of areas $I = 4$) [30]. The ranking of the value r_i and impact value v_i of each impact area is decided by the security manager. The notes in Table 1 explain the reason of imposing impact degree on each impact area. In the case study, impact values are assigned quantitative values as follows; High (3), Medium (2), and Low (1). Ranking of each impact area is decided by the security manager and is listed in the ranking column of Table 2. Risk scores calculated using Equation (1) are listed in the risk score row of Table 2. We total the score column, which is the relative risk score.
- Risk evaluation: Tables 1 and 2 show risk evaluation criteria and risk score calculation for risks 1–3.

Table 1. Impact degree and its reason of impact areas. (a) Risk 1 (impossibility of outsourcing and contracting with transport partners), (b) risk 2 (Azure cloud intrusion), and (c) risk 3 (data loss on premises).

(a)

Impact Area	High (3)	Medium (2)	Low (1)	Notes
Reputation	O			Reputation is destroyed.
Customer confidence	O			Huge drop in customers due to loss of availability.
Productivity		O		Inability to access order table to deliver products.
Fines/legal penalties	O			High profile, deep investigation of the person who violates the rules.

(b)

Impact Area	High (3)	Medium (2)	Low (1)	Notes
Reputation		O		Unauthorized access to the orders application affects how the company is viewed from externals.
Customer confidence	O			The orders table privacy is highly violated, and sensitive information can be hijacked.
Productivity			O	The intrusion may get unauthorized access on orders application, but it would not stop the cloud to deliver orders.
Fines / legal penalties	O			Investigations should operate in depth and huge fines could be imposed if the intrusion comes out to be quality.

(c)

Impact Area	High (3)	Medium (2)	Low (1)	Notes
Reputation		O		News about the data loss may affect reputation of the company.
Customer confidence			O	Online shopping process does not stop because necessary information is stored in cloud.
Productivity			O	There are a little or no delay on order and delivery processes because the processes use data in cloud.
Fines/legal penalties		O		People responsible of this data loss must be under investigation.

Table 2. Risk scores, RS_k.

Impact Area	Risk 1			Risk 2			Risk 3		
	Ranking	Impact Value	Score	Ranking	Impact Value	Score	Ranking	Impact Value	Score
Reputation	2	3	6	2	2	4	1	2	2
Customer confidence	4	3	12	4	3	12	2	1	2
Productivity	1	2	2	1	1	1	4	1	4
Fines/legal penalties	3	3	9	3	3	9	3	2	6
Risk score			29			26			14

P3.3 Create risk response and protection strategy
Risk response

- For risk 1 (impossibility of outsourcing and contracting with transport partners), the risk response is "Avoidance" and "Shared" because it has the highest risk score value 29. We consider it as top priority risk and must be immediately and fully mitigated.
- For risk 2 (Azure cloud intrusion), the risk response is "Reduction" and "Shared" because we already have an existing authentication mechanism in which we will just improve the mechanism.
- For risk 3 (data loss on premises), the risk response is "Reduction". Although risk 3 has a low risk score value 14, there are many methods to reduce the risk. For example, backup could be used to reduce the risk.

Protection strategy

- What training innovation could help an organization adopting cloud computing used to improve its security posture?
  - We update security specialist with latest technologies through specific courses on Azure cloud computing.
- How to ensure that all staff in organization using cloud understand their security roles and responsibilities?
  - We include an important example in the security awareness documentation. The example consists of severe consequences if policies are not respected (for example, access to database is temporary blocked or suspended from work).
- What can be done to improve resource protection of an organization when dealing with external partners?
  - We include all procedures in SLA and outsourcing contracts in the content security policy (CSP) [31].
- How to ensure that staff is aware of business continuity and disaster recovery plans?
  - We include the business continuity and disaster recovery plans for the on-premises policies and procedures.

P3.4 (Create risk mitigation plans)
Which risks will be immediately mitigated?

- Risk 1 (impossibility of outsourcing and contracting with transport partners)

Which risks will be mitigated later?

- Risk 2 (Azure cloud intrusion)
- Risk 3 (data loss on-premises)

What actions could be taken to make the mitigation plan?

- For risk 1 (impossibility of outsourcing and contracting with transport partners), the service-level agreement must be made, although it is not specified at the contract at the first time. In the case of SLA with cloud computing, QoS is specified. If the service quality gets down below the QoS, compensation is given by the cloud company. If interactions against the transport partners do not work because of protocol, secure annotation representation can be considered [32].
- For risk 2 (Azure cloud intrusion), we can accept Azure multifactor authentication on the server.

- For risk 3 (Data loss on premises), we install Azure backup server on premises. Microsoft Azure backup server offers on-premises backup and online backup. We can select a subset or all of the backup data in the local repository and forward them to an Azure backup service [33].

P3.5 Control activities

Service-level agreement establishment (mitigation of risk 1 (Impossibility of outsourcing and contracting with transport partners)).

- Check if every service has corresponding SLA.
- Check if compensation of the SLA is satisfiable considering the cost which occurs from the QoS dissatisfaction.
- Check if a contact with another cloud service is necessary considering the QoS unsatisfaction of Azure cloud.

Multifactor authentication (mitigation of risk 2 (Azure cloud intrusion))

- Azure multifactor authentication server from Azure portal can be used for reducing the probability of intrusion.

Azure backup and disaster recovery plan (mitigation of risk 3 (Data loss on-premises))

- Azure backup server is used for backup on premises.
- In order to recover data from failure, Azure backup vault is created and managed.

P3.6 Identify next steps and monitoring: As a summary and suggestions of the entire process, the output can be a form as shown in Table 3.

Table 3. Security review, management, and plans.

Category	Title	Contents
review	security policies	• review policies and procedures regarding Azure cloud at all levels and actively enforce them. • review all policies and procedures; compare them to other cloud infrastructures considered to have best in practices. • make sure that IT laws and regulations are incorporated into policies, procedures, and training.
	physical security	• review, update, and enforce our policies on database on premises.
management	security management	• allocate greater funds for cloud system security. • clearly define responsibilities of staff and communicate it to all personnel.
	collaborative security management	• update current policies for working with third parties.
	staff security	• clearly document procedures for incident identification.
plan	security awareness and training	• provide all new employees with baseline training about Azure cloud computing. • provide annual training in cloud physical security for all staff.
	disaster recovery plan	• review contingency plans and procedures annually. • update business continuity plan.
	physical security	• establish a policy in which internal and external personnel are responsible for physical security.

5. Functionality Comparison

The functionality of the proposed ERMOCTAVE is compared with ENISA cloud risk assessment and Microsoft cloud risk assessment based on ISO 31000. Table 4 shows a comparison between the three frameworks.

Table 4. Functionality comparison of risk management frameworks.

Function	ERMOCTAVE	ISO 31000	ENISA
key objectives and strategies	O	X	X
critical asset	O	X	X
risk impact criteria	O	X	X
risk impact	O	O	O
risk likelihood	O	O	O
specification of inherent and residual risk	O	X	X
risk response	O	O	X
mitigation plan	O	X	X
risk control area	X	O	O
dedicated method	O	O	X

The table shows that ERMOCTAVE method has some important features that the ISO 31000 Cloud Risk Framework and ENISA cloud risk assessment fail to provide. These features and their role in the cloud risk management process are specified below.

- Key objectives and strategies establishes a philosophy regarding risk management in the cloud computing by recognizing that unexpected and expected events may occur [34].
- The critical asset is the most important asset in the cloud computing network. The organization would be largely impacted if something happens to critical assets [35].
- Risk impact criteria which defines and specifies quantitative measures that are used to evaluate a risk's effect on the organization's mission and business objectives.
- Specification of inherent risk refers the level of risk where no control is applied, while specification of residual risk refers the level of risk where all controls are applied.
- Risk response provides options and determines actions to enhance opportunities and to reduce threats to the objectives. It includes the identification of actions and decisions on each agreed risk response [36].
- Mitigation plan refers as action plan to reduce the impacts of the identified risks, even before any damage or disaster takes place. Risk mitigation plans incorporate a list of actions designed to counter the threats linked to each asset. It also serves as the security manager's checklist for monitoring.
- Dedicated method: Other approaches are only guidelines and documentations while ERMOCTAVE method is a dedicated and core framework which provides a detailed methodology.

6. Conclusions

The paper proposes a risk management method, ERMOCTAVE, for dealing with risks that arise when an organization uses cloud computing as a part of its system. The proposed method combines the Enterprise Risk Management framework and Operationally Critical Threat, Asset, and Vulnerability Evaluation method with a proper assessment of cloud computing risks. ERMOCTAVE identifies critical assets of cloud computing and links different risks to each specific asset.

Unlike the previous approaches, which are only guidelines or documentations and do not provide the plan of mitigating and controls activities, ERMOCTAVE is a dedicated and core framework providing a detailed mitigation plan and control actions of each identified risk of the organization with cloud computing.

After applying ERMOCTAVE to a chosen Azure cloud scenario, the results are compared with exiting methods (ENISA and Cloud Risk Assessment). The comparison shows that ERMOCTAVE provides important features of effective risk managements in cloud computing.

There are various avenues for further research regarding risk management on cloud computing immigration. One direction is to introduce additional features, like risk appetite, to provide full detail to specific risk identification, such as a risk profile tree. It would be interesting to analyze risk communication by which results of assessment are transferred to decision makers or the public. Good risk communication is essential in explaining official policies to stakeholders, containing relations between risk, cost, and benefit, in detail. Future research is to evaluate and analyze effects of adding more risk criteria. It might allow us to identify risks from new area impacting the cloud computing.

Author Contributions: Conceptualization, S.-Y.S.; Formal analysis, T.-Y.C.; Investigation, M.M.; Project administration, T.-Y.C.; Supervision, T.-Y.C.; Validation, S.-Y.S.; Writing—original draft, M.M.; Writing—review & editing, T.-Y.C.

Funding: This research was conducted during the sabbatical year awarded by Kumoh National Institute of Technology.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Regenscheid, A.; Scarfone, K. *Recommendations of the National Institute of Standards and Technology*; NIST Spec. Publ.: Gaithersburg, MD, USA, 2011; pp. 2–3.
2. Crawshaw, J. *Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide*; The Santa Fe Group: NM, USA, 2019; pp. 8–9.
3. Ferguson, T. Salesforce.com Outage Hits Thousands of Businesses. Available online: https://www.cnet.com/news/salesforce-com-outage-hits-thousands-of-businesses/ (accessed on 9 September 2019).
4. Threat, Vulnerability, Risk - Commonly Mixed up Terms. Available online: https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/ (accessed on 19 June 2019).
5. Alberts, C.; Dorofee, A.; Stevens, J.; Woody, C. *Introduction to the OCTAVE Approach*; Technical Report; Software Engineering Institute: Carnegie-Mellon University, Pittsburgh, PA, USA, 2003.
6. Bediako, T. Enterprise Risk Management - Integrated Framework. In Proceedings of the ISACA's IT Audit, Information Security & Risk Insights Africa, Alisa Hotel, Ghana, 20 May 2014.
7. De Hert, P.; Papakonstantinou, V.; Kamara, I. *The New Cloud Computing ISO/IEC 27018 Standard through the Lens of the EU Legislation on Data Protection*; Technical Report; IEC: Geneva, Switzerland, 2014.
8. Catteddu, D. Cloud Computing: benefits, risks and recommendations for information security. In Proceedings of the Iberic Web Application Security Conference, Madrid, Spain, 10–11 December 2009; p. 17.
9. Dekker, M.; Dimitra, L. *Cloud Security Guide for SMEs*; ENISA: Heraklion, Greece, 2015.
10. Hubbard, D.; Sutton, M. *Top Threats to Cloud Computing v1.0.*; Cloud Security Alliance: Seattle, WA, USA, 2010; pp. 1–14.
11. Ouedraogo, M.; Mignon, S.; Cholez, H.; Furnell, S.; Dubois, E. Security transparency: The next frontier for security research in the cloud. *J. Cloud Comput.* **2015**, *4*, 1–12. [CrossRef]
12. Badger, L.; Grance, T.; Patt-Corner, R.; Voas, J. *Cloud Computing Synopsis and Recommendations*; NIST Spec. Publ.: Gaithersburg, MD, USA, 2012.
13. Hogan, M.; Liu, F.; Sokol, A.; Tong, J. *Nist Cloud Computing Standards Roadmap*; NIST Spec. Publ.: Gaithersburg, MD, USA, 2011; pp. 6–11.
14. ISACA. *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*; ISACA: Schaumburg, IL, USA, 2011.
15. Stone, G.; Noel, P. *Cloud Risk Decision Framework*; Technical Report; Microsoft: Redmond, WA, USA, 2015.
16. Fitó, J.O.; Macías, M.; Guitart, J. Toward business-driven risk management for cloud computing. In Proceedings of the 2010 International Conference on Network and Service Management, Niagara Falls, ON, Canada, 25–29 October 2010; pp. 238–241.

17. Martens, B.; Teuteberg, F. Decision-making in cloud computing environments: A cost and risk based approach. *Inf. Syst. Front.* **2012**, *14*, 871–893. [CrossRef]
18. FICO Xpress Optimization. Available online: https://www.fico.com/en/products/fico-xpress-optimization (accessed on 9 September 2019).
19. Fan, C.K.; Chen, T.C. The risk management strategy of applying cloud computing. *Risk Manag.* **2012**, *3*. [CrossRef]
20. Mackita, M. ERMOCTAVE: A Novel Risk Management Method for Cloud Computing Security. Master's Thesis, Kumoh National Institute of Technology, Gumi, Korea, August 2016.
21. Brunschwiler, C. Lean Risk Assessment Based on OCTAVE Allegro. Available online: https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/ (accessed on 18 June 2019).
22. Pieplow, B.U. Project Risk Management Handbook: A Scalable Approach. *Risk* **2012**, *1*, 27–29.
23. Baldwin, A.; Pym, D.; Shiu, S. Enterprise information risk management: Dealing with cloud computing. In *Privacy and Security for Cloud Computing*; Springer: London, UK, 2013; pp. 257–291.
24. Homer, A.; Narumoto, M.; Sharp, J.; Zhang, H.; Densmore, S. *Building Hybrid Applications in the Cloud on Windows Azure*; Microsoft Patterns & Practices: Redmond, WA, USA, 2013.
25. Canalys. Cloud Infrastructure Services Spend up by US$7.2 Billion in Q2 2019, Driven by Cloud Migration. Available online: https://www.canalys.com/newsroom/cloud-market-share-Q2-2019 (accessed on 18 June 2019).
26. Chappell, D. *Introducing the Windows Azure Platform*; David Chappell & Associates: San Francisco, CA, USA, 2010.
27. Hiles, A. *The Complete Guide to IT Service Level Agreements: Aligning IT Services to Business Needs*; Rothstein Associates Inc.: Brookfield, CT, USA, 2002.
28. Topal, B. Comparison of Methods of Single Sign-On: Post Authentication Methods in Single Sign on. Available online: https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/160302-BaranTopal-with-cover.pdf (accessed on 18 June 2019).
29. Matchett, M. Integrate cloud storage with on-premises arrays. *Storage* **2015**, *14*, 8–12.
30. Alberts, C.J.; Dorofee, A. *Managing Information Security Risks: The OCTAVE Approach*; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 2002.
31. Sterne, B.; Barth, A. *Content Security Policy 1.0.* Technical Report, W3C Working Group, 2015. Available online: https://www.w3.org/TR/CSP1/ (accessed on 19 June 2019).
32. Karam, Y.; Baker, T.; Taleb-Bendiab, A. Security support for intention driven elastic cloud computing. In Proceedings of the 2012 Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation, Valetta, Malta, 14–16 November 2012; pp. 67–73.
33. Rayne Wiselman. Back up Windows Machines with the Azure Backup MARS Agent, 2019. Available online: https://docs.microsoft.com/en-us/azure/backup/backup-configure-vault (accessed on 15 August 2019).
34. Dafikpaku, E.; Eng, M.; Mcmi, M. The strategic implications of enterprise risk management: A framework. In Proceedings of the ERM Symposium, Chicago, IL, USA, 14–16 March 2011; Volume 48.
35. Behnia, A.; Rashid, R.A.; Chaudhry, J.A. A survey of information security risk analysis methods. *SmartCR* **2012**, *2*, 79–94. [CrossRef]
36. Radack, S. *Managing Information Security Risk: Organization, Mission and Information System View*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.