Sustainability **2015**, *7*, 12032-12051; doi:10.3390/su70912032

OPEN ACCESS

sustainability

ISSN 2071-1050

www.mdpi.com/journal/sustainability

Article

Information Security Management as a Bridge in Cloud Systems from Private to Public Organizations

Myeonggil Choi [1,†] and Changhan Lee [2,†,*]

[1] Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul 156-756, Korea; E-Mail: mgchoi@cau.ac.kr

[2] Dongguk (Seoul) Univeristy, 1 Pildong-ro, Jung-gu, Seoul 100-715, Korea

[†] These authors contributed equally to this work.

[*] Author to whom correspondence should be addressed; E-Mail: lch28@dongguk.edu; Tel.: +82-22260-3248; Fax: +82-22260-3104.

Academic Editor: Marc A. Rosen

Received: 27 March 2015 / Accepted: 25 August 2015 / Published: 28 August 2015

Abstract: Cloud computing has made it possible for private companies to make rapid changes in their computing environments. However, in the public sector, security issues hinder institutions from adopting cloud computing. To solve these security challenges, in this paper, we propose a methodology for information security management, which quantitatively classifies the importance of information in cloud systems in the public sector. In this study, we adopt a Delphi approach to establish the classification criteria of the proposed methodology in an objective and systematic manner. Further, through a case study of a public corporation, we try to validate the usefulness of the proposed methodology. The results of this study will help public institutions to consider introducing cloud computing and to manage cloud systems effectively and securely.

Keywords: information classification; information security management; criteria for security measurement; Delphi approach

1. Introduction

The increasing complexity of computing environments and the increasing computing costs have encouraged enterprises and individuals to adopt cloud computing and thereby reduce their computing

investment and improve usability [1]. Private companies using huge computing infrastructures, such as Google, Microsoft, and Amazon, have actively constructed cloud computing infrastructures. However, information security issues hinder the adoption of cloud computing by public entities in spite of the high demand for cloud computing [2]. Therefore, solutions for providing security against the vulnerabilities of cloud computing will pave the way for the acceptance of cloud computing in public organizations.

For providing security for cloud computing in private entities, various approaches for information security management, such as ISO27001, Cloud Security Alliance (CSA), and European Union Agency for Network and Information Security (ENISA), have been suggested. These approaches focus on private industries and are not suitable for public entities as these approaches mainly reflect the nature of private organizations. The nature of computing in public organizations depends on a combination of factors, such as the different sensitivities of data, the general management staff for information systems, and compliance with laws and regulations [3]. Information security management systems using cloud computing reflect the nature of computing in public entities. In this study, we aimed to develop a methodology for the information security management of cloud computing in public organizations and to validate the usefulness of this methodology. The proposed methodology is expected to lessen the security vulnerabilities of introducing cloud computing to public entities, resulting in an improved security level of the public enterprises.

2. Related Works

The security issues of cloud computing have been discussed in the literature [4–6]. CIO research conducted in the U.S. has revealed [7] that the loss of rights in controlling data, availability of data, and compliance with IT governance and regulations lead to security issues in cloud computing. Gartner has reported [8] that issues related to risk management, such as those related to e-discovery, compliance with regulations, and audit, need to be resolved. As these reports mention, these security issues are the highest barrier to the introduction of cloud computing in public entities. For relatively strong security of cloud computing, various security regulations, such as CSA Security, Trust, and Assurance Registry (CSA STAR) [9], ENISA [10], and Federal Risk and Authorization Management Program (FedRAMP) [11], have been adopted, and security controls such as ISO/IEC 27001 [12] and BSI IT Baseline Protection Manual (BSI) [13] have been utilized as security management systems for cloud computing. In this study, we briefly analyze these security regulations and information security management systems.

CSA STAR ensures the consumers of the trust and assurance of a cloud provider. The CSA STAR program is designed to show the varying assurance requirements and maturity levels of cloud providers and consumers. To meet these objectives, the CSA has developed an open certification framework. The purpose of this framework is to provide an evaluation methodology for data protection and the mobility and flexibility of the cloud services to consumers. The framework consists of a three-level certification, wherein Level 1 is self-assessment, Level 2 is third-party assessment-based certification, and Level 3 is continuous monitoring-based certification. Each level implies gradual visibility and transparency of the operations in cloud computing and thus, provides the corresponding assurance to the consumers [9]. CSA STAR provides two types of research controls, namely Cloud Controls Matrix (CCM) v.3 and Consensus Assessments Initiative Questionnaire (CAIQ). CCM v.3 provides security controls, consisting of 16 control domains and 136 items utilized for a third-party assessment. Further, CCM v.3 provides

the mapping information of control items related to Cobit, PCI-DSS, and FedRAMP [11]. CSA STAR scores functions for each CCM security domain. These scores represent the maturity of processes in an organization and indicate the parts that need to be improved. The maturity levels are defined as No, Bronze, Silver, and Gold, and the certified organizations are registered as "STAR Certified" in CSA STAR. This STAR certification represents the overall evaluation of efficiencies, goals, domains, and processes of information management systems. Further, STAR conveys the priorities and the domains that need to be improved in an organization and compares the certification results of cloud providers.

The ENISA guideline [10] deals with risk assessment and divides the risks of cloud computing into policy and organization risks, technical risks, legal risks, and risks not specific to clouds. The guideline classifies vulnerabilities and assets in cloud computing and establishes 12 information assurance requirements. The guideline involves a combination of risk analysis methods to be applied to cloud computing and the corresponding set of security controls.

FedRAMP is a program providing security assessment, authorization, and continuous monitoring for cloud products and services [11]. The goals of the program are that the U.S. government efficiently certifies and delivers cloud products and services for federal agencies. In this program, a third-party audit organization (3PAO) evaluates the cloud services and products of the cloud service provider and the U.S. government certifies the provider on the basis of the evaluation results. The processes of FedRAMP are divided into four levels. First, a 3PAO is accredited at Level 1, and then, the accredited 3PAO assesses the security of cloud products and services at Level 2. At Level 3, a U.S. agency that wants to introduce cloud services and products designates a service provider from the relevant list from the security repository database. At Level 4, the 3PAO continuously monitors the approved cloud provider at least once every year. The assessment criteria are drawn from the control items of the SP 800-53 revision of National Institute of Standards and Technology (NIST). Although FedRAMP has a solid basis in certifying cloud providers, its approach demands a considerable amount of resources for establishing certification programs and strongly unites with the Federal Information Security Management Act (FISMA). The application of FedRAMP to public entities other than those in the U.S. requires significantly more effort and a well-pre-established security infrastructure [11].

ISO/IEC27001 is a popular and an internationally recognized standard for information security management systems, specifying the requirements of these systems. ISO/IEC27001 ensures that the security requirements are fine-tuned to keep pace with security environments [12]. Further, ISO/IEC27001 adopts the plan-do-check-act (PDCA) model and is not restricted to a specific industry. It defines the requirements for implementing, monitoring and auditing, maintaining, and improving information security management systems. ISO/IEC27001 defines the goals and domains of information security management systems considering the relevant businesses and organizations and the nature of the information assets and technologies owned by these organizations. On the basis of the strategy of risk processing, ISO/IEC27002 selects security controls from the standard ones. Further, ISO/IEC27005 conducts a risk analysis and defines a strategy for risk reduction, risk avoidance, and risk transfer for compliance with an information security policy.

The Federal Office for Information Security established BSI standard-100 and IT-Grundschutz Catalogues [14]. IT-Grundschutz Catalogues is a collection of modules, threat catalogs, and a safeguard catalog. Each module of IT-Grundschutz describes the applicable components, approaches, and IT systems, as well as the threat scenarios and the appropriate safeguards. IT-Grundschutz consists of five

different layers [15], which are S1 the generic security of information technology, S2 the security of the infrastructure, S3 the security of IT systems, S4 the security in networks, and S5 the actual application. Threat catalogs contain threats such as T0 basic threat, T1 force majeure, T2 organizational shortcomings, T3 technical failure, and T4 deliberate acts. The safeguard catalog contains a description of the security safeguards mentioned in the module, and is defined as S1 infrastructure, S2 organization, S3 personnel, S4 hardware and software, and S5 communication. GSK (IT-Grundschutz Catalogues) classifies risks through combinations of threats and safeguards for a designated module [16]. BSI standard 100-1 defines the requirements for ISMS [17]. BSI standard 100-2 (IT-Grundschutz Catalogues: GSK) describes how to establish and monitor security based on the standard of security safeguards [18]. BSI standard 100-3 discusses a method for analyzing risks that is based on IT-Grundschutz (BSI standard 100-2) [19]. BSI-Standard 100-4 describes business continuity management. BSI standards and IT-Grundschutz Catalogues are well-defined standards in that the methodology systematically combines the threat and the corresponding safeguard for a specific layer. In terms of feasibility, it demands considerably more resources to establish and manage information security systems.

3. Information Security Management Systems for Cloud Computing in Public Organizations

This study analyzes the representative methodologies for cloud systems, such as FedRAMP and ENISA's security management, and proposes a methodology for the security management of cloud systems in public organizations.

3.1. FedRAMP

For the security management of cloud systems, FedRAMP utilizes NIST special publication 800-60. To introduce suitable security controls for cloud systems, FedRAMP categorizes cloud systems in terms of their impact level. NIST special publication 800-60 categorization determines the security impact level for the cloud environment that may host any or all of the service model information as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The goal of the security categorization is to help the cloud service provider (CSP) to select and implement the FedRAMP security controls applicable to its environment [11].

The categorization is based upon NIST special publication 800-60. An analysis of the data contained in the systems will determine whether the security categorization for the systems is at the low, moderate, or high impact level. The security categories are determined upon the potential impact on an organization when certain events occur [20].

FedRAMP defines three levels of potential impact on organizations or individuals when a breach of security events (*i.e.*, a loss of confidentiality, integrity, or availability) occurs. Conducting an appropriate security category for a cloud system simply requires determining the potential impact for each security objective of the particular cloud systems. For the categorization of cloud systems, the following processes are required. First, identify the relevant cloud systems and the document organization's business and mission area. Second, identify the cloud information that are input, stored, processed, and/or output from each system. Third, select the security impact level for the identified information type on the basis of qualitative criteria. Security category of cloud systems = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the values for potential impact are low, moderate, or high. The resulting

security level of the cloud systems is decided on the basis of the highest value among confidentiality, integrity, and availability. Fourth, adjust the impact levels for reflecting situations, operational drivers, and legal reasons related to the organization. Fifth, determine the security impact level of cloud systems on the basis of the aggregate of information type.

The completed security categorization will help the CSP in the selection and implementation of FedRAMP security controls at the determined categorization level. The FedRAMP program takes into account that systems may vary between vendors and allows some flexibility in the implementation of compensating controls or in alternative implementations.

3.2. Security Framework for Government Clouds by ENISA

ENISA adopts the Plan–Do–Check–Act (PDCA) model identified as a suitable model for information security management systems in government cloud systems. In the Plan phase, the security policy is set for implementing controls to achieve security objectives. In the Do phase, the controls are implemented and operated. In the Check phase, a review and an evaluation of the performance of systems are performed, and in the Act phase, remedial actions are taken for the deficiencies or gaps identified in the Check phase [21].

In the Plan phase, security activities such as risk profiling, architectural modeling, and security and privacy requirements occur. The risk profiling activity consists of the following actions: (1) selection of the security dimensions (properties) that are relevant for each cloud service (e.g., confidentiality, integrity, and availability); (2) evaluation of the potential impact on the cloud service (*i.e.*, low, medium, or high) when a threat exploits a vulnerability and its likelihood to happen; (3) determination of the risk level of the service; and (4) determination of the overall risk profile. Based on the overall risk profile, the list of security requirements is formulated. The methodology of the security framework by ENISA is similar to that of FeDRAMP in that ENISA's methodology determines the security impact level of each service qualitatively.

In the Do phase, specific security controls or security measures are implemented to fulfill the security requirements drawn during the Plan stage. Deployment and accreditation form phases 3 and 4, and imply the actual formalization and implementation of the selected security controls, as well as the start of the operation of the government cloud service.

3.3. Methodology for Security Management for Cloud Systems in Public Organizations

This study suggests a methodology for information security management for cloud computing in public organizations. The methodology classifies the importance of information security in cloud systems used in public organizations in terms of security. The importance of information is classified on the basis of the potential impacts of the information on a public organization. The classification of information importance in cloud systems enables an organization in the public sector to effectively manage the security of its cloud systems and efficiently select the appropriate security controls, reflecting the characteristics of the public organization.

Information is processed, stored, sent, and deleted in the form of data, and represents the status of tasks in the organization. The processes for classifying the importance of information involve four steps, namely the

identification of information in cloud systems, the classification of information importance, the adjustment of information importance, and the specification of information resources in a sequence.

In the first step, the information in the cloud systems of a public organization is identified. This step recognizes the information related to the considered tasks, the management, the software and hardware, and the staff of the public organization. Thereafter, the relationships among these types of information are clearly defined.

In the second step, the importance of information is classified as low, medium, or high. The importance of information represents the potential impact of the information on the organization when an event occurs [20]. The importance of information is measured through the quantification of the criteria for confidentiality, integrity, and availability of cloud systems. Confidentiality preserves authorized rights to information access and disclosure, including protection of personal privacy and proprietary information [22]. Further, without permission to disclose certain information, an enterprise may incur some damages. Integrity represents the unauthorized modification or destruction of information adversely affecting the organization [20]. Availability assures timely and reliable usage of information [22]. Disruption of availability prevents users from accessing information and information systems. The approach of quantitative measurement prohibits an evaluator from subjectively judging and overestimating the importance of information in cloud systems.

To establish the criteria measuring the importance of information, in this study, we utilized a simplified Delphi approach, which is a useful method for drawing expert opinions without any interference [23]. We conducted two rounds of the Delphi. In the first round, we asked 10 security experts to write down the criteria quantifying the three security objectives for cloud systems in public organizations. Two professors, four practitioners, and four researchers participated in this round of the Delphi. The experts returned eight criteria for the nature of information, seven criteria for the mission of public-sector organizations, four criteria for the corruption of information resources, two criteria for privacy, and eight criteria for the characteristics of the sector. In the second round, we informed the experts of the results from the first round and asked them to select the criteria for the quantitative assessment from these results. On the basis of the results of the second round, we selected the most commonly appearing criteria and determined the final set of 24 criteria for quantifying the security objectives of cloud systems. Table 1 lists the criteria obtained from two rounds of the Delphi approach. These criteria are measured on a five-point scale.

Table 1. Criteria for quantification of information importance.

Quantification Criteria	Score				
Criteria for confidentiality	1	2	3	4	5
Relevance to sensitive information such as unrevealed policies, sensitive issues of management, and privacy					
Necessity of protecting the information					
Possibility of arguments caused by unauthorized disclosure of the information					
Necessity of restrictions to access the information					
Degree of damage caused by a misuse of the information					
Possibility of damage caused by a disclosure of the information					
Necessity of audit in the case of information retrieval					
Necessity of certificates or biometric certification to access the information					

Table 1. *Cont.*

Quantification Criteria	Score				
Criteria for integrity	1	2	3	4	5
Necessity of restrictions on modification or deletion of the information					
Necessity of audit logging a modification of the information					
Possibility of arguments caused by unauthorized modifications or deletions of the information					
Degree of misuse caused by modification or deletion of the information					
Trust level among citizens in publishing the information officially					
Necessity of backing up the information					
Necessity of certificates or other certification tools for processing the information					
Necessity of validating information integrity					
Criteria for availability	1	2	3	4	5
Necessity of having continuous access to the information					
Necessity of the information's continuously supporting the tasks of an organization					
Number of users of the cloud systems					
Degree of disorder caused by restrictions to the use or access of the information					
Necessity of dual infrastructures to access the information					
High recovery priority after disasters					
Possibility of arguments caused by restrictions to the access or use of the information					
Necessity of backing up the information					

The importance of the information is decided by the scores obtained on the abovementioned five-point scale and is classified as high, medium, or low depending on this score. The importance of information is categorized as follows:

$$\begin{gathered} \text{High: } 31 \leq \text{informtion importance score} \leq 42 \\ \text{Medium}: 23 \leq \text{informtion importance score} \leq 31 \\ \text{Low}: 8 \leq \text{informtion importance score} \leq 23 \end{gathered} \quad (1)$$

The information importance score is calculated as follows:

$$\text{Information importance score} = (\Sigma \text{ score of the confidentiality} + \Sigma \text{ score of the integrity criteria} + \Sigma \text{ score of the availability}) \quad (2)$$

In the third step, the importance of the information is adjusted qualitatively taking into account the following factors: The environment surrounding the organization, the number of users of cloud systems, the distinct characteristics of the organization, and the legislation and regulations related to cloud computing.

In the fourth step, information resources such as specific hardware, specific software, and the corresponding organization staff are specified according to the importance of the information in the cloud systems. The above classification enables an organization to securely manage its information resources and appropriately establish security controls for its cloud systems [24].

3.4. Security Controls for Cloud Systems in Public Organizations

In this paper, we propose the use of a set of security controls for cloud systems in the public sector matching the methodology discussed above. In this study, we compared various security controls such as CSA-CCM, FedRAMP, and ISO27000 and conducted a comparison of the security controls of ENISA, Gartner, BSI, and FISMA. On the basis of this comparison, we selected a set of common security controls for the cloud systems. Table 2 lists the set of security controls; there are 12 domains and 30 security controls listed. The security controls can be divided into detailed components and differently applied according to the different levels of importance of the information in the cloud systems used in the public sector.

The evaluation programs of CSA STAR, ENISA, ISO/IEC 27001, and BSI do not concentrate on the classification of information and the establishment of different security controls for the different levels of information importance in cloud systems.

Table 2. A set of security controls for cloud security in the public sector.

Domain	Security Control	Description
Access control	Access enforcement	Assignment of privilege-based and role-based access control
	Wireless access restrictions	Monitoring and controlling wireless access to cloud system
	Session lock	Preventing further access to the system after a session lock
	Access restrictions for change	Restricting developer access to H/W, S/W, and F/W directly through automatic mechanism
	Automatic detection mechanism for non-authorized device	Detecting automatically non-authorized components or systems attaching to or accessing cloud systems
Audit and backup	Audit, analysis, backup	Analyzing correlations of log-in supporting suspicious actions and backup log to other storage
	Storage of backup	Storing backup of operation systems and other software
Cryptographic controls	Encryption of storage	Encrypting information in storage
	Usage and management of verified cryptography	Protecting information in storage through verified cryptography
Vulnerability scanning	Vulnerability evaluation	Planning analysis and evaluation of vulnerability, penetration test
	Vulnerability management	Identifying and managing new vulnerabilities through automatic tools
	Developer security testing	Requiring developers to conduct security test and evaluation plan, implement the plan, and document the results
Program management	List of programs	Listing approved programs
	Management program	Developing, documenting, certifying, and implementing information security management program
Data management	Media categorization	Classifying media containing sensitive information
	Resource priority	Preventing any higher-priority process from delay or interference of a lower-priority access
Operation management	Boundary protection	Certifying communications at the external boundary and at key internal boundaries within cloud systems
	Trusted path	Establishing trusted path between user and security function
	Acquisition	Acquiring certified security systems
	External information system service	Analyzing risk before external outsourcing service and information systems

Table 2. *Cont.*

Domain	Security Control	Description
Virtual security	Virtual technology	Using virtual technology to different components
	Automatic configuration	Managing, applying, and validating configuration through automatic mechanism
Emergency	Contingency planning	Conducting capacity planning for information processing, telecommunications, and environmental support in crisis
	Contingency policy	Building emergency organization, systems, and an emergency network
Legislation	Location of data	Clarifying the location of data
	Support of survey	Supporting forensics and e-discovery for customers
Availability	Long-term viability	Ensuring availability of customer data in closure, acquisition, and merger
	Data and service portability	Standardizing, documenting, and testing APIs and processes for data and service portability
Identification and authentication	Non-repudiation	Providing non-repudiation tools protecting later false claims
	Identifier management	Identifying unique users

4. Validation for Methodology in a Public Corporation

4.1. Applying the Methodology to the Case of Korea Expressway Corporation

In this study, we try to validate the proposed methodology for information security management through cloud systems in Korea Expressway Corporation (KEC). KEC is one of the largest public companies owned and regulated by the Korean government. In particular, KEC is obliged to follow official security guidelines and ensure the security of its many information systems. KEC depends heavily on its information systems, and through these systems, it manages expressways, road charges, emergency, convenience facilities, and traffic information for users. KEC is now using cloud systems for the management of these systems. To validate the methodology for information security management for cloud systems, we interviewed the security managers and the managers of the cloud systems at KEC six times between October and November 2012. Three researchers, three security managers, and six managers of the KEC cloud systems participated in this validation.

[Step 1] Identification of cloud systems

We identified many information systems and selected four cloud systems for validating the proposed methodology. These cloud systems had different characteristics in terms of data, users, and sensitivity. The four selected cloud systems were electronic service area management systems, electronic procurement management systems, electronic documents management systems, and electronic toll management systems. Table 3 presents a summary of these systems.

[Step 2] Classification of the importance of information in the cloud systems

To classify the importance of information in the cloud systems, we simultaneously measured the importance of information in a cloud system qualitatively and quantitatively. First, we asked the security managers and the manager of each cloud system to qualitatively assign the importance of the information in the cloud systems, a grade of high, medium, or low. Second, we explained the criteria for the importance of the information in the cloud systems to them and asked them to assign a score to the abovementioned criteria through interviews. The interviews were conducted twice. Table 4 shows the

results of the importance of information in the cloud systems. A comparison of the results of the information importance between the qualitative measurement and the quantitative measurement revealed that the results did not differ for most of the considered cloud systems. Therefore, we concluded that the proposed methodology for information security management for cloud systems is valid.

Table 3. Cloud systems of KEC.

Name	Purposes of the Systems	Functions of the Systems
Electronic service area management systems	- Computation of rent fee in service areas - Report of real-time sales volume in service areas - Management of sales volume - Management of unit price	- Recognizing and collecting sales volume in service areas, - Calculating rent fee of service areas between KEC and leaser
Electronic documents management systems	- Computerization of management information systems - Management of electronic documents - Computation of rent fee in service areas - electronic approval	- Drafting and approving electronic documents - Delivering electronic documents - Storing electronic documents
Electronic procurement management systems	- Ensuring build integrity and transparency of electronic biding - Convenience of bid and contract - Issues of actual proof	- Giving public notice of a bid - Managing the process of a successful bid - Managing an interim payment of construction - Issuing actual proof
Electronic toll management systems	- Collection of toll - Collection of traffic information - Provision of credit information to credit companies	- Collecting toll - Informing toll to the holders of prepaid cards and credit cards - Collecting traffic information and displaying it to drivers - Analyzing traffic information and statistics

Figure 1 shows the software used for classifying the importance of information in the cloud systems of KEC.

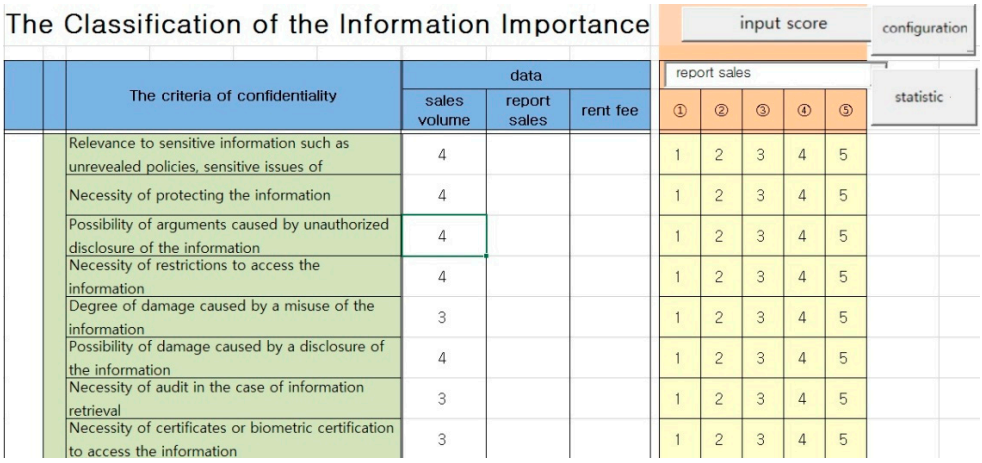

Figure 1. The software used for classifying the information importance in the cloud systems of KEC.

Table 4. The importance of information in the cloud systems of KE.

Quantification criteria	Name of cloud systems			
Criteria for confidentiality	**Service area management systems**	**Electronic documents management systems**	**Electronic procurement management systems**	**Electronic toll management systems**
Relevance to sensitive information such as unrevealed policies, sensitive issues of management, and privacy	3	3	4	4
Necessity of protecting the information	4	3	5	5
Possibility of arguments caused by unauthorized disclosure of the information	3	3	5	5
Necessity of restrictions to access the information	4	3	5	5
Degree of damage caused by a misuse of the information	4	4	4	4
Possibility of damage caused by a disclosure of the information	4	3	5	5
Necessity of audit in the case of information retrieval	4	3	4	5
Necessity of certificates or biometric certification to access the information	3	3	5	4
Criteria for integrity				
Necessity of restrictions on modification or deletion of the information	4	4	5	5
Necessity of audit logging a modification of the information	5	3	5	5
Possibility of arguments caused by unauthorized modifications or deletions of the information	5	3	5	5
Degree of misuse caused by modification or deletion of the information	4	3	5	5
Trust level among citizens in publishing the information officially	5	4	5	5
Necessity of backing up the information	4	5	5	5
Necessity of certificates or other certification tools for processing the information	3	4	4	4
Necessity of validating information integrity	5	4	5	5
Criteria for availability				
Necessity of having continuous access to the information	3	3	5	5
Necessity of the information's continuously supporting the tasks of an organization	3	4	4	5
Number of users of the cloud systems	5	4	4	5
Degree of disorder caused by restrictions to the use or access of the information	4	5	4	5

Table 4. *Cont.*

Quantification criteria	Name of cloud systems			
Criteria for confidentiality	**Service area management systems**	**Electronic documents management systems**	**Electronic procurement management systems**	**Electronic toll management systems**
Necessity of dual infrastructures to access the information	5	3	5	5
High recovery priority after disasters	3	3	5	5
Possibility of arguments caused by restrictions to the access or use of the information	2	4	5	5
Necessity of backing up the information	4	5	5	4
The score of the information importance	31	28.6	37.6	38.3
The importance of information	High	Medium	High	High

[Step 3] Adjustment of the importance of information in the cloud systems

We did not need to adjust the importance of information in the considered cloud systems, classified in the second step, according to the environments, the number of users, and the relevant legislation and regulations.

[Step 4] Specification and classification of the information resources by information importance

The information resources in the cloud systems are specified to users, database, operating systems, local area network, applications and wide area network. The importance of an information resource belonging to a specific cloud system is classified according to that of the system. Table 5 shows the specifications and the importance of the information resources.

Table 5. Specifications and importance of resources of the cloud systems of KEC.

Cloud system	**Service area management systems**			
System resources	Hardware	Solaris, ver.9.9.x.x	Importance	High
	Software-1	Apache, Tomcat, ver.x.x.x		High
	Software-2	PHP		High
	Software-3	Oracle		High
	Communication	LAN		High
Information owners	Director of the service area division		Locations	Offices of the service area division
Information managers	Employees of the service area division			Offices of the service area division Data room
Information users	Employees of the service area division Employees of the customer division			Offices of the service area division Offices of the customer division
Data entry personnel	Employees of a service facility			Service area on an expressway

Previously, KEC had tried to classify the importance of information in its cloud systems and planned to classify the security controls in the near future. We did not have any opportunity to validate the appropriateness of the suggested set of security controls. The classification of information importance in cloud systems is expected to help KEC to easily adopt a categorization of security controls in accordance with the proposed methodology.

4.2. Applying FedRAMP to the Case of Korea South-East Power Corporation

In this study, we apply FedRAMP to the case of Korea South-East Power Cooperation (KOSEP) in order to compare FedRAMP with the proposed methodology for security in cloud systems. KOSEP is one of the largest public companies that own and operate power stations. In particular, KOSEP is sensitive to information security and plans to transform its information systems into cloud systems. In this study, we apply FedRAMP processes to the cloud systems of KOSEP. This experiment is based on interviews and documents produced during the process of security consulting. Table 6 shows the application of FedRAMP to Management Information Systems (MIS) in KOSEP. The procedures applied are as follows:

[Step 1] Identify the type of cloud system.

KOSEP has different types of information systems from MIS systems to Supervisory Control and Data Acquisition Systems (SCADA). Among information systems, MIS systems could be the first target for the transformation into cloud systems. KOSEP implements MIS systems in Enterprise Resource Planning (ERP). The ERP systems process information related to finance, budget, accounting, fuel, and material. Further, they process various types of information, such as business information, mission information, and data. Personnel information systems and accounting systems are selected for the categorization of the impact level.

[Step 2] Select provisional impact level.

This study selects personnel information systems among MIS systems. The provisional impact level of personnel information systems could be assessed as follows: {Confidentiality, moderate; integrity, moderate; availability, low}. The provisional impact level of accounting systems could be assessed as follows: {Confidentiality, moderate; integrity, moderate; availability, high}.

[Step 3] Review provisional impact level and adjust impact level.

Security managers are asked to review the provisional impact level and adjust the impact level. They review the provisional impact level of the personnel information systems and adjust it as follows: {Confidentiality, high; integrity, high; availability, moderate}. The adjusted impact levels of the accounting information systems are as follows: {Confidentiality, moderate; integrity, moderate; availability, moderate}.

[Step 4] Assign the importance of cloud systems to the security category.

The categorization of MIS systems is decided to be high.

Table 6. Application of FedRAMP to MIS.

[Step 1] Identify information type	**[Step 2] Select provisional impact level**		
Personnel information	Confidentiality Moderate	Integrity Moderate	Availability Moderate
Accounting information	Confidentiality Moderate	Integrity Moderate	Availability High
Categorization		High	
	[Step 3] Adjustment of provisional impact level		
Personnel information	Confidentiality High	Integrity High	Availability Moderate
Accounting information	Confidentiality Moderate	Integrity Moderate	Availability Moderate
[Step 4] Categorization		High	

4.3. Application of Security Framework to the Case of Korea South-East Power Corporation

To compare the effectiveness among security methodologies, we applied the security framework of ENISA to the case of KOSEP. To apply the security framework of ENISA, we also interviewed the security managers and referred to documents from KOSEP. In this study, we confined the application of the security framework to the risk profiling process of the Plan phase. Table 7 shows the application of the security framework to MIS systems. The application procedure is as follows:

[Step 1] Identify a cloud service.

MIS systems, such as personnel information systems and accounting information systems, are transformed into cloud systems by the security managers.

[Step 2] Select the relevant security dimensions.

Confidentiality, integrity, and availability are identified as the security dimensions of personnel information systems. The security dimensions of accounting information systems are identified as confidentiality, integrity, and availability.

[Step 3] Evaluate the individual impact on the MIS.

The security dimensions of personnel information systems are evaluated as follows: {Confidentiality, moderate; integrity, moderate; availability, moderate}. Accounting information systems are also evaluated as follows: {Confidentiality, moderate; integrity, moderate; availability, moderate}.

[Step 4] Determine the risk profile of MIS.

The security level of personnel information systems is decided to be moderate and that of accounting information systems is determined to be moderate.

Table 7. Application of risk profiling of the security framework to MIS.

[Step 1] Identify a cloud service
MIS systems such as personnel information systems and accounting information systems
[Step 2] Select the relevant security dimension of the systems
Security dimension of personnel information systems: Confidentiality, integrity, and availability
Security dimension of accounting information systems: Confidentiality, integrity, and availability
[Step 3] Evaluate the individual impact on the MIS
Personnel information systems: {Confidentiality: Moderate, integrity: Moderate, availability: Moderate}
Accounting information systems: {Confidentiality: Moderate, integrity: Moderate, availability: Moderate}
[Step 4] Determine the risk profile of MIS
Overall risk level of personnel information systems: Moderate
Overall risk level of accounting information systems: Moderate

4.4. Comparison of FedRAMP, Security Framework, and the Proposed Methodology

This study compares FedRAMP, the abovementioned security framework, and the proposed methodology in terms of the approach to the evaluation of the impact level, the priority among cloud systems, and the business effects on the categorization of cloud systems. FedRAMP and the security framework adopt a qualitative approach and have advantages in terms of cost savings of the evaluation and simplicity over the proposed methodology. However, the proposed methodology has other benefits over the existing approaches such as the following:

First, FedRAMP and the security framework qualitatively evaluate the impact level on the organization when certain events occur, whereas the proposed method quantitatively evaluates the impact level. As the experiment of FedRAMP shows, even a fine adjustment in the impact level leads to significant changes in the overall categorization of cloud systems. In the proposed methodology, a fine adjustment of the impact level confines the security dimension within the security objectives. A qualitative approach can tolerate the differences in the impact level depending on the evaluators, whereas a quantitative approach can minimize the differences in the impact level by evaluators.

Second, priority among cloud systems can clearly be established in the aggregation of cloud systems by the impact level. FedRAMP and the abovementioned security framework aggregate the results of the impact level evaluation of cloud systems. The results of the impact level of cloud systems are one of the following: Low, moderate, or high. To establish the priority impact level of cloud systems, the evaluator qualitatively adjusts the results of the impact level among cloud systems. The proposed methodology has readiness in establishing priority among cloud systems.

Third, factors influencing the impact level of the cloud systems in FedRAMP and the abovementioned security framework are subjectively identified by the evaluators. In selecting the impact level of cloud systems, each evaluator could adopt his/her criteria. In the proposed methodology, the evaluator just selects the impact level according to the established criteria. The proposed methodology increases the objectivity of the impact level of the cloud systems.

4.5. Validating the Effectiveness of the Proposed Security Controls

To validate the effectiveness of the proposed security controls, we compared the security controls with the representative security controls such as FedRAMP and ENISA [25] in this study. As shown in Figure 2, the proposed security controls match the security measures of ENSIA. The proposed security control emphasizes the importance of cryptography and legislation. Public institutions have to protect public information from external threats and internal threats. To protect secure data, a cryptography technology and the usage and management of verified cryptography are essentially required. The operation of cloud systems in public domains has to satisfy legal requirements. The proposed security controls satisfy official requirements, such as the usage of verified cryptography and legal requirements and simultaneously provides the security functions of ENISA.

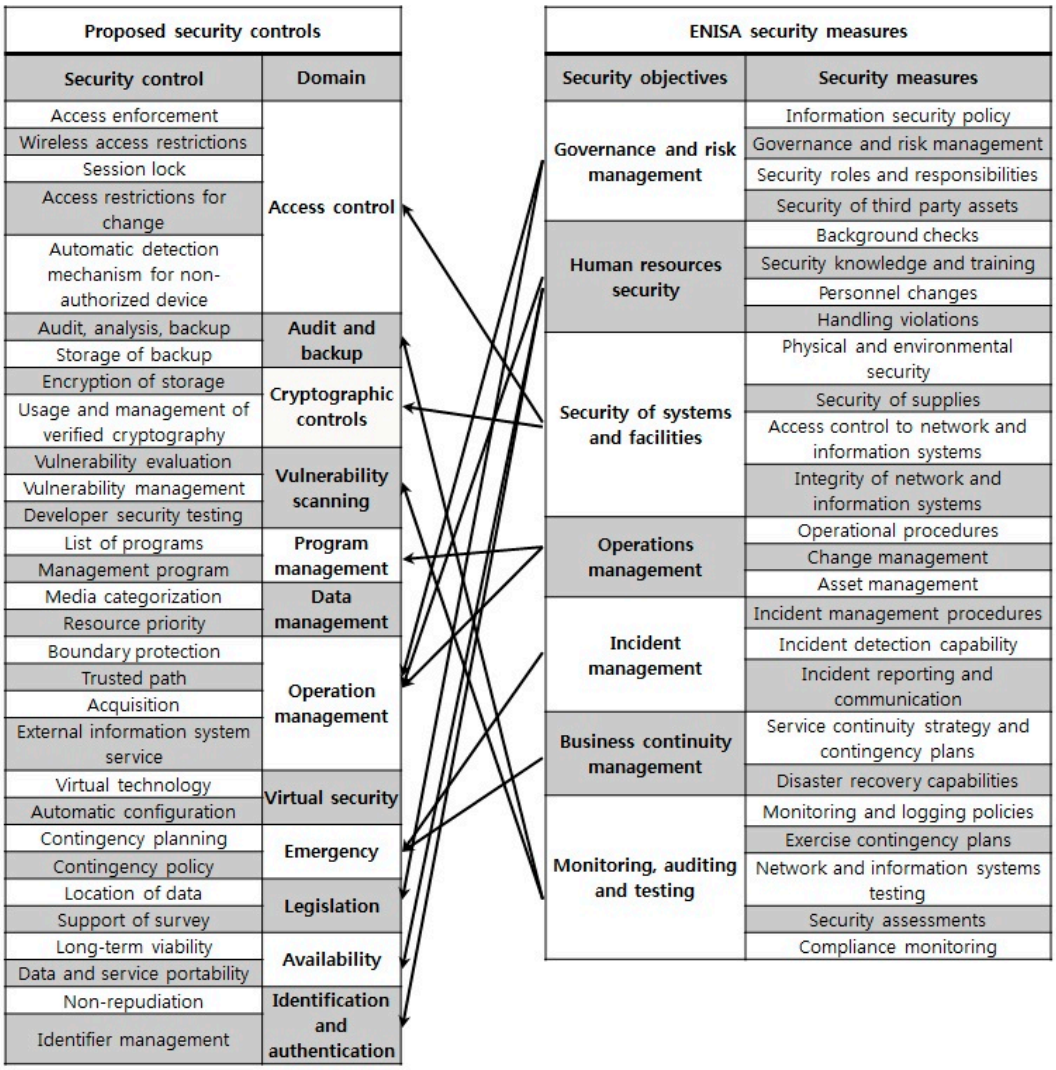

Figure 2. Comparison between the proposed security controls and the security controls of ENISA.

Figure 3 compares the security controls between the proposed method and FedRAMP. The proposed security controls map the security controls in FedRAMP. As shown in Figure 2, FedRAMP and the proposed security controls simultaneously satisfy the requirements of cryptography functions and legislation. The

structure of the proposed security controls is relatively simple and easy as compared to FedRAMP. Accordingly, the proposed security control reflects its specific requirements and simple structure and can be easily applied to the cloud systems of public organizations.

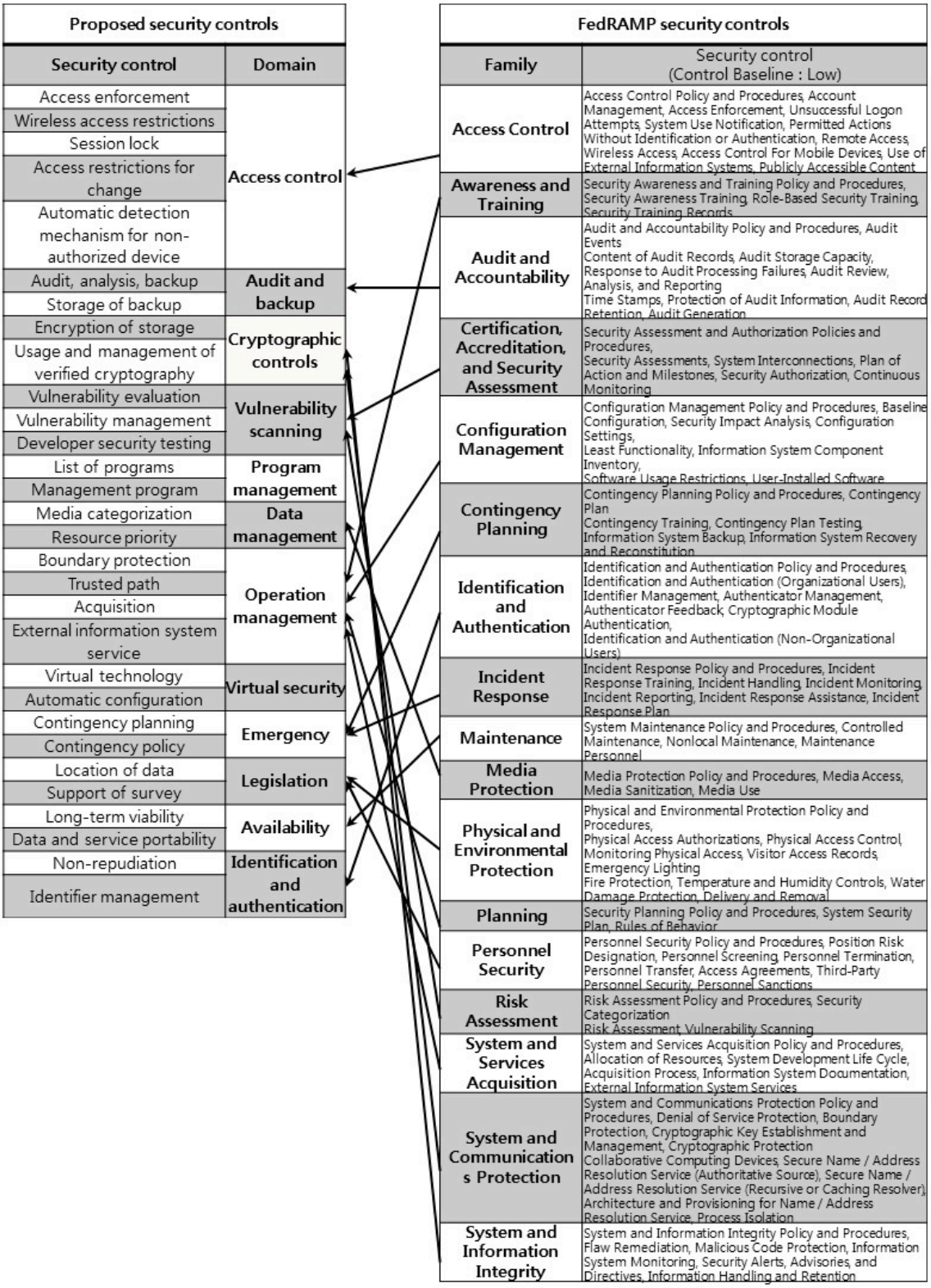

Figure 3. Comparison between the proposed security controls and the security controls of FedRAMP.

The simple structure and specific requirements of the proposed security controls, reflecting the characteristics of public organizations, allow users to flexibly select security controls in accordance with the importance of information in their cloud systems. Thus, the proposed methodology is expected to be useful for saving costs and effort.

The emphasis on cryptography and legislation in the proposed security controls assures the security of cloud systems of public organizations, resulting in actively introducing cloud systems to public organizations and resolving the legal hindrances in establishing cloud systems in public organizations.

The proposed security controls can be an example that can be applied to public organizations. The security environment of each public organization may differ. An approach using the derived security controls of the proposed methodology reveals the minimum security requirements of public organizations.

5. Conclusions

To vitalize cloud systems in the public sector, the related security issues need to be resolved as the public sector considers more sensitive security issues than the private sector. To ensure the security of cloud computing in the public sector, security management has to reflect the characteristics of public institutions. For a consolidation of security, in this paper, we proposed a methodology for the information security management of cloud systems in the public sector and validated its usefulness through a case study. The proposed methodology has the following advantages: First, it makes it possible to establish the appropriate security level of the security controls in the public sector. However, to determine the appropriate security level of the security controls and security activities, a risk analysis and other technical consulting have to be considered [26]. Such a risk analysis requires complex processes, and the practitioners tend to find it difficult to conduct [27]. The abovementioned classification is less difficult than a risk analysis and produces a clear direction for the security activities and the security controls of the public sector. The above classification could efficiently invest the resources of an organization in security. Second, in the process of the classification of information importance in the cloud systems, the managers and the users surrounding the cloud systems come to identify their security responsibility. This ensures their active involvement in the security of cloud systems. Third, the completion of the classification enables an organization to recover its information resources quickly. Further, the classification, requiring detailed information about the information resources of the organization, enables a systematic recovery from a disaster.

Author Contributions

Myeonggil Choi generated idea and conducted the experiments and Changhan Lee reviewed related works.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Plummer, D.C.; Bittman, T.J.; Austin, T.; Cearley, D.W.; Smith, D.M. Cloud Computing: Defining and Describing an Emerging Phenomenon, Gartner. Available online: https://www.gartner.com/doc/697413/cloud-computing-defining-describing-emerging (accessed on 10 February 2015).
2. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; *et al.* A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58.
3. Rainey, H.G. *Understanding and Managing Public Organizations*, 3rd ed.; Jossey-Bas: San Francisco, CA, USA, 2003; pp. 55–79.
4. Zissis, D.; Lekkas, D. Addressing cloud computing security issues. *Future Gener. Comput. Syst.* **2012**, *28*, 583–592.
5. Feng, D.G.; Zhang, M.; Zhang, Y.; Xu, Z. Study on cloud computing security. *J. Softw.* **2011**, *22*, 71–83.
6. Jamil, D.; Zaki, H. Cloud computing security. *Int. J. Eng. Sci. Technol.* **2011**, *3*, 3478–3483.
7. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11.
8. Heiser, J.; Nicolett, M. Assessing the Security Risks of Cloud Computing, Gartner Report. 2008. Available online: https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing (accessed on 25 February 2015).
9. Cloud Security Alliance (CSA). The Security, Trust & Assurance Registry (STAR). 2011. Available online: https://cloudsecurityalliance.org/star/ (accessed on 25 February 2015).
10. Dekker, M.; Karsberg, C. Technical Guideline in Security Measures Version 2.0, European Union Agency for Network and Information Security. 2014. Available online: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures (accessed on 20 February 2015).
11. The Federal Risk and Authorization Management Program (FedRAMP) PMO. Guide to Understanding FedRAMP Version 2.0, U.S. General Services Administration (GSA). Available online: https://cio.gov/protect/fedramp/ (accessed on 26 February 2015).
12. International Organization for Standardization (ISO). ISO/IEC 27001: 2013, Information Technology-Security Techniques-Information Security Management Systems Requirements, International Organization for Standardization in Switzerland. Available online: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (accessed on 26 February 2015).
13. Henze, D. IT Baseline Protection Manual, Federal Office for Information Security (BSI). Available online: http://www.iwar.org.uk/comsec/ (accessed on 25 February 2015).
14. Nikolić, B.; Ružić-Dimitrijević, L. Risk assessment of information technology systems. *Issues Inf. Sci. Inf. Technol.* **2009**, *6*, 595–615.
15. Federal Office for Information Security (BSI), Risk Analysis with the New Threat Catalogue T0 "Elementary Threats". Available online: www.bsi.bund.de/grundschutz (accessed on 25 February 2015).
16. Hange, M. IT—Grundschutz Catalogues Version 13, Federal Office for Information Security (BSI). 2013. Available online: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html (accessed on 25 February 2015).

17. Federal Office for Information Security (BSI), BSI-Standard 100-1: Information Security Management Systems (ISMS) Version 1.5. Available online: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html (accessed on 28 February 2015).
18. Federal Office for Information Security (BSI), BSI-Standard 100-2: IT-Grundschutz Methodology Version 2.0. Available online: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html (accessed on 24 February 2015).
19. Federal Office for Information Security (BSI), BSI-Standard 100-3: Risk Analysis Based on IT-Grundschutz Version 2.5. Available online: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html (accessed on 25 February 2015).
20. Stine, K.; Kissel, R.; Barker, W.C.; Fahlsing, J.; Gulick, J. NIST SP 800-60 Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories. Available online: http://csrc.nist.gov/publications/PubsSPs.html (accessed on 10 February 2015).
21. Dimitra L.; Dekker, M. Security Framework for Governmental Clouds, European Union Agency for Network and Information Security. 2015. Available online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds (accessed on 20 February 2015).
22. Joint Task Force Transformation Initiative; NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments. Available online: http://csrc.nist.gov/publications/PubsSPs.html (accessed on 10 February 2015).
23. Rowe, G.; Wright, G. The Delphi technique as a forecasting tool: Issues and analysis. *Int. J. Forecast*. **1999**, *15*, 353–375.
24. Mather, T.; Kumaraswamy, S.; Latif, S. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*; O'Reilly Media: Sebastopol, CA, USA, 2009; pp. 109–141.
25. Dekker, M. Technical Guideline on Security Measures, European Union Agency for Network and Information Security. 2015. Available online: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures (accessed on 24 February 2015).
26. Gerber, M.; von Solms, R. From risk analysis to security requirements. *Comput. Secur*. **2001**, *20*, 577–584.
27. Slovic, P.; Finucane, M.L.; Peters, E.; MacGregor, D.G. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Anal.* **2004**, *24*, 311–322.