Information Security Management in Cloud Computing

MSc Thesis of: *Nikolaos Papatheodoulou*

Supervisor: *Assistant Professor Constantinos Lamprinoudakis*

Table of Contents

Chapter 1

Cloud Computing Overview

Nick Papatheodoulou

Cloud Computing

A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers. [1] Cloud can be divided in four categories; Public, Community, Hybrid and Private.

Public cloud

Public cloud or external cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who bills on a fine-grained utility computing basis.

Community cloud

A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. With the costs spread over fewer

users than a public cloud (but more than a single tenant) this option is more expensive but may offer a higher level of privacy, security and/or policy compliance. Examples of community cloud include Google's "Gov Cloud".

Hybrid cloud

A hybrid cloud environment consisting of multiple internal and/or external providers. By integrating multiple cloud services users may be able to ease the transition to public cloud services while avoiding issues such as PCI compliance[1]. Another perspective on deploying a web application in the cloud is using Hybrid Web Hosting, where the hosting infrastructure is a mix between Cloud Hosting for the web server, and Managed dedicated server for the database server.

A hybrid storage cloud uses a combination of public and private storage clouds. Hybrid storage clouds are often useful for archiving and backup functions, allowing local data to be replicated to a public cloud.

Private cloud

Douglas Parkhill first described the concept of a "Private Computer Utility" in his 1966 book “The Challenge of the Computer Utility”. The idea was based upon direct comparison with other industries (e.g. the

[1] *Payment Card Industry Data Security Standards (PCI DSS) are network security and business practice guidelines adopted by Visa, MasterCard, American Express, Discover Card, and JCB to establish a “minimum security standard” to protect customer’s payment card information. It’s a requirement for all merchants that store, transmit, or process payment card information.*

electricity industry) and the extensive use of hybrid supply models to balance and mitigate risks.

Private cloud and internal cloud have been described as neologisms, however the concepts themselves pre-date the term cloud by 40 years. Even within modern utility industries, hybrid models still exist despite the formation of reasonably well-functioning markets and the ability to combine multiple providers.

Some vendors have used the terms to describe offerings that emulate cloud computing on private networks. These (typically virtualisation automation) products offer the ability to deliver some benefits of cloud computing whilst mitigating some of the pitfalls. These offerings capitalise on data security, corporate governance, and reliability concerns during this time of transition from a product to a functioning service-based industry supported by competitive marketplaces. [3]

Cloud Computing Architecture

The most important goal of cloud computing is that provides a portable, on demand network, using available resources in a virtual domain. Cloud computing is using internet accessible services on demand. The services are being provided only when and if are needed by a user. As a result, this technology is getting closer to the next generation of computing. The provided services are accessible from any place of the world. In such a model, users can access services, based on their requirements, without regard the geographical place of the users, or the place where the data are stored.

A dynamic set of hardware, software and humans, such as Cloud Computing Infrastructure, should have a strong architecture design. In figure 1, the Cloud Computing Architecture is presented in three layers [2].

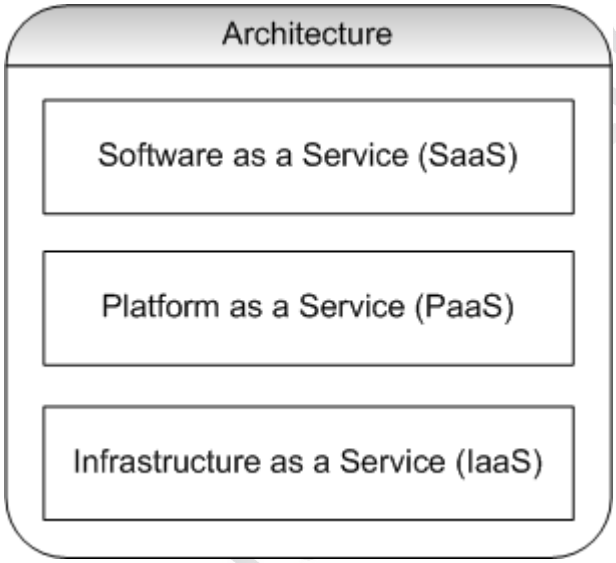

Figure 1 – *Layered Cloud Computing Architecture*

Infrastructure-as-a-Service (also referred in bibliography as Hardware as a Service – HaaS) is the delivery of huge computing resources such as the capacity of processing, storage and network. Taking storage as an example, when a user use the storage service of cloud computing, he just pay the consuming part without buying any disks or even knowing nothing about the location of the data he deals with.

Platform-as-a-Service generally abstracts the infrastructures and supports a set of application program interface to cloud applications. It is the middle bridge between hardware and application. Because of the importance of platform, many big companies want to grasp the chance of

predominating the platform of cloud computing. The well known examples are Google App Engine and Microsoft's Azure Services Platform.

Software-as-a-Service aims at replacing the applications running on PC. There is no need to install and run the special software on your computer if you use the SaaS. Instead of buying the software at a relative higher price, you just follow the pay-per-use pattern which can reduce you total cost. The concept of SaaS is attractive and some software runs well as cloud computing, but the delay of network is fatal to real time or half real time applications such as 3D online game.

Currently, there is no standard definition or specification for Cloud Computing. Cloud Computing involves a set of key technologies to address resource sharing based on business requirements. Accordingly to [4] the following two key enabling technologies could play very important roles in this revolutionary phase:

- Virtualization technology
- Service-Oriented Architecture (SOA).

The virtualization technology handles how images of the operating systems, middleware, and applications are pro-created and allocated to the right physical machines or a slice of a server stack. The images could be moved around and put into production environment on demand. On the other hand, virtualization technology can also help reuse licenses of operating systems, middleware, or software applications, once a subscriber releases his/her service from the Cloud Computing platform.

The SOA is the evolution of a system or software architecture for addressing componentization, reusability extensibility, and flexibility. In order to construct scalable Cloud Computing platforms, we need to leverage SOA to build reusable components, standard-based interfaces, and extensible solution architectures. [4]

The two key entities that take part in the cloud are:

- A *customer* or *potential customer* of a cloud computing service is a user. The user may be an individual, business, government agency, or any other entity.
- The organization that offers the cloud computing service is a *cloud service provider*, or *cloud provider*. A cloud provider may be an individual, a corporation or other business, a non-profit organization, a government agency or any other entity. A cloud service provider is one type of third party that maintains information about, or on behalf of, another entity.[5]

Cloud Characteristics

Cloud computing has five common characteristics, different than the other architectures [10].

On-demand self-service: Without the need of human interactions with cloud providers, a cloud user can have computing capabilities and storage automatically.

Broad Network Access: Cloud services can be accessed through standard mechanisms, from different kinds of client platforms. (e.g. smart phones, computers, netbooks, Personal Digital Assistants)

Resource Pooling: There is not a known, discreet location of data and cloud resources. Cloud services are pooled and can be assigned and reassigned according to the consumer's request.

Rapid Elasticity: Capabilities can be rapidly provisioned in an elastic mode. This fact could mean that, for a consumer's point of view, cloud resources and provided services are unlimited.

Measured Service: Cloud systems can automatically control and optimize resource use. Resource usage can be monitored, controlled and reported providing transparency. Here could be used AAA (Authentication, Authorization, Accounting) techniques, such as Trend Analysis [8].

Security Issues

Within the cloud computing world, the virtual environment let users access computing power that exceeds that contained within their own physical worlds. To enter this virtual environment requires them to transfer data throughout the cloud. Consequently, several data storage concerns can arise. Typically, users will know neither the exact location of their data nor the other sources of the data collectively stored with theirs. To ensure data confidentiality, integrity, and availability (CIA), the storage provider must offer capabilities that, at a minimum, include

- a tested encryption schema to ensure that the shared storage environment safeguards all data;
- stringent access controls to prevent unauthorized access to the data; and
- scheduled data backup and safe storage of the backup media.

Security is implicit within these capabilities, but further fundamental concerns exist that need attention. For example, is security solely the storage provider's responsibility, or is it also incumbent on the entity that leases the storage for its applications and data? Furthermore, legal issues arise, such as e-discovery, regulatory compliance (including privacy), and auditing. The range of these legal concerns reflects the range of interests that are currently using or could use cloud computing. These issues and their yet-to-be-determined answers provide significant insight into how security plays a vital role in cloud computing's continued growth and development.

To overcome these and other concerns, we must develop a security model that promotes CIA. This model could enable each cloud to offer a measure of its to date and projected CIA, but the obvious difficulty is that obtaining security data is difficult, if not impossible. This problem has existed since computing's advent due to financial, business, and national security concerns. It might be exacerbated in cloud computing because the need to provide data confidentiality can also impact incident reporting.

Confidentiality

Confidentiality is one of the most important parts of Security Analysis. In Cloud Computing, multiple confidentiality issues are identified in a strong complexity, for all participants of a cloud. First of all, users store their data on remote servers, which in most cases are in a different location from the user's place of activity. This fact requires a careful research in possible confidentiality threats and security risks. In addition, there are different laws related to confidentiality, from place to place. Thus, something that is legal for a user located in place A, may be not legal for another user in place B, both connected in the same Cloud.

The cloud providers have the right to change or update the terms of use of their services. Another confidentiality issue is that the terms and conditions of service providers may violate the laws under which the user's information was collected. For example two companies may share their commercial information in the same cloud, on which only the policies of its service provider could limit the use of this information by other users in the cloud.

Information stored in a specific cloud is protected by the laws of the geographical domain, in which the data center is located. In most cases, the information is stored in a different place than the owner's. For example a user located in Greece could store data in a cloud, whose data store center is located in United States. Then the Greek user's information will be under the legal authority of United States, where is the physical place of server. Also, Cloud providers, could change the place where the data are stored, from an administration domain to another, without notice

the owner. As a result, after this transfer, data will be under an alternative legal framework. This fact focuses a plenty of confidentiality issues, which differ from place to place, accordingly with its laws related to Confidentiality.

In many times, some companies cooperate with other organizations in order to store their data in a specific Cloud. Those organizations act as a third party. Thus, the information has a weaker confidentiality, than without the third party cooperation.

It is now clear that Confidentiality has a strong relation with laws and legal issues around the administration domains, located in different geographical places around the world.

Data Integrity

One of the most critical components to focus in Cloud Computing is data, as it is a key actor in each Cloud. The users pass their data to be stored under different circumstances from Cloud to Cloud. Also they are sending their data using multiple web platforms and web applications. As a result, the Cloud providers should adopt the most efficient way to collect and store data in order to ensure the integrity.

The traditional RAID (Redundant Arrays of Independent Disks) techniques are not appropriate to solve this problem. In addition, many users have reported loss or corruption of their data. The Data Integrity Field standard (DIF) provides storage-centric data integrity as well as end-to-end data integrity. Cloud service providers should adopt DIF

standard, as it is a best practice to store the data on disks that perform the DIF function.

Storage Networks Industry Association (SNIA) introduces the term Data Storage as a Service (DaaS) [6]. In summary DaaS means the delivery of virtual stored and related data, over a network after a request.

Availability

Basic information Security consists on three on three components which have to be ensured; Confidentiality, Integrity and Availability (CIA). Last but not least, Availability, in such a dynamic infrastructure as Cloud Computing, should be ensured in a great manner.

Some Cloud Computing platforms faces a lot of availability isues in the past. In a specific month of 2008, those platforms were unavailable for a time period from two to eight hours [7]. Nevertheless, cloud Computing is in most cases reliable and provides a high level availability.

In order to succeed a hundred per cent availability in cloud computing environments, there should be a strong availability architecture, where the testing of necessary web platforms is a prerequisite. Moreover, the data and the server side applications should be stored on a backup server, or a backup Cloud. Finally, an applicable Disaster Recovery Plan (DRP) should be adopted from providers, after an accurate risk analysis [9].

Chapter References

[1] Rajkumar Buyyaa, Chee Shin Yeoa, Srikumar Venugopala, James Broberg, Ivona Brandic, *"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility"*, Future Generation Computer Systems, Elsevier, 2009

[2] Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, *"A Taxonomy and Survey of Cloud Computing Systems"*, 5th International Joint Conference on INC, IMS and IDC, 2009

[3] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong, *"The Characteristics of Cloud Computing"*, in Proceedings of IEEE 39th International Conference on Parallel Processing Workshops, 2010

[4] Liang-Jie Zhang and Qun Zhou, *"CCOA: Cloud Computing Open Architecture*", in Proceedings of 2009 IEEE International Conference on Web Services, 2009

[5] Robert Gellman, *"Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing"*, World Privacy Forum, 2009

[6] SNIA, *"Cloud Data Management Interface*", Storage Networking Industry Association, Technical Position, 2010

[7] Won Kim, *"Cloud Compting: Today and Tomorrow"*, Journal of Object Technology, Zurich 2009

[8] Nick Papatheodoulou, Nicolas Sklavos, *"Architrecture and System Design of Authentication, Authorization and Accounting Services"*, in Proceedings of 2009 IEEE International Conference EUROCON'09, 2009

[9] Mladen A. Vouk, *"Cloud Computing – Issues, Research and Implementations"*, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[10] Peter Mell, Timothy Grance, NIST, "The NIST Definition of Cloud Computing (Draft)"

Chapter 2

Information Security Management

Nick Papatheodoulou

Information Security Management

Security Management is a broad field of management related to asset management, physical security and human resource safety functions. It entails the identification of an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.

Information Security Management is the set of functions that protects telecommunications, networks and systems from unauthorized access by persons, acts, or influences and that includes many subfunctions, such as:

- creating, deleting, and controlling security services and mechanisms
- distributing security-relevant information
- reporting security-relevant events
- controlling the distribution of cryptographic keying material
- authorizing access, rights, and privileges.

Management tools such as information classification, risk assessment and risk analysis are used to identify threats, classify assets and to rate system vulnerabilities so that effective control can be implemented.

Information Security Management System Requirements

The information security management (ISM) process describes the structured fitting of security in the management organization. One of the best approaches for ISM is the ISO 27001 standard. This standard covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 propose the processes that ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. [11]

The primary goal of information security is to guarantee safety of information. When protecting information it is the value of the information that has to be protected. These values are stipulated by the confidentiality, integrity and availability (CIA). Inferred aspects are privacy, anonymity and verifiability.

The goal of the Security Management is split up in two parts [11,2]:

1. The realization of the security requirements defined in the service level agreement (SLA) and other external requirements which are

specified in underpinning contracts, legislation and possible internal or external imposed policies.

2. The realization of a basic level of security. This is necessary to guarantee the continuity of the management organization. This is also necessary in order to reach a simplified service-level management for the information security, as it happens to be easier to manage a limited number of SLAs as it is to manage a large number of SLAs.

The input of the security management process is formed by the SLAs with the specified security requirements, legislation documents (if applicable) and other (external) underpinning contracts. These requirements can also act as key performance indicators (KPIs) which can be used for the process management and for the justification of the results of the security management process.

The output gives justification information to the realization of the SLAs and a report with deviations from the requirements. The most obvious relations will be the relations to the service level management process, the incident management process and the Change Management process.

The PDCA Model

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes as it is presented in figure 2.

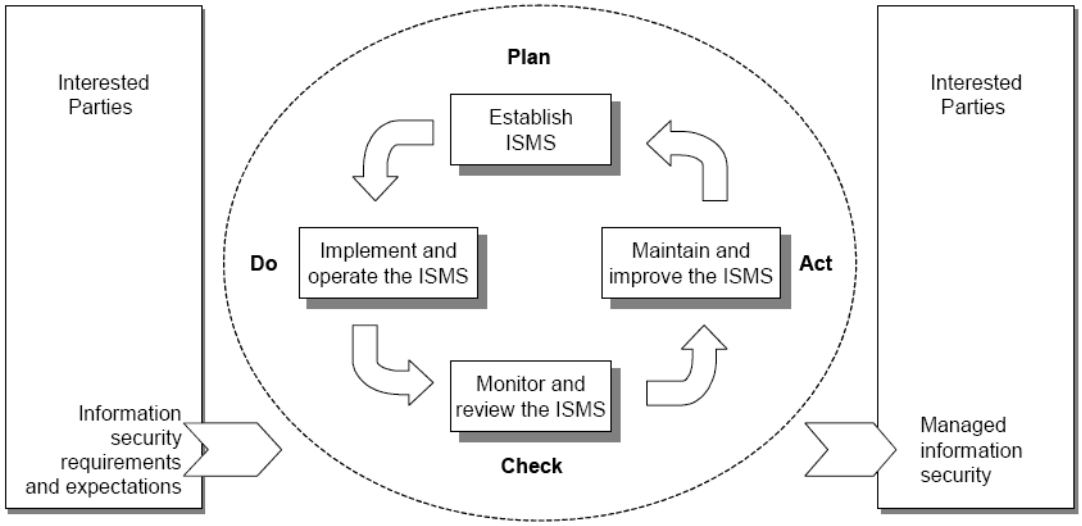

Figure 2 – *The PDCA model*

The Plan phase

Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.

The Do phase

Implement and operate the ISMS policy, controls, processes and procedures.

The Check phase

Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

The Act phase

Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Information Security Management System Design

In designing the ISMS, the following matters should be considered:

- Organizational Security
- ICT Security
- Physical Security
- ISMS specifications

Organizational security

This phase covers the administrative aspects of information security including the responsibility of the organization's operation for risk treatment. This should be formed into the set of activities resulting in the

policies, objectives, processes and procedures to handle and improve information security in relation to the organization's needs and risks.

ICT security

ICT Security covers aspects of information security specifically related to the responsibility of the ICT operations for risk reduction. This is to fulfill the requirements set by the organization and the technical implementation of controls to reduce risks.

Physical security

Physical Security covers aspects of information security specifically related to the responsibility of the handling of the physical environment, such as buildings and their infrastructure for risk reduction. This is to fulfill the requirements set by the organization and the technical implementation of controls to reduce risks.

ISMS specific security

ISMS specific security covers the aspects of the different specific requirements for an ISMS according to ISO/IEC 27001:2005 [11], apart from what is covered in the other three areas. The focus is on certain activities that should be conducted in the implementation to achieve an operational ISMS which are:

- monitoring

- measuring
- internal ISMS auditing
- training and awareness
- incident management
- management review
- ISMS improvement including corrective and preventive actions

The development of the ISMS Project and the design of its related planned implementation of controls should involve and make use of the skills and experience of staff from those parts of the organization that are either within the ISMS scope or have ISMS related management responsibilities. The ISMS specific aspects requires dialogue with management.

To design the selected controls for the risk treatment, it is crucial to design the ICT and physical security environment and the organizational security environment. ICT security deals not only with information systems and networks but also with operational requirements. Physical security deals with all aspects of access control, non-repudiation, physical protection of information assets and what is stored or kept in, as well as being itself a means of protection for security controls itself. [12]

Chapter References

[2] Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, *"A Taxonomy and Survey of Cloud Computing Systems"*, 5th International Joint Conference on INC, IMS and IDC, 2009

[11] ISO/IEC 27001:2005, International Standard

[12] ISO/IEC 27003:2010, International Standard

Chapter 3

Cloud Computing Security Management

Nick Papatheodoulou

Introduction

As we have referred earlier in this work, ISO-27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof [11]. On the other hand when ISO-27001:2005 was designed, the Cloud technology did not have arrived yet.

The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. But how it could be adopted in a Cloud Computing Environment?

Cloud Computing Security Issues

The ISO-27000 faced the security issues by controls that organized as [11,12]:

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems acquisition, development and maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

One of the today's cloud security approaches believes about the cloud computing adoption problem, many of the issues are essentially old problems in a new setting. For example we can move best practices of some traditional security issues to the cloud in different settings. NIST categorize the control of Cloud Security issues in nine areas of focus [13]:

- Governance
- Compliance
- Trust
- Architecture
- Identity and Access Management
- Software Isolation
- Data Protection
- Availability
- Incident Response

Government

Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

Compliance

Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements.

Trust

Incorporate mechanisms into the contract that allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Institute a risk management program that is flexible enough to adapt to the continuously evolving and shifting risk landscape.

Architecture

Understand the underlying technologies the cloud provider uses to provision services, including the implications of the technical controls involved on the security and privacy of the system, with respect to the full lifecycle of the system and for all system components.

Identity and Access Management

Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions. In addition, providers must have a high level of trust in privileged administrators and individuals [14].

Software Isolation

Understand virtualization and other software isolation techniques that the cloud provider employs, and assess the risks involved.

Data Protection

Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned. Moreover, national privacy requirements must be considered, because of the different geographical location of data [14].

Availability

Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed and that all operations can be eventually reinstituted in a timely and organized manner.

Incident Response

Understand and negotiate the contract provisions and procedures for incident response required by the organization.

Chapter References

[11] ISO/IEC 27001:2005, International Standard

[12] ISO/IEC 27003:2010, International Standard

[13] NIST, "Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144

[14] Jay Heiser, Mark Nicolett, *"Assesing the Security Risks of Cloud Computing"*, Gartner Inc, 2008

Chapter 4

International Standards for Information Security Management

Nick Papatheodoulou

Introduction

In our days there are many standards developed in order to support Information Security Management. In these standards there are many issues mentioned, but we focus only those sections that are related, or could be, in Cloud reality. The standards we selected are [11, 12]:

- ISO 27001:2005
- BSI Standars

British Standard ISO 27001:2005

This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline

for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

Addressing security in third party agreements

The proposed control for addressing security in outsourcing is:
Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.
In addition, the following terms should be considered for inclusion in the agreement in order to satisfy the identified security requirements:

a) the information security policy;

b) controls to ensure asset protection, including:

1) procedures to protect organizational assets, including information, software and hardware;

2) any required physical protection controls and mechanisms;

3) controls to ensure protection against malicious software;

4) procedures to determine whether any compromise of the assets, e.g. loss or modification of information, software and hardware, has occurred;

5) controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the agreement;

6) confidentiality, integrity, availability, and any other relevant property of the assets;

7) restrictions on copying and disclosing information, and using confidentiality agreements;

c) user and administrator training in methods, procedures, and security;

d) ensuring user awareness for information security responsibilities and issues;

e) provision for the transfer of personnel, where appropriate;

f) responsibilities regarding hardware and software installation and maintenance;

g) a clear reporting structure and agreed reporting formats;

h) a clear and specified process of change management;

i) access control policy, covering:

1) the different reasons, requirements, and benefits that make the access by the third party necessary;

2) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;

3) an authorization process for user access and privileges;

4) a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use;

5) a statement that all access that is not explicitly authorised is forbidden;

6) a process for revoking access rights or interrupting the connection between systems;

j) arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement;

k) a description of the product or service to be provided, and a description of the information to be made available along with its security classification;

l) the target level of service and unacceptable levels of service;

m) the definition of verifiable performance criteria, their monitoring and reporting;

n) the right to monitor, and revoke, any activity related to the organization's assets;

o) the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;

p) the establishment of an escalation process for problem resolution;

q) service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities;

r) the respective liabilities of the parties to the agreement;

s) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries;

t) intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work;

u) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;

v) conditions for renegotiation/termination of agreements:

1) a contingency plan should be in place in case either party wishes to terminate the relation before the end of the agreements;
2) renegotiation of agreements if the security requirements of the organization change;
3) current documentation of asset lists, licences, agreements or rights relating to them.

Physical security perimeter

In this standard is referred the physical security perimeter control as:
Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

Service delivery

It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the organization should plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and should ensure that security is maintained throughout the transition period.

The organization should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

Monitoring and review of third party services

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

Monitoring and review of third party services should ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly.

Managing changes to third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

Information back-up

Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

Information exchange policies and procedures

Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

On-Line Transactions

Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Publicly available information

The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

User access management

The objective of this standard for the issue of user access management is to ensure authorized user access and to prevent unauthorized access to

information systems. Formal procedures should be in place to control the allocation of access rights to information systems and services.

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

Network access control

Objective: To prevent unauthorized access to networked services. Access to both internal and external networked services should be controlled.

User access to networks and network services should not compromise the security of the networkservices by ensuring:
a) appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks;
b) appropriate authentication mechanisms are applied for users and equipment;
c) control of user access to information services in enforced.

Application and information access control

Objective: To prevent unauthorized access to information held in application systems. Security facilities should be used to restrict access to and within application systems.

Logical access to application software and information should be restricted to authorized users.

Application systems should:
a) control user access to information and application system functions, in accordance with a defined access control policy;
b) provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls;
c) not compromise other systems with which information resources are shared.

Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.
The protection required should be commensurate with the risks these specific ways of working cause.

When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the

teleworking site and ensure that suitable arrangements are in place for this way of working.

Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

Where evidence is required, it should be collected to ensure compliance with legal requirements.

Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization.

Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country.

BSI Standard

Involving personnel in the information security process

Information security concerns all personnel without exception. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Increasing the awareness for information security and providing appropriate training for staff members as well for as all management personnel are therefore fundamental prerequisites for information security. In order to be able to implement security measures as planned, personnel must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves an understanding for the spirit and purpose of security measures. The work atmosphere, common ideals and the commitment of personnel are all factors that decisively influence information security.

If new personnel are taken on or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of their job. If personnel leave the institution or their responsibilities change, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards).

Business continuity, recovery, and restoration

The most important goal of the business continuity response and crisis management is to maintain business continuity. This means the impaired business processes are somehow put back into operation quickly. Business continuity therefore includes specific measures and procedures that allow the operation of the corresponding business processes to be recovered within the recovery time objective specified in advance. Emergency operation can be obtained by running a “normal operation” using fewer resources, running a reduced operation using alternative resources, or by using alternative operational resources.

If a business process is disrupted, then business continuity can be obtained in the best-case scenario by recovering the undamaged resources. If resources were destroyed or are not available any more for some other reason, then they must be recovered. Depending on the type of resource, this means that the resource needs to be replaced, re-installed, and set up again.

For the business continuity response, the current situation is analysed and a decision is made for each process regarding which of the business continuity alternatives is possible, reasonable, and the fastest and best alternative in view of the overall situation.

As soon as all recovery and restoration measures have been executed, a message should be sent to the crisis team, regardless of whether or not the measures were successful. The organisation cannot return to normal operations until every point in the restoration plan has been implemented

successfully. The organisation remains in the emergency operation phase until this point.

Returning to normal operations and post-emergency tasks

If the resources needed for the normal operation of business processes are available again, then emergency operation should be terminated and normal operation resumed. Since there are dependencies between the business processes that need to be taken into account, the return to normal operations should proceed in an orderly manner to avoid discrepancies between or in the business processes. For this reason, the crisis team must specify the order in which each business process is to be returned to normal operation and at which time, and must also co-ordinate their return to normal operation. This prevents problems from arising while returning to normal operation that could lead to another collapse of the business activities.

In general, there will be work backlogs because emergency operation was performed using fewer resources. To check for backlogs and work off the backlog promptly, one person should be named as responsible in the business continuity plan in each organisational unit for creating an overview of the corresponding work backlogs and specifying a plan to work off these backlogs. When creating the plan to work off the backlog, the currently pending work load, the work load during emergency operations, and the legal work restrictions should be taken into account. Strategic specifications on how to handle the additional time and expense required to work off the backlogs (e.g. using overtime, working in shifts, or using additional personnel) should be specified during contingency

planning. These specifications must be agreed to by the personnel representative.

The post-emergency tasks should be supervised by the business continuity co-ordinators of the particular organisational units. It must be specified who will report the status of the post-emergency tasks to whom and at what times.

Analysis of the business continuity response

After completing the business continuity response and de-escalation, the business continuity response should be analysed so that measures for improvement can be taken to counteract any weaknesses discovered. The analysis should be performed by the business continuity officer with the persons responsible from business continuity response, and if necessary in co-operation with the business continuity co-ordinators of the affected areas. Suggestions for improvement are worked out during this analysis.
When responding to an emergency, it may also become apparent that there is a need to improve the organisational structures, the IT, or the business processes. In such cases, the business continuity officer should meet with the people responsible for the particular area and work out suggestions for improvement together. For example, it may make sense to make changes to the fire protection equipment or the information security system.

People must be assigned responsible for the implementation of the suggestions for improvement, and deadlines must be specified for their implementation. The business continuity officer should monitor the

timely implementation of the measures for improvement and report to the organisation's management at prescribed intervals. The plans and procedures used for implementation should be revised and updated by the corresponding organisational units responsible if they are found to be deficient. The functionality and efficiency of the newly implemented measures and procedures should be verified through exercises.

Chapter References

[11] ISO/IEC 27001:2005, International Standard

[12] ISO/IEC 27003:2010, International Standard

Chapter 5

Security Controls in the Cloud

Nick Papatheodoulou

Introduction

A typical cloud is structured as a set of three entities (figure 3);

- *Cloud Provider*
- *Cloud Service Providers*
- *Organizations*

In this chapter, we will assign the security controls and control objectives [11, 13, 14] in each entity of the cloud.

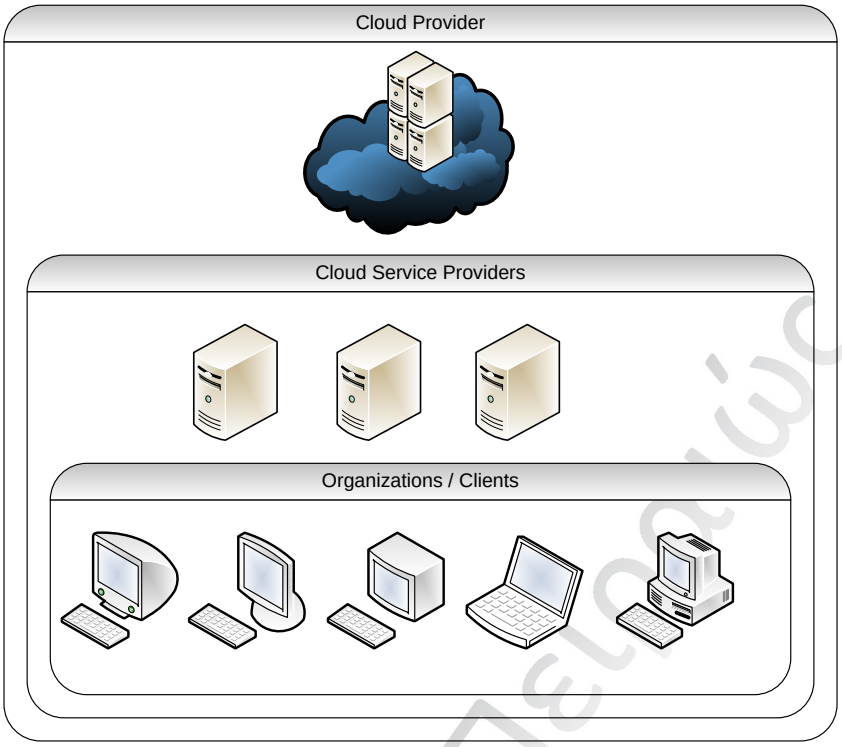

Figure 3 – *Cloud Entities*

Security Policy

Cloud Provider must have set and update an Information security policy document. Cloud Service providers must also have their own information security policy document based on the cloud providers document. Cloud providers and Cloud service providers should review the information security policy.

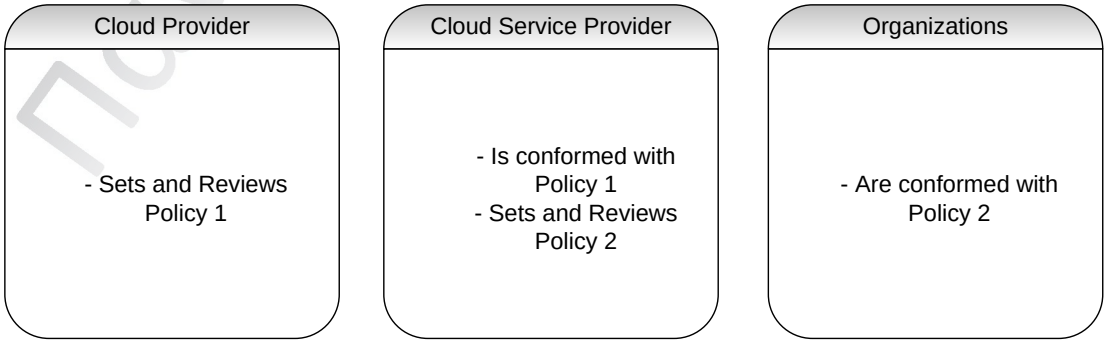

Figure 4 – *Information Security policies of the Cloud*

Organization of information security

In this section we should adopt controls to target the objective of managing information security within the cloud entity (Provider, Service Provider, or Organization). In addition, to maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties. An external party is any Cloud entity except the current entity where the control is applied.

BS ISO/IEC 27001:2005 says that appropriate contacts with relevant authorities shall be maintained. This control may not be applicable in Cloud, because of many different authorities that have different security requirements.

In addition, the organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur. This should be minded also when security changes are applied on the upper levels of the Cloud.

The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access. As external parties we could face upper and lower levels of the Cloud.

All identified security requirements shall be addressed before giving customers access to the organization's information or assets. As customers we could face the lower levels of the Cloud.

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements. As third party we could face upper and lower levels of the cloud.

Asset Management

Asset is anything that has value to the organization [14]. In our case as asset we define anything that has value to a part of the Cloud.

Types of assets

- Information: Databases and Data files, contracts and agreements
- Software Assets: Application software, system software, development tools, and utilities.
- Physical Assets: Computer equipment, communications equipment, removable media, and other equipment.
- Services: Computing and communication services, general utilities.
- People: People and their qualifications, skills and experience.
- Intangibles: Reputation and image of the organization

[15]

The responsibility for assets has the objective to achieve and maintain appropriate protection of organizational assets. Inventory, ownership and acceptable use of assets are suggested in [11]. Here we could include the "chartering of assets", where we face the responsibility of chartered assets by third parties.

Moreover, information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization. But in the Cloud the legal requirements may vary in each country where an entity is placed, and sensitivity and criticality of a specific information vary for each entity of the Cloud.

Human Resources Security

Human resources security is structured in three key categories:

- *Prior to employment:* Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy, in accordance with Cloud security policy. In addition, background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Laws, regulations and ethics vary in different areas, so this fact makes the objective more difficult to achieve (maybe not applicable). Furthermore, as part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security. This could be achieved by a contract between neighbour levels of the Cloud.

- *During employment:* First of all management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the Cloud. Also, all employees of the organization and, where relevant, contractors and third party users shall receive appropriate

awareness training and regular updates in organizational policies and procedures, as relevant for their job function. Finally, there shall be a formal disciplinary process for employees who have committed a security breach.

- *Termination or change of employment:* To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner, three controls should be applied; Firstly, responsibilities for performing employment termination or change of employment shall be clearly defined and assigned. Secondly, all employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement. Finally, The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Human being is vulnerable entity of an information system and also for the cloud. In a Cloud there are many humans with different objectives, different roles and responsibilities, and – the most important – with different education, knowledge, ethics and characters. Thus the main target of Cloud security, and also the most important vulnerability (in some cases also a threat) is human.

Physical and Environmental Security

In order to prevent unauthorized physical access, damage and interference to the organization's premises and information, intermanagement responsibility should be applied in all levels of a Cloud. Also, in order to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities, the equipment of the cloud should referred clearly and assigned to specific entities in the contract.

It is difficult to define the exact physical limits of an area, as cloud is distributed in the whole world. Thus a lot of controls in this section are not applicable in the whole Cloud but only in each entity.

Communications and Operations management

In order to ensure the correct and secure operation of information processing facilities, operating procedures shall be documented, maintained, and made available to all users who need them. In addition, changes to information processing facilities and systems shall be controlled. Moreover, duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized modification or misuse of the organization's assets. Finally, development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system. The possible changes or updates of information, shall be sent to all parties, in order to be informed and up to date.

To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements, It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. Also, the services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly. In addition, changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

To minimize the risk of systems failures, we face two controls. The first is that the use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. The results should be sent to the upper levels of the Cloud. The second is that acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance. After that, new versions of contract, or new contracts should be signed.

Protection against malicious and mobile code should be established in order to protect the integrity of software and information. Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. Also, where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing. Both controls shall be applied in each level of the Cloud.

To maintain the integrity and availability of information and information processing facilities, back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy. If a level is responsible for taking backup of lower levels, this must be included in the contract.

In network security management, to ensure the protection of information in networks and the protection of the supporting infrastructure, networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. In addition, security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. For these controls, it is better to follow a top-to-bottom approach.

For media handling, to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities, there shall be procedures in place for the management of removable media and media shall be disposed of securely and safely when no longer required, using formal procedures. Furthermore, procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse and system documentation shall be protected against unauthorized access. The management of removable media, the disposal of media, security of system documentation controls, also the information handling procedures should be applied in each level independently. Finally, the information handling procedures should be documented in the contract.

To maintain the security of information and software exchanged within an organization and with any external entity, formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities and agreements shall be established for the exchange of information and software between the organization and external parties. For information exchange and exchange agreements a new contract should be established. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries. This control should be applied in each level. Moreover, information involved in electronic messaging shall be appropriately protected, in cooperation with all levels in a unique shared log file. Finally, policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

A very important objective for a Cloud is to ensure the security of electronic commerce services, and their secure use. The controls to target this objective are three; The first is that Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. The second is that Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. The last is that the integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.

To detect unauthorized information processing activities [11] recommends six controls:

- Audit logging
- Monitoring system use
- Protection of log information
- Administrator and Operator logs
- Fault logging actions
- Clock synchronization

For the Cloud we could add one more control; Monitoring electronic messaging in the Cloud. It is necessary for Cloud provider, to have the global control of sensible information communicated.

Access Control

For access control in all levels Cloud provider should be responsible. It is clear the need of only one entity to have the control. We may have single point of failure, but global administration for access control is the best solution could be applied in the cloud reality. Also a new authority could be founded (under the Cloud provider supervision) responsible for access control.

Information systems acquisition, development and maintenance

The controls related to security requirements of information systems, correct processing in applications, security of system files, security in

development and support processes, and technical vulnerability management, should be applied in all levels.

The most important controls in this section are related to cryptographic controls, such as policy on the use of cryptographic controls and key management. In a cloud we face different parties and different crypto-algorithms in each entity. Thus, the controls may be not applicable or could be applicable only using central administration from the highest levels. An other idea is to define minimum security requirements in order to be part of a specific cloud.

Information Security Incident management

A central authority should be responsible for security incident management for all levels of the cloud. This authority should communicate with the whole cloud as soon as possible, for any security incident. Reporting information security events and security weaknesses, responsibilities and procedures, learning from incidents and collection of evidence should be managed by one authority.

Business Continuity management

In order to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption, five security controls should be followed [11]:

- A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
- Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
- Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
- A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
- Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

All of the above should be managed by the cloud provider, in cooperation with cloud service providers and organizations. Also an authority could be founded responsible for the business continuity plan.

Compliance

ISO 27001:2005 faces the compliance in two categories [11]:

- *Compliance with legal requirements*: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
- *Compliance with security policies and standards, and technical compliance*: To ensure compliance of systems with organizational security policies and standards.

Compliance with legal requirements is very difficult to achieve, as a cloud is distributed around the world and in each place there are different regulations and lows. This issue could be faced if minimum legislation requirements applied to the whole cloud, but this fact could produce new functional issues.

Compliance with security policies and standards, and technical compliance could be faced by the cloud provider in cooperation with the custom authorities.

Updating ISO 27000 controls for the Cloud

A.5 Security policy

- Cloud provider defines Policy_1
- Cloud Service providers run the policy_1 and make recommendations to the Cloud Provider, as reviewers
- Cloud Service provider sets Policy_2
- Internal organizations run Policy_2

A.6 Organization and Information Security

A.6.1.6 Contact with Authorities (NOT applicable)

- Many different authorities in the whole Cloud
- Contract between all authorities with similar requirements

A.6.1.8 Independent review of Information Security

- Even if changes are applied in upper levels

A.6.2 External parties

- As external party we include any node for each other

A.7 Asset management

New control A.7.n Chartering of Assets

- Responsibility of chartered assets
- Contract between Owner and Charterer

A.8 Human Resources security

A.8.2.2 Information Security awareness, education and training

- Adjustments to the training program in order to depend on the cultural, national and educational characteristics of each set of employments

New control A.8.n Termination or change of a Cloud Communication, connection or usage

A.9 Physical and environmental Security

- NOT applicable to the whole Cloud
- Only on each party

A.10 Communications and operations management

- Applicable to the whole Cloud

A.11 Access control

- Only one authority responsible for access control
- Cloud provider or an independent authority

A.12 Information systems acquisition, development and maintenance

A.12.3 Cryptographic controls

- Different cryprtographic algorithms in each organizations
- Set of minimum cryptographic requirements in order to join the Cloud

A.12.5.5 Outsourced software development

- Shall be supervised and monitored by the cloud provider

A.13 Information Security Incident management

- A central independent authority responsible for all levels
- In cooperation with all parties

A.14 Business Continuity management

- Supervised by the Cloud provider or an independent authority

A.15 Compliance

- Compliance with legal requirements is not applicable unless we make a collection of all legal requirements around the countries involved in the cloud
- Compliance with security policies is applicable to all levels

Chapter References

[11] ISO/IEC 27001:2005, International Standard

[13] NIST, "Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144

[14] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.

[15] ISO/IEC 27002, International Standard

Chapter 6

Conclusions And Outlook

Nick Papatheodoulou

The standards we should adopt should be more suitable to cloud reality. One of the most important differences is that the security controls should be distributed to each cloud entity.

The ideal standard should be focused in national characteristics and culture of the human as a part of information system. In this phase we should examine the critical infrastructures of each region.

Also, the standard should mind the geographical natural characteristics of each region involved in the cloud. For example if an entity of the cloud is placed in an area that has a lot of physical disasters (such as earthquakes), is more dangerous than an entity placed in a safe area.

In addition, we should research the legal notices and laws of its nation, before applying a security control.

Another issue is that we should know the average education of the human entities of the cloud, in order to approach a security awareness program.

Thus, we understand that the security controls should be adaptable in each case. Another approach is that the controls should not be unique for a reason. We could have more than one control for the same reason, or different instances of the same control.

There is no one-size-fits-all model for security in the Cloud. Organizations have different security requirements that are determined by the unique characteristics of the business workload they intend to migrate to the Cloud.

Organizations have many different requirements for integration between the cloud environment and their back-end systems. Some organizations are developing entirely new applications and are prepared to build their cloud environment to be independent from any existing operations, but most enterprise clients will start with a hybrid or private cloud where integration with their enterprise systems is a central requirement.

Different types of workloads require different levels of security. One of the most important requirements is the need for a third-party security audit or validation, and governments are even expressing a need for formal validation and certification. The strength of identity proofing – making sure that the users who log on to the service are really who they claim they are – and the strength of authentication mechanisms may vary depending on the workload type. In response, new public services for identity verification are being set up, offering vary degrees of service quality.

Encryption requirements are very different from one client to another. Certain clients mandate the use of specific crypto-algorithms and require very high restrictions on who can have access to the keys, while other clients may demand encryption only for specific data and may want to delegate key management to a trusted cloud provider.

There is a large variation in availability requirements, including the time allowed for the provider to react to and recover from failure. Requirements also vary for the intervals at which security and compliance checks are performed.

As a result, information security management in cloud computing must be flexible and adaptable in each case of Cloud scenarios and implementations. An Information Security Management System for Cloud computing could be implemented in two approaches:

- Non-centric approach
- Object Oriented Approach

In the non-centric approach we examine the specific security characteristics of each node. As a node we could name each part of the cloud. (For example: cloud service providers, cloud providers and each organization in the cloud). On the other hand, in the Object Oriented approach, each node could be focused as an object with specific security attributes, as presented on figure 4.

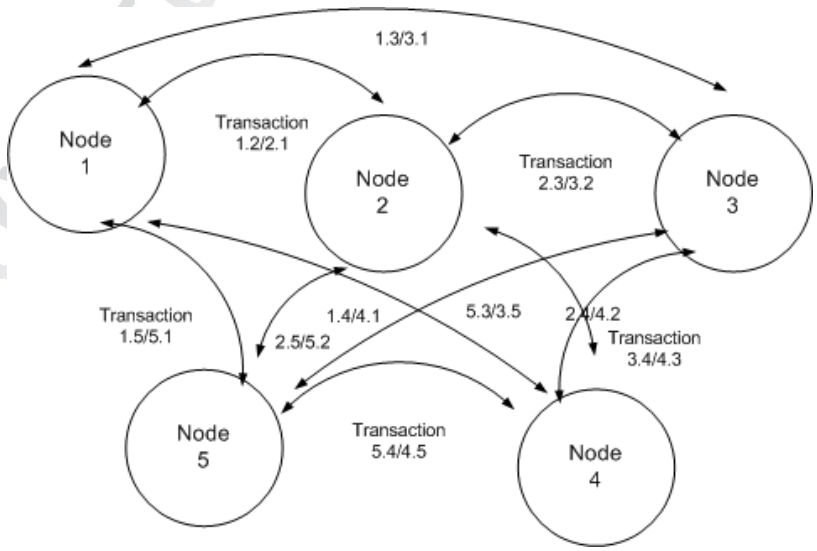

Figure 4 – *Object Oriented Approach of the Cloud Security Management*

In this approach we should mind the transactions between the nodes as object attributes.

Chapter 7
Global References

[1] Rajkumar Buyyaa, Chee Shin Yeoa, Srikumar Venugopala, James Broberg, Ivona Brandic, *"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility"*, Future Generation Computer Systems, Elsevier, 2009

[2] Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, *"A Taxonomy and Survey of Cloud Computing Systems"*, 5th International Joint Conference on INC, IMS and IDC, 2009

[3] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong, *"The Characteristics of Cloud Computing"*, in Proceedings of IEEE 39th International Conference on Parallel Processing Workshops, 2010

[4] Liang-Jie Zhang and Qun Zhou, "*CCOA: Cloud Computing Open Architecture*", in Proceedings of 2009 IEEE International Conference on Web Services, 2009

[5] Robert Gellman, *"Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing"*, World Privacy Forum, 2009

[6] SNIA, "*Cloud Data Management Interface*", Storage Networking Industry Association, Technical Position, 2010

[7] Won Kim, *"Cloud Compting: Today and Tomorrow"*, Journal of Object Technology, Zurich 2009

[8] Nick Papatheodoulou, Nicolas Sklavos, *"Architrecture and System Design of Authentication, Authorization and Accounting Services"*, in Proceedings of 2009 IEEE International Conference EUROCON'09, 2009

[9] Mladen A. Vouk, *"Cloud Computing – Issues, Research and Implementations"*, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[10] Peter Mell, Timothy Grance, NIST, *"The NIST Definition of Cloud Computing (Draft)"*

[11] ISO/IEC 27001:2005, International Standard

[12] ISO/IEC 27003:2010, International Standard

[13] NIST, "Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144

[14] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.

[15] ISO/IEC 27002, International Standard