Information Security Management System (ISMS) Standards in Cloud Computing-A Critical Review

Conference Paper · August 2013

DOI: 10.13140/RG.2.1.3687.4649

3 authors, including:

Manish Kumar Pandey
Birla Institute of Technology, Mesra
34 PUBLICATIONS **183** CITATIONS

SEE PROFILE

Karthikeyan Subbiah
Banaras Hindu University
43 PUBLICATIONS **300** CITATIONS

SEE PROFILE

Information Security Management System (ISMS) Standards in Cloud Computing-A Critical Review

Manish Kumar Pandey
Department of Computer Science
Faculty of Science
Banaras Hindu University
Varanasi, Uttar Pradesh, India
pandey.manish@live.com

Sunil Kumar
Department of Computer Science
Faculty of Science
Banaras Hindu University
Varanasi, Uttar Pradesh, India
Sunilphd.bhu@gmail.com

S Karthikeyan
Department of Computer Science
Faculty of Science
Banaras Hindu University
Varanasi, Uttar Pradesh, India
karthinikita@gmail.com

***Abstract*—Information security plays an important role for the survival of any organization. So information belonging to an organization must be proactively secured against malicious attacks. Securing of information is more important and much more complex in the present era of cloud computing where whole information is carried over networks. In this paper we discuss about how Information Security Management System (ISMS) standards can be supportive in overcoming the security challenges faced by Cloud Service Providers (CSP) during cloud engineering.**

Keywords—ISMS, CSP, ISO/IEC 27001, PDCA Model, Cloud Security.

I. INTRODUCTION

An information security management policy is very much essential for enterprises and organizations in order to have better management of information security and better fabrication of information. Enterprises and organizations with the help of these policies promises better business operation and accomplish this purpose by applying different set of laws. If the businesses successfully use these standards and get benefits like return on investment in terms of protecting their critical assets at affordable price, then one can conclude that the organization is secured enough to do business that is 'Fit for Purpose' by enforcing Information Security Management system (ISMS) Standards.

There are three main cloud systems categories: Software as a Service, Platform as a Service and Infrastructure as a Service and are explained in more details below:

1) Software as a Service (SaaS): In SaaS Here the cloud users do not required purchasing the software rather the payment will be based on pay-per-use model. It support multi-resident which means that the physical backend infrastructure is shared among a number of users but logically it is unique for each user [4].

2) Platform as a Service (PaaS): In PaaS the development environment will be provided as a service. The developers will use cloud service provider's facilities to create code for their own applications. The platform will be hosted in the cloud and will be accessed using the browser.

3) Infrastructure as a Service (IaaS): In IaaS, cloud service providers offer the infrastructure as a service where it is delivered in form of technology, datacenters and IT services to the customer, which can be compared to the "outsourcing" business with lesser expense and effort [5]. The goal is to provide a solution to the customer based on their desired applications.

978-1 - 4799 - 1375 - 6/13/$31.00 ©2013 IEEE

Cloud Computing refers to deliver services over the internet or on cloud infrastructure. The cloud computing will bring several advantages to the market and cost efficiency, security and scalability are significant among them.

International Data Corporation (IDC) conducted a survey [1] on use of IT cloud services by taking opinion from 263 IT executives and their line-of business colleagues. The major outcome of the survey was Security concern which was ranked first among the challenges of cloud computing.

Most of the organizations are analyzing the cloud technology as cost economy tool despite of the consequences of the level of the security provided by the Cloud Service Provider (CSP), but it is difficult to measure the payback in term of single category where the saving represents the cloud computing Rate of Interest (RoI) from the research conducted by IBM group as discussed by Richard Mayo and Charles Perng in [2].

In this paper, we will mainly focus on various Information Security Management System Standards and how these could be useful in building confidence in Cloud Computing environment as far as security is concerned.

II. HISTORICAL ROOTS OF ISMS

In the early 90s a business group was set up by the UK government to take ahead the idea of best security practice for the advantage of business at large. The conclusion was a code of practice for information security management to be adopted as a UK standard BS 7799-1 in 1995. Two years later the UK published a second standard BS 7799-2, which has title ISMS specification as outlined in [3].

The main motive behind this second publication was to have an agreement standard against which organizations ISMS performances could be certified.

Subsequently the UK developed an ISMS certification scheme based on BS 7799-2 standard and success of its testing resulted in official launch of the first ISMS certification scheme.

In October 2000 UK standard BS 7799-1(code of practice for information security management) was submitted to ISO/IEC and was accepted for publication as ISO/IEC 17799. This standard was eventually renumbered as ISO/IEC 27002 in 2006.This was followed by next set of regularity when BS

7799-2 which was introduced in to ISO and was published as ISO/IEC 27001.

ISO/IEC 27001 provides a sequence of security process based on the well known Plan-Do-Check-Act (PDCA) model as described in Figure 1[3].

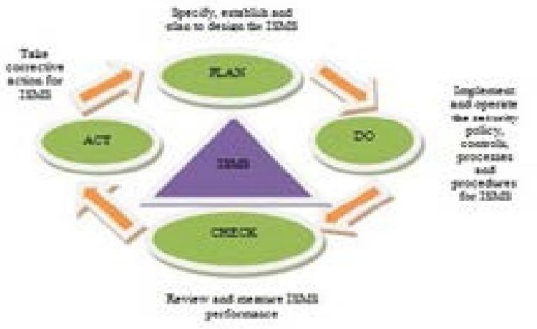
Specify, establish and plan to design the ISMS
Take corrective action for ISMS
PLAN
Implement and operate the security policy, controls, processes and procedures for ISMS
ACT
ISMS
DO
CHECK
Review and measure ISMS performance

Figure 1 | ISMS Process Model

III. INFORMATION SECURITY MANAGEMENT SYTEM (ISMS) STANDARDS

(a) ISO\IEC 27001 standard

BS7799 was published in 1995 and first part of it is accepted by international standard organization in 2000. Its second part was published in 1997 as title "how we implement the information security management?" Its third part was published in 2005 and covered risk analysis and management and named as ISO\IEC 27001. This standard uses clear administration in order to provide information security. This standard requires that:

i. Administration must check the information security risk and consider threats.
ii. There has to be a logical design and accomplishment of information security control and
iii. Information Security control continuously provides specified security requirements.

(b) ISO\IEC 27002 standard

This standard provides suggestions which are very useful in realistic accomplishment. These are:

1. Information Security Policy
2. Risk Assessment
3. Organizing Information Security
4. Asset management
5. Human Resources Security
6. Physical and environmental security
7. Communications and Operations management
8. Access control
9. Maintenance and development of Information Systems
10. Information Security Incident management
11. Compliance with standards.

Note: - *In most cases ISO\IEC 27001 and ISO\IEC 27002 are applied together. In other words they compensate each other. The organization or enterprise that implements ISO\IEC 27002, must consider the requirements of ISO\IEC 27001 simultaneously.*

(c) ISO\IEC 27003 standard

This standard is introduced in 2010 and its intention is to provide guidance for accomplishment of information security management in accordance with ISO/IEC 27001. These are:

1. Introduction and Scope of ISMS
2. Organizational Structure Definition
3. Assurance to access management for implementation of information security management
4. Definition and scope of information security policies
5. Organizational investigation control
6. Risk evaluation control and risk management investigation
7. Information security management system design

This standard does not cover the operational activities and other ISMS behavior, but covers the concepts on how to design the behavior, which will result after the ISMS operations start.

(d) ISO\IEC 27004 standard

This standard is introduced in 2010. Its purpose is to evaluate non compliant and ineffective ISMS processes and systematically improve ISMS processes. The parts of this standard are:

1- Information security measurement
2- Management Accountability
3- Measurement and development
4- Measurement operation
5- Report Information analysis and results of measurement
6- Evaluation and improvement of information security management program

(e) ISO\IEC 27005 standard

This standard is introduced in 2008. Its purpose is to provide guiding principle for information security risk management in an organization. This standard supports ISO\IEC 27001 concepts. This standard doesn't advocate or establish unusual way of risk analysis but specify structured and systematic process for it.

(f) ISO\IEC 15408 standard

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. This standard was published in later 1994. Its purpose is to provide a framework in which users can enter their assurance requirement and functional security, on the basis of these requirements, implementation and evaluation is done for their products. Main steps in this standard are:

1. Profile security
2. Target security
3. Security functional requirements
4. Security assurance requirements
5. Evaluation assurance level

IV SECURITY ISSUES IN THE CLOUD

Security issues and challenges

Malicious Security threats needs to be conquered in order to take advantage of cloud computing paradigm. Some security concerns are listed:

- Physical security is lost because of sharing computing resources with other companies.
- Violation of the law which results in data seize.
- Incompatibility with another vendor's services if user decides to move from one to the other.
- Control of the encryption/decryption keys has to be with customer.
- Ensure the integrity of the data that is it changes only in case of authorized transactions.
- Users have to keep up to date with application improvements to make sure that they are protected.
- A number of government rules have severe restrictions on what information about its people can be stored and for how long, and some banking authorities require that customer's financial information remain in their home nation.
- The dynamicity of virtual machines will make it hard to maintain the consistency of security and ensure the audit ability of records.
- Customers may be able to take legal action against cloud service providers if their privacy rights are violated, and in every case the cloud service providers may spoil their status.

Privacy sensitive information: [6]

- Personally identifiable information (PII [7]): any information that could be used to recognize or find an individual (e.g. state, name, address) or information that can be correlated with other information to recognize an individual (e.g. Social Security number, Internet protocol (IP) address).
- Data collected from computer devices.
- Information uniquely traceable to a user device (e.g. IP address, MAC address).

Supplementary considerations to be aware of:

- *Access*: Data subjects can claim what personal information is held and, in some cases, can make a request to stop processing it. If a data subject can claim to ask the organization to delete its data, will it be possible to guarantee that all of its information has been deleted in the cloud?
- *Compliance*: What are the valid laws, policies, standards, and contractual commitments that govern this information, and who is responsible for maintaining the compliance? Clouds can cross multiple jurisdictions in multiple states.
- *Storage*: Where is the information in the cloud stored? Was it transferred to another data center in another country? Privacy laws in a number of countries put restrictions on the ability of organizations to move some types of personal information to other countries.
- *Retention*: What is the duration of retention of personal information? Who governs the retention policy in the cloud, and how any exceptions (if any) are managed?
- *Destruction*: What is the guarantee of cloud service providers (CSP) not retaining additional copies of data?
- *Audit and monitoring*: How organizations monitor their CSP and promise to relevant stakeholders that privacy is maintained when their PII is in the cloud?
- *Privacy breaches*: How can we make sure that the cloud service provider (CSP) notify us when a violation occurs, and who is in charge for running the violation notification process as well as costs associated with the process.

V ISMS USED AS A STANDARD TO MANAGE CLOUD COMPUTING SECURITY THREATS

Standards those are relevant to security management practices in the cloud are Information Technology Infrastructure Library (ITIL), ISO/IEC 27001/27002 and Open Virtualization Format (OVF).

Here we will discuss ISO/IEC 27001/27002 standard.

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It is also a certification standard and uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS.

Essentially, the ITIL, ISO/IEC 20000, and ISO/IEC 27001/27002 frameworks help IT organizations internalize and respond to basic questions such as:

- "How we make sure that the present security levels are suitable for your needs? "
- "How we apply a security baseline all the way through your operation? "

In a word, they assist us to respond to the question: "how we guarantee that our services are secure?"

With cloud computing and success of doing business online, customer spending and accessing huge amount of information and also the increasing customer demand for more connectivity and mobile technologies ways of business, organizations have been exposed to a sequence of risks due to the lack of information security. When something goes wrong and data is lost, damaged, stolen or unavailable then business and customer confidence gets eroded. More and more tenders, contracts and service level agreements necessitate that the provider has implemented suitable information security measures.

ISO/IEC 27001 has become a world renowned "common business language' for information security management systems. It provides a risk management approach to determine a proper set of security measures or controls to ease and manage an organization's risk to an acceptable level to solve the problems mentioned above.

Following are the measures that can be used in cloud environment for delivering business value.

Tactical Configuration

- ISMS should be driven by project requirements;
- Security solutions should be 'fit for purpose' for project processes;
- Investment in information security needs to be allied with enterprise strategy and agreed upon the organization's risk profile.

Value delivery

- A standard set of security practices (following the

ISO/IEC 27002);

- Prioritized and distributed effort to fields with greatest impact and business benefit;
- Full and tailored solutions covering organization's process as well as technology;

Risk Management (ISO/IEC 27001 and 27005);

- Identification of various risks and decision on risk profiles has to be made*;*
- Understanding the impact of risk exposures*;*
- Risk awareness by users*;*
- Risk management plan and priority for taking action;
- Risks and information security measurements (ISO/IEC 27004);
- Review of risks regularly.

Performance and System Assurance Measurement (ISO/IEC 27004);

- Set of metrics needs to be defined;
- Feedback enabled measurement process on progress made is required;
- Reviews and audits (ISO/IEC 27007 + 27008);

Performance Maintenance and/or Improvement

- Monitoring and review of the ISMS – Whether the output from security investment is fruitful or is there a need for ISMS improvements;
- Assessment of performance and the effectiveness of the ISMS controls;
- Implement improvements – add new conduct and/or improve existing conducts.

VI CONLUSION

Cloud computing is very profitable and successful environment if provided with sufficient security. Enhancing the security and privacy policies will attract more organizations to come under the cloud environment. The ISMS standards play a vital role in managing and certifying information security in organizations. Thus by improving ISMS standards in cloud computing environment could result in better confidence of organizations in cloud environment.

VII REFERENCES

[1]. International Data Corporation, http:// blogs.idc.com /ie /wpcontent /uploads /2009 /12 /idc_cloud_challenges_2009.jpg, 2009

[2]. Richard Mayo, Charles Perng, "An explanation of where the ROI comes from", IBM, November 2009.

[3]. James Butler-Stewart author (2009), Father of ISMS Standards (BS 7799-1 | ISO/IEC 27002 & BS 7799-2 | ISO/IEC 27001), Infosec Publications, Australia, India and USA

[4]. T. Mather, S. Kumarasuwamy and S. Latif, "Cloud Security and Privacy", O'Rielly, ISBN: 978-0-4596-802769, 2009.

[5]. J. W. Rittinghouse,J. F. Ransome, "Cloud Computing: Implementation, Management and Security" CRC Press, ISBN: 978-1-4398-0680-7, 2009.

[6]. S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", CLOUD'09, May 23, 2009, Vancouver, Canada

[7]. Wikipedia, 20 January 2010, http:// en.wikipedia.org /wiki / Personally_identifiable_information