2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010)

Information Security Risk Management Framework for the Cloud Computing Environments

Xuan Zhang
School of Software
Yunnan University,
Yunnan, China
zhxuan@ynu.edu.cn

Nattapong Wuwong
School of Information,
Yunnan University, Yunnan, China
wojiaowudapeng@qq.com

Hao Li
School of Software
Yunnan University,
Yunnan, China
Lihao707@ynu.edu.cn

Xuejie Zhang
School of Information,
Yunnan University,
Yunnan, China
xjzhang@ynu.edu.cn

***Abstract*-The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security controls involved in a particular cloud environment [7].Over time, organizations tend to relax their security posture. To combat a relaxation of security, the cloud provider should perform regular security assessments [3]. Risk management framework is one of security assessment tool to reduction of threats and vulnerabilities and mitigates security risks.**

The goal of this paper is to present information risk management framework for better understanding critical areas of focus in cloud computing environment, to identifying a threat and identifying vulnerability. This framework is covering all of cloud service models and cloud deployment models. Cloud provider can be applied this framework to organizations to do risk mitigation.

Keywords-cloud computing; risk management framwork

I. INTRODUCTION

Although the benefits of cloud computing are clear, so is the need to develop proper security for cloud implementations. In addition to the usual challenges of developing secure IT systems, cloud computing presents an added level of risk because essential services are often outsourced to a third party. The externalized aspect of outsourcing makes it harder to maintain data integrity and privacy, support data and service availability, and demonstrate compliance [1]. For example, IDC recently conducted a survey (see Figure 1) of 244 IT executives/CIOs and their line-of business (LOB) colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing [10].

Supported by the Science Project of Yunnan University (No. 2007Q025C).

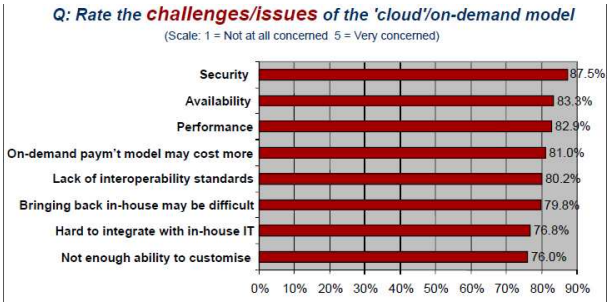

FIGURE 1. Cloud User Surveys 3Q09 – Security is the "Usual" Challenge (Source: IDC Enterprise Panel, September 2009)

Many of the risks frequently associated with cloud computing are not new, and can be found in enterprises today. Well planned risk management activities will be crucial in ensuring that information is simultaneously available and protected [9]. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

In cloud computing environment is available in several service models and different models have various ways to mitigation a vulnerabilities and threats, as this paper provides a comprehensive framework for better understanding enterprise security. Cloud provider can be applied this framework to organizations to do risk mitigation.

II. INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK

This framework was developed in a standard quality management (or Plan, Do, Check, Act) cycle of continuous improvement based on evolving ISO/IEC 27001 standards [8], NIST risk management guide for information technology systems [12] and Booz Allen Hamilton information security governance government considerations for the cloud computing environment [2]. The framework was to describe in terms of the Cloud Security Alliance security guidance for critical areas of focus in cloud computing [6] that should be protected and

978-0-7695-4108-2/10 $26.00 © 2010 IEEE
DOI 10.1109/CIT.2010.501

designed to protect the confidentiality, integrity and availability of information assets.

The framework have seven processes, including: processes-selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. Each process will be necessary to clarify specific roles, responsibilities, and accountability for each major process step. Assumption in the following discussion is that Chief Information Security Officer (CISO) and Chief Information Officer (CIO) are primarily the responsibility of a centralized information security function.

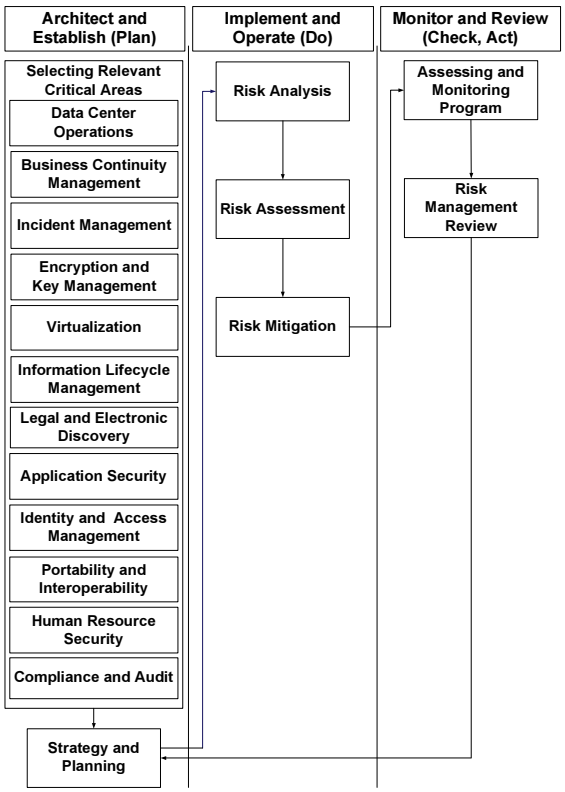

FIGURE 2. Overview of risk management framework for cloud computing environment

A. Architecting and Establishing the Risk Management Program (PLAN)

Designing and planning for an effective information security risk management occurs through two major processes: selecting relevant critical area, strategy and planning.

1) Selecting Relevant Critical Area

The twelve domains which comprise the Cloud Security Alliance security guidance for critical areas of focus in cloud computing [6] and Booz Allen Hamilton information security governance government considerations for the cloud computing environment [2] highlight area of concern for cloud computing and are tuned to address both the strategic and tactical security "pain points" within cloud environment. It covers all of cloud service models and cloud deployment models.

Before move to next step must select at least one critical area that relevant, for example if you are SaaS provider you may select application security, identify access management, or encryption and key management area to analyzing, assessing threats and risks of vulnerabilities to organization.

2) Strategy and Planning

Strategy and Planning are essential to an effective information security risk management program. The primary purposes of the strategy and planning process are to:

- Establish risk management program direction and guide activities.
- Create steering committee and working committee.
- Define the risk management program goals, requirements, and scope.
- Proactively plan activities to achieve goals and meet requirements.

The process is performed in collaboration with the selecting relevant critical area and strategy planning processes to ensure plans effectively communicate management intent clearly define roles and responsibilities, identify critical area of focus, and provide management clear choices for resource allocation and optimization.

B. Implement and Operate (Do)

Implement and operate encompasses three processes: risk analysis, risk assessment, and risk mitigation.

1) Risk Analysis

Risk analysis is the first process in the implement and operates of risk management framework. The greatest benefit of a risk analysis is whether it is prudent to proceed. It allows management to examine all currently identified vulnerability concerns. To be effective, a risk analysis process must be accepted as part of the business process of the enterprise.

Most qualitative risk analysis methodologies make use of a number of interrelated elements [4]:

- **Threat Identification**. – The ability for malware (or a cracker) to remotely exploit vulnerabilities of infrastructure components, network services, and applications remains a major threat to cloud services. It is an even greater risk for a PaaS and IaaS delivery model where vulnerability, patch, and configuration management responsibilities remain with the customer [12]. Table 1 shows the output from threat identification step.

TABLE 1. OUTPUT FROM THREAT IDENTIFICATION

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	Hacking, Social engineering, System intrusion, Unauthorized system access
Computer criminal	Destruction of information, Illegal information disclosure, Monetary gain, Unauthorized data alteration	Computer crime (e.g., cyber stalking), Fraudulent act (e.g., replay, impersonation, interception), Information bribery, Spoofing, System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/Terrorism, Information warfare, System attack (e.g., distributed denial of service), System penetration, System tampering

- **Vulnerability Identification**. – is an essential vulnerability identification element to help protect hosts, network devices, and applications from attacks against known vulnerabilities. Mature organizations have instituted a vulnerability identification process that involves routine scanning of systems connected to their network, assessing the risks of vulnerabilities to the organization, and a remediation process to address the risks**.** Table 2 shows the output from vulnerability identification step.

TABLE 2. OUTPUT FROM VULNERABILITY IDENTIFICATION

Vulnerability	Threat-Source	Threat Action
Terminated employee's system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has indentified flaw in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist. The output of this process helps to identify vulnerabilities and threats for reducing or eliminating risk during the risk mitigation process.

The tangible way to measure success is to see a lower bottom line for cost. Risk analysis can assist in this process by identifying only those controls that need to be implemented.

Another way that the success of a risk analysis is measured is if there is a time when management decisions are called into review. By having a formal process in place that demonstrates the due diligence of management in the decision-making process, this kind of inquiring will be dealt with quickly and successfully [15].

2) Risk Assessment

Risk assessment is the determination of quantitative or qualitative an output from risk analysis process. In this step have four major processes-likelihood determinations, impact analysis, risk determination, Control Recommendations.

- **Likelihood Determination**. – To derive an overall likelihood rating that indicates the probability vulnerability may be exercised within the construct of the associated threat environment. The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, low. The output from likelihood determination step is likelihood rating.

TABLE 3. LIKELIHOOD DEFINITIONS

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

- **Impact Analysis**. The step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or combination of any, of the following three security goals: integrity, availability, and confidentiality that can be describes qualitative categories as high, medium, low.

TABLE 4. MAGNITUDE OF IMPACT DEFINITIONS

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

- **Risk Determination**. – The purpose of this step is to find the risks and opportunities that impact of critical area's risk that selected in (Selecting Critical Area) section. The sample matrix in Table 5 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level.

TABLE 5. RISK DETERMINATION – RISK LEVEL

Threat Likelihood	Impact		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	High 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Medium 50 x 0.1 = 5	High 100 x 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Table 6 describes the risk levels shown in the above matrix. This risk scale, with its rating of High, Medium, and Low, represents the degree of level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level. Output from this step is risk level (High, Medium, or Low).

TABLE 6. RISK SCALE AND NECESSARY ACTIONS

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be out in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA (Designated Approving Authority) must determine whether corrective actions are still required of decide to accept the risk.

- **Control Recommendations. -** During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommend controls is to reduce the level of risk to cloud computing environment and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solution to minimize or eliminate identified risks: Implement and maintain a security program, Build and maintain

a secure cloud infrastructure, Ensure confidential data protection, Implement strong access and identity management, Establish application and environment provisioning, Implement governance and audit management program, Implement a vulnerability and intrusion management program, Maintain environment testing and validation, etc.. [1].

3) Risk Mitigation

Cloud provider must development of risk treatment plans (RTP) with multiple options (avoidance, transfer, retention, reduction, and acceptance). The outcomes of risk treatment plans should be incorporated into service agreements. Because different models of cloud computing have various ways to mitigation a vulnerability and threat.

C. Monitoring and Review (Check, Act)

After the risk treatment plans are implemented, cloud provider subsequently initiates specific follow-on actions as part of comprehensive assessing and continuous monitoring program for effectiveness. Monitoring the risk treatment plan is one of the major areas of activity as part of the Plan, Do, Check, Act (PDCA) process model. Cloud provider should be monitoring risk treatment plan, such as: Monitoring effectiveness and performance, Monitoring the risks and business impacts, Monitoring people awareness, competence and utilization of the risk treatment plans (RTP).

1) Assessing and Monitoring Program

The organization subsequently initiates specific follow-on actions as part of a comprehensive continuous monitoring program. The continuous monitoring program includes an ongoing assessment of risk to determine if there is a need to modify or update the current deployed set of security controls based on changes in the information system or its environment of operation. In particular, the organization revisits on a regular basis, the risk management activities described in the risk management framework, there are certain events which can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls [13].

2) Risk Management Review

The purpose of the risk management reviews is to assist in the development of a focused approach to loss prevention. The review is used to develop a program effectiveness grid that is used first to establish a baseline, then set goals and objectives and evaluate progress.

III. USE OF THE FRAMEWORK

Use of the framework in this paper came from E-commerce Technology Laboratory at Yunnan University, China. They recognized that risk management was an integral part of information security management. They developed a logistics web-based application which is the Software as a Service (SaaS) platform to provide a real-time software service to support logistic industry.

In this section is an example to applying information security risk management framework for the cloud computing into logistic solution to identifying and managing risks. The framework has seven processes-selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. Each process will be necessary to clarify specific roles, responsibilities, and accountability for each major process step.

- **Selecting relevant critical areas.** Relevant critical areas of Software as a Service (SaaS) model are portability and interoperability, incident management, application security, encryption and key management, identity and access management.
- **Strategy and planning.** The goal of this process is to analyze, evaluate risk to do risk reduction to make customer ensure.
- **Risk analysis.** Risk analysis is a step in a risk management process. Risk analysis help organization to do threat, and vulnerability identification**.** OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) is one of risk analysis techniques to examine organizational and technology issues to assemble a comprehensive picture of the information security needs of an enterprise. OCTAVE has three phase-build asset-based threat profiles, identify infrastructure vulnerabilities, and develop strategy and plans [5]. An organization should be use OCTAVE technique to do risk analysis of relevant critical areas that selected in selecting relevant critical areas process. The output of this process helps to identify vulnerabilities and threats for reducing or eliminating risk during the risk mitigation process.
- **Risk assessment.** The risk assessment process using COBRA (Console Operator Basic Requirements Assessment) to assessing output from risk analysis process. The default process usually consists of four stages- likelihood determinations, impact analysis, risk determination, Control Recommendations [14].
- **Risk mitigation.** Creating risk treatment plan to mitigation risk. The plan covers functions/activity, compiled by, compiled date, reviewed by, reviewed date, risks in priority

order, treatment options, preferred options, risk rating after treatment, cost/benefit analysis result (Accept/Reject), person responsible for implementation, timetable for implementation, how to monitor the risk and the treatment options.

- **Assessing and monitoring program.** Conducting internal audit, corrective and preventive defect. The output of this process is internal audit report and corrective and preventive action request.
- **Risk Management review.** Team meeting attendees, team leader, and team committee examine the risk assessment meet plan or not.

IV. The Delicate Balance between Risks and Benefits

The shift of the computing stack provides an opportunity to eliminate complexities, cost and capital expenditure in much the same way that using an electricity provider removes the need for every company to build power generators. The main benefits of cloud computing are therefore economies of scale through volume operations, pay-per-use through utility charging, a faster speed to market through componentization and the ability to focus on core activities through the outsourcing of that which is not core (including scalability and capacity planning).

Providing self-service IT while simultaneously reducing costs may be highly attractive but it creates a competitive risk to doing nothing.

Though service level agreements (SLAs) can help alleviate some concerns, any fears can only be truly overcome once customers can easily switch between providers through a marketplace. This already occurs in many industries from electricity to telephony and it is this switching, which has created competitive markets with competitive price pressures. Until such markets appear, it is probable that many corporations will continue to use home-grown solutions, particularly in industries that have already expended capital to remove themselves from lock-in, which is widespread in the product world.

While the cloud lacks any functioning marketplaces today, it is entirely possible that ecosystems of providers will emerge based on easy switching and competition through price and quality of service. In such circumstances, many of the common concerns regarding the uncertainty of supply will be overcome.

While the benefits of cloud computing are many and obvious, there exist the normal concerns associated with the outsourcing of any activity, combined with additional risks due to the transitional nature of this change [16].

Keep in mind that before moving to the cloud (as with any emerging technology and business model) the most important aspect is that you know your team, know your solutions, and know the cloud providers. The decision to move to the cloud should involve at minimum enterprise architects, developers, product owners/stakeholders, IT leadership, and outsourcing teams. Take into account that human capital in your organization may be lacking. Because exploring new models requires an adventurous spirit and technical astuteness, and if your team is not willing to stretch and learn new things, cloud computing can be very frustrating. Also consider the chance that some of your team elements, may think (and with some reason) that cloud computing may place their jobs at risk.

Some business managers are simply too scared to move forward with cloud initiatives! However, this concern, while valid, is not insurmountable. Solutions do exist and are being fine-tuned every day. There are countless examples of successful cloud computing implementations [11].

V. Conclusion

Cloud computing provides an efficient, scalable, and cost-effective way for today's organizations to deliver business or consumer IT services over the Internet. A variety of different cloud computing models are available, providing both solid support for core business functions and the flexibility to deliver new services.

However, the flexibility and openness of cloud computing models have created a number of security concerns. Massive amounts of IT resources are shared among many users, and security processes are often hidden behind layers of abstraction. More to the point, cloud computing is often provided as a service, so control over data and operations is shifted to third-party service providers, requiring their clients to establish trust relationships with their providers and develop security solutions that take this relationship into account [1]. In this paper we provide a risk management framework for better understanding enterprise security. This framework is covering all of cloud service models and cloud deployment models. Cloud provider can be applied this framework to organizations to do risk analysis, risk assessment, and risk mitigation.

Key to the successful adoption and transition of information systems to a cloud computing environment is the implementation or modification of a strategic proactive information security risk management framework for cloud computing environment. We developed a framework that implemented in logistics Software as a Service (SaaS) project of E-commerce Technology Laboratory at Yunnan University, China. Then we will apply this framework to Infrastructure as a Service (IaaS) environment and Platform as a Service (IaaS) to testing this framework.

References

[1] Axel Buecker, Koos Lodewijkx, Harold Moss, Kevin Skapinetz, Michael Waidner, "Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security," IBM Corp. 2009, pp. 2, pp. 7, pp. 19.

[2] Booz Allen Hamilton, Jim Miller, Larry Candler, and Hannah Wald, "Information Security Governance Government Considerations for the Cloud Computing Environment," pp. 4-11.

[3] Carl Almond, “A Practical Guide to Cloud Computing Security What you need to know now about your business and cloud security,” Avanade Inc., pp. 6, 27 August 2009.
[4] Carrison K.S. Tong and Eric T.T Wong, “Governance of Picture Archiving and Communications Systems: Data Security and Quality Management of Filmless Radiology,” pp. 63.
[5] Christopher Alberts and Audrey Dorofee (CERT), “An Introduction to the OCTAVE Method,” http://www.cert.org/octave/methodintro.html
[6] Cloud Security Alliance, “CSA Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” pp. 30-68, December 2009.
[7] CPNI Centre for the Protection of National Infrastructure, “Information Security Briefing 01/2010 Cloud Computing,” pp. 36, March 2010.
[8] Edward Humphreys, “Implementing the ISO/IEC 27001 Information Security Management System Standard,” pp. 22-25.
[9] ISACA, “Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives,” An ISACA Emerging Technology White Paper, pp 7.
[10] John W. Rittinghouse, James F. Ransome, “Cloud Computing Implement, Management, and Security,” pp. 153.
[11] Maria Spinola, “An Essential Guide to Possibilities and Risks of Cloud Computing,” pp. 12, June 2009.
[12] National Institute of Standards and Technology, Gary Stoneburner, Alice Goguen, and Alexis Feringa, “NIST SP 800-30 Risk Management Guide for Information Technology Systems,” pp. 8-26.
[13] National Institute of Standards and Technology, “NIST SP 800-53 Revision 3 Recommended Security Controls for Federal Information Systems and Organizations,” pp. 27, August 2009.
[14] The Security Risk Analysis Directory, “The Risk Assessment Process,” http://www.security-risk-analysis.com/cobproc.htm
[15] Thomas R. Peltier, “Information Security Risk Analysis,” pp. 3.
[16] Ubuntu, “An Introduction to Cloud Computing,” pp. 5.