# Risk Management Framework in Cloud Computing Security in Business and Organizations

Ibraheem Kateeb
North Carolina A&T State University
kateeb@ncat.edu

Madallah Almadallah
North Carolina A&T State University
malmadal@aggies.ncat.edu

## Abstract

This paper highlights the overview, benefits, and security challenges of cloud computing. The main problem discussed is that several security risks and problems occur when using cloud computing in both sides: users and providers. These problems can decrease the level of trust between the users and providers. Also, as more security incidents occur, more people are worried about using the cloud. In terms of providers, they need to be able to detect and deal with security risks and problems before and after they occur. Thus, a risk management plan for dealing with a few security issues is proposed from the cloud provider's perspective. The main two goals are to increase confidence between the users and cloud provider and to increase the use of cloud computing in all levels.

## Introduction

Cloud-computing technology has rapidly developed. Widespread application is anticipated in social, business, and computing aspects. Cloud computing changes the Internet into a new computing and collaborative platform. It is a business model that achieves purchase on-demand and pay-per-use in a network. Many competitors, organizations, and companies in industry have jumped into cloud computing and implemented it.

Despite of all the advantages cloud computing provides us with, such as convenience, reduced coast, and high scalability, there are a number of enterprises, individual users, and organizations that have still not deployed this innovative technology. Several reasons lead to this problem; however, the main concern is related to security, privacy, and trust. In 2009, international classification of diseases examined 244 IT executives/CIOs and their line-of-business colleagues about their opinions of cloud computing usage. They found that security is the greatest challenge of using the cloud; see Figure 1 [10]. Low trust between users and providers is reported in the literature. It is important to note that choosing cloud computing assumes a high degree of trust between the organization and its provider, as the provider will be trusted with sensitive information and security details. In an attempt to solve the problem and increase the investment and adoption of this technology, this paper provides a comprehensive cloud computing risk management framework based on previous work. This framework can be applied in small and large enterprises, organizations, and companies.

Cloud computing has become popular in the IT industry. Among various virtual ways to deliver computing resources and services is the cloud-computing provider, which is one of the best self-services of the Internet infrastructure.

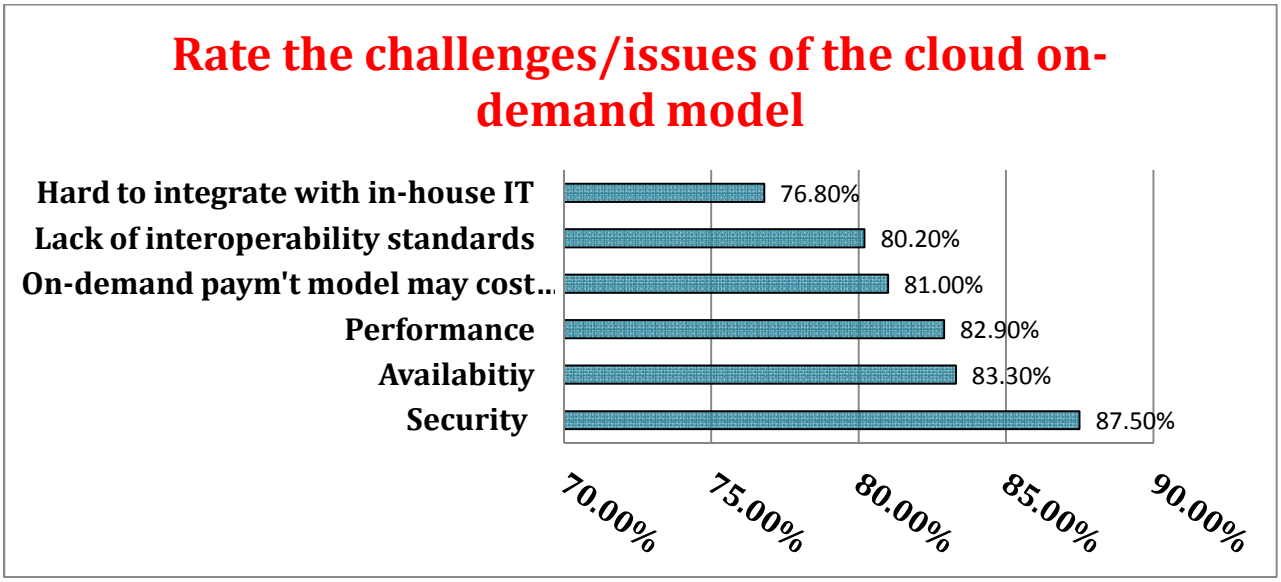


Figure 1. Cloud user surveys 3Q09: security is the "usual" challenge [10]

Cloud computing is a virtual server available over the Internet that enables the user to access computing resources and services, regardless of time and place. Well-knowing cloud computing providers include Amazon Web Services, Microsoft Windows Azure, and Google's Google App Engine. The two main purposes of using cloud computing are to maintain data and get applications. In fact, cloud computing has been improved rapidly and is used widely, especially in the business field. However, no one agrees upon definition of cloud computing. Vaquero et al. defined cloud computing as "a large pool of easily and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized service-level agreements" [1]. Moreover, the National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configuration computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2].

In the 1960s, John McCarthy introduced the fundamental concept of cloud computing. He believed that "computation may someday be organized as a public utility." The term cloud came from the telecommunications world, where telecom companies started offering high quality of virtual private network (VPN) services at a much lower cost [5]. By using VPN services, these companies can switch traffic to balance utilization of the overall network. Now, cloud computing extends this to cover servers and network infrastructure.

Cloud computing has numerous advantages of for providers, adopters, and users. Gupta, Seetharaman, and Raj reviewed some empirical studies on the usage and adoption of cloud computing by small and medium enterprises or small and medium businesses (SMBs) and found that cost reduction, avoiding natural disaster mishaps, sharing and collaboration, trust in cloud providers, reliability, security breaches, and service disruption are the most important parameters. They stated, "One of the biggest advantages of moving to cloud computing is the opportunity cost of freeing up some of the IT administrative time, which can now be applied to the business aspects of growing the core business of SMBs." Jadeja and Modi provided five benefits of cloud computing: easy management, cost reduction, uninterrupted services, disaster management, and green computing. In addition, Brohi and Bamiah revealed that cost reduction, easy scalability, and increased productivity are the main advantages of applying cloud computing [5]. Accordingly, cost reduction, ease of use and convenience, more productivity, reliability, sharing, and collaboration are the highlighted benefits of applying cloud computing.

As any new concept, cloud computing is facing several critical issues; the most prominent is the security issue. According to [3], the "Gartner survey showed that more than 70% of respondents said they do not intend to use the cloud computing at recent, the main reason is afraid of the data security and privacy." Also, they stated that a large number of Google users' files were leaked in March. Aleem and Sprott, as cited in [7], "interviewed 200 Information and Communications Technologies professionals worldwide. Respondents' most cited concern regarding the use of cloud computing was security, as reported by 93.4 percent of interviews." Brohi and Bamiah stated, "According to a survey conducted by International Data Corporation (IDC), 53% of organizations in the Asia-Pacific region are already using some form of cloud computing services, and the remaining 47% of the organizations have plans to adopt private or public cloud services in the next 12 months" [16]. Additionally, they revealed that the survey results indicate that cloud computing is a not highly adopted technology; however, the growing contributions by researchers and IT industries will increase the use of cloud computing globally. As the number of security incidents continues to increase, more people are worried using the cloud. Many studies and researchers have addressed cloud computing threats and other problems.

## Threats

Although many cloud-computing users tend to not worry about doing backups, keeping hackers out of their data or providing more virtual storage space, there are still various risks that users might not realize. The security is a significant problem. Cloud computing contains important and sensitive data, such as personal, government or business data, that attract hackers' attention. Therefore, the cloud-computing system must be protected more carefully than the traditional system. The traditional security mechanisms cannot protect the cloud system entirely [4]. Some of the main security problems include data security, user data privacy protection, cloud computing platform stability, and cloud computing administration [4]. In 2008, "the U.S. information technology research and consulting firm Gartner issued a 'cloud computing security risk assessment' report, mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud, listing seven major security risks that the cloud computing technology exist"; see Table 1 [2]. Cloud-computing

threats can be divided into two types: network and security. Both threats will be discussed in the next section; however, the focus will be on security threats.

Table 1. Seven Top Security Risks

| Risk | Description |
|---|---|
| Privileged user access | Sensitive data processed outside the enterprise brings with it an inherent level of risk |
| Regulatory compliance | cloud computing providers who refuse to external audits and security certifications |
| Data location | The customer probably don't know exactly where your data is hosted |
| Data segregation | Data in the cloud is typically in a shared environment alongside data from other customers |
| Recovery | A cloud provider should tell what will happen to the data and service in case of a disaster |
| Investigative support | Investigating inappropriate or illegal activity may be impossible in cloud computing |
| Long-term viability | Data should remain available even after such an event |

***Security Threats***

As cloud-computing users, we lose control over physical security. So how can we ensure that data will not leak and privacy can be protected? In order to understand the suggested solutions available, types of attack that we might experience should be highlighted. Several security threats can occur in cloud computing:

***Browser Security***. Once a user requests a service from the cloud server, the user's Web browser plays a significant role. Even if the Web browser uses SSL, sniffing packages on an intermediary host can get decrypted data [1]. Also, the attacker uses decrypted data (credentials) as a valid user on cloud system. Web Services Security is a method to eliminate the browser threat by using XML Encryption and XML Signature to guarantee confidentiality and integrity to SOAP messages [1], for example, Kerberos, standard usernames, passwords, and X.509.

***Insecure Interfaces and Application Programming Interfaces APIs***. Cloud users are provided with set of software interfaces or APIs to manage cloud services. Unsecure APIs, which allow software applications to interoperate with each other by passing login information between them, are among the top cloud threats [7]. According to Peerson and Yee, "From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy" [8]. The big concern with this threat is that third parties often build upon these interfaces to offer value-added services to their customers, which increases the security risks.

***Cloud Malware Injection Attack***. This attack works against cloud services, applications, or virtual machines [7]. Attackers can create their own malicious service by using functionality changes or data modifications for specific purpose [1]. Then, they upload this service into the cloud system by tricking it. The cloud system automatically redirects valid user's requests to the malicious service implementation, and that code is executed. To prevent cloud malware injection attack, it is necessary to use the hash function, store a hash value on the original service instance's image file, and compare this value with the hash values of all new service instance images [1].

***Flooding Attacks***. This attack exploits some cloud's features, which increases and initializes new services in order to maintain user's requirements and requests. The attacker requests a huge amount of particular service; this means that cloud computing would not be capable of supplying service to normal users' requests because the system works against the attacker's requests [1]. A denial of service (DoS) attack is one type of forceful flooding attack. According to Qaisar and Khawaja, installing firewall to detect and filter fake requests is a countermeasure for flooding attacks [1].

***Data Protection***. Data protection is very important and complicated for a cloud consumer because it is hard to ensure that the data are handled in a lawful way [1]. For this attack, the consumer should be aware of whether or not the data is handled in a rightful way. In addition, data compromise can occur due to unauthorized parties' accesses, loss of an encoding key, or deletion or alteration of records without a backup of the original content [8].

***Incomplete Data Deletion***. The significant risk that a cloud consumer might experience is incomplete data deletion. The reason is that there are many replicas of these data in other servers, maybe as backup. Also, the majority of operating systems do not delete data accurately or completely. Jamil and Zaki, as cited in [1], revealed that "Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients." Additionally, Qaisar and Khawaja suggested using VPN and query for securing and completing removing of data from cloud servers that have replicate data [1].

***Locks In***. The last security issue is locks in. It is related to data, application, and service portability. There is little offered in the way of tools, procedures, or standard data formats that could assure data, application, and service portability [1]. Therefore, the cloud customer cannot move from provider to another or shift the services back to an in-house IT environment.

***Network Threats***

There are six network issues related to cloud computing:

***Denial of Service (DoS)***. DoS attacks are not new; they can make cloud computing resources and services unavailable to the users [7]. Overflow frequent requests send to the server by attacker to stop the server functionality that provides the services. As a result, the server is

unable to respond to the regular users. According to Qaisar and Khawaja [1], to avoid cloud computing DoS attack, it is important to reduce users/attackers' privileges based on their behaviors when they are connected to cloud server.

***Network Sniffing***. It is a way of analyzing network traffic for hacking unencrypted data that is transmitted through cloud network. To illustrate, if the user does not use encryption techniques during communication with the cloud server, hackers can capture data such as username and password. Therefore, an encryption technique is an effective method to eliminate network-sniffing threat [1].

***Man in the Middle Attack***. During data transmission between user and cloud server, there is a potential threat called "Man in the Middle Attack." According to [7], data that are transmitted without encryption may be hack or stolen. [1] suggested encrypting and compressing the data during transmission by installing a secure socket layer (SSL) to prevent man in the middle attacks.

***Port Scanning***. Attackers use port scanning to discover exploitable communication channels/ports between the user and cloud server. The attacker's goal is to find an active port and exploit vulnerable cloud services [1]. Thus, one main component of network security structure is the firewall. Both user and cloud server need to employ firewalls to detect and filter authorized traffic.

***Structured Query Language (SQL) Injection Attack***. This is a technique that uses a special character/string to gain unauthorized access or to retrieve information from cloud database [7]. For example, if the attacker types 1==1 as an argument value of query in the form field, that may retrieve a whole database table.

***Cross Site Scripting (XSS)***. It is an attack method to obtain the user's sensitive data (credentials) or user's session. The attacker uses a malicious script Web application to redirect the user to the attacker's target [1]. The script will be activated when it is read by an unsuspecting user's browser or by an unprotected application. For example, consider a login or payment page that is hosted on the cloud.com domain: if the attacker discovers XSS vulnerabilities in the domain, the attacker can use Java scripting to steal a user's information. [1] has stated, "Cross site scripting attacks can provide the way to buffer overflows, DoS attacks and inserting spiteful software in to the web browsers for violation of user's credentials."

**Risk Management Framework (RMF)**

In this paper, RMF is suggested for cloud-computing providers regardless of their types and models, based on the NIST risk management guide and McGraw's security risk management. From business perspective, cloud-computing providers were basically found to provide products and services for their own profits. Among various ways to deliver computing resources and services, cloud-computing providers' underlying mission is that every user can use available applications and get services easily regardless of location and the device

operating system. Their basic business goal is to deliver high secure and reliable applications and services. Also, the providers aim to gain costumers trust and loyalty.

Cloud-computing providers have encountered dangerous security risks and problems. These security risks would negatively affect confidentiality, privacy, reliability, and integrity of a provider's services. Therefore, a specific RMF process dealing with security risks and problems is recommended. The basic idea of RMF is simply identify, rank, track, and understand software security risk as it changes over time. This framework can be used widely and flexibly because it can fit with small and large enterprises. Also, the advantage of using RMF is that it "is not specific to security risks; it can be applied in non-software situations" [11]. However, the main goal of using RMF with cloud-computing providers is to consistently track and handle risks and threats.

It is significant to define risk management and its purpose in general. Stoneburner, Goguen, and Feringa defined it as "the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions." The explicit goal of applying risk management in any organization is to minimize negative impacts on organizations and fulfill a need for sound basis in decision making [20].

Tanimoto et al. analyzed cloud computing security problems in detail based on the risk breakdown structure method and the risk matrix method. They provided risks that extracted from user's viewpoints. Xie et al. suggested a risk management framework for cloud computing, which consisted of five components: user requirement self-assessment, cloud service providers desktop assessment, risk assessment, third-party agencies review, and continuous monitoring. Our framework is different from Xie et al. who involved users, providers, and third parties in their framework. We emphasize the business angle in this framework; the marriage of business and technical concerns is the central driver of our risk management plan. Also, increasing the adopters and users of cloud computing is one of this framework goals [13]. Our RMF consists of six stages, discussed in detail in the next section.

A continuous risk management process is a necessity in cloud computing. Also, continuous monitoring process is highly required through ongoing risk identification, implementation and assessment. The risk management plan should be well planned and collaborative between and among different departments. So, sufficient time must be given for planning, collaboration, and communications.

Figure 2 shows that monitoring is needed all the time to ensure that what was expected is actually working. This needs to be performed at consistent time intervals set in the risk management documentation. Sometimes it is necessary to place a watch on areas, and at other times, it will be prudent to change a certain process. If the process has been changed, it is added to the risk management documentation. Some organizations prefer to outsource the monitoring, and others will keep the monitoring in-house. When monitoring cloud services, it might be logical to form a team between several different companies for better mobility in the documentation.

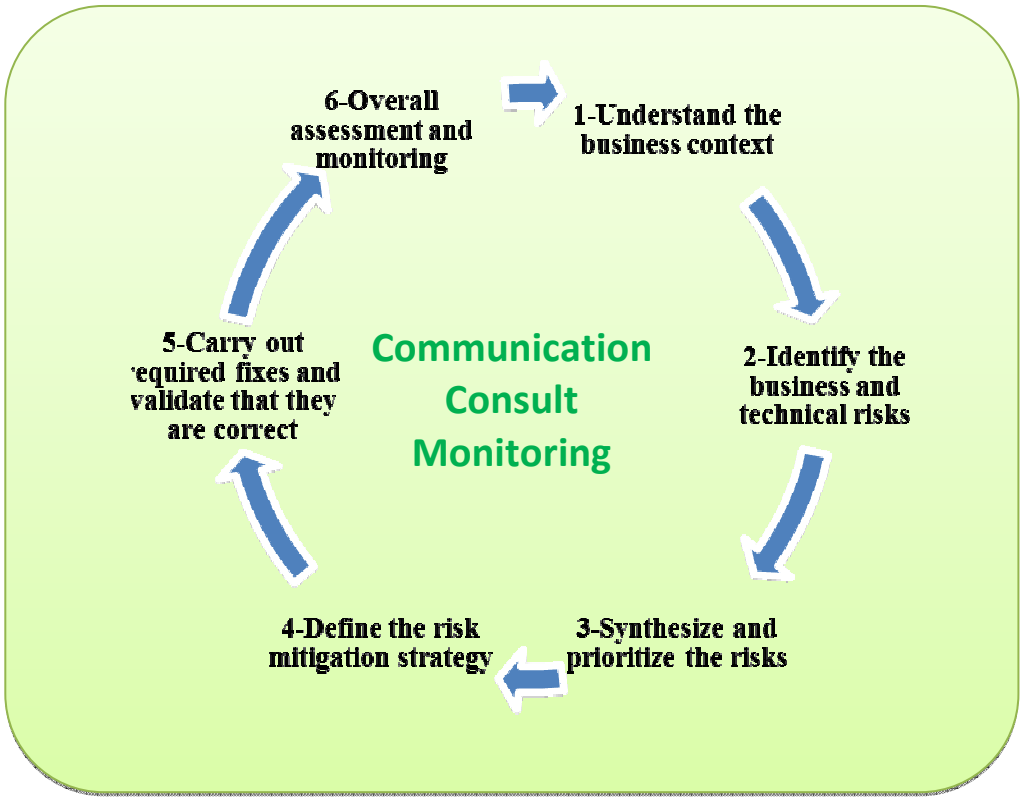


Figure 2. RMF for business and enterprise consists of six fundamental activity stages

Also, in the middle of Figure 2, it states communication and consulting. This implies that we should keep all stakeholders informed of what the risk management documentation states and if it changes, we will need to contact all those stakeholders. This is why outsourcing of monitoring is currently popular in the cloud. Small businesses lack the resources to deal with constantly talking with stack holders while monitoring their systems.

**Risk Management Framework Stages**

The RMF consists of six fundamental activity stages: (1) understand the business context, (2) identify the business technical risk, (3) synthesize and prioritize the risk, (4) define the risk mitigation strategy, (5) carry out required solutions and validate that they are resolved, and (6) overall assessment and monitoring of the system:

***Understand the Business Context***

This includes describing the business's goals, priorities, and circumstances to understand what software risks and which business goals are paramount. Different information, including quantitative and qualitative data, will be gathered. System analysts should develop several questions to interview and survey different people (e.g., manager, IT management, clients, developers, employees). Also, they are encouraged to develop research projects to examine the overall system and reduce it to a reasonably small set of components. Also, choosing relevant critical areas to focus on is necessary, especially if an area needs

immediate attention. NIST's rough guidelines for ranking business goals can be used; Table 2 provides a guideline for ranking goals in a way that effectively meet standards required by federal regulations. This ranking places business goals under three broad heading of high (H), medium (M), and low (L), depending on the extent of its impact on the project, the employees, and the company at large. The goal is ranked high if it is crucial to the existence and continuity of the project. Failure of such goals has the potential to halt the entire project and directly affect the company. Medium-ranked goals are crucial to the existence of the project, and their failure may adversely affect many employees and also impact some higher ranked goals. Failure of a lower ranked goal can affect just a small portion of the company's revenue, and the impact may be felt by just a small portion of the company's employees.

Creating risk management plan's directions, committees, goals, requirements, timeline and scope is required in the beginning. The goal for doing this is to ensure that everyone in the committee is aware of his/her responsibility, role, and time. Also, it would make the efforts spend more effectively and directly.

Table 2. Guidelines for business goals rankings from NIST

| Rank | Definition |
|---|---|
| **High** | These goals are critical to the existence of the project (and possibly the company). If not met, there is a real risk that the project will cease to exist and the company will be directly impacted. |
| **Medium** | These goals are very important for the existence of the project (and possibly the company). A large number of employees may be affected if these goals are not met. A failure to achieve a medium-ranked business goal may result in a negative affect to high-rank goals. |
| **Low** | These goals affect only a small portion of the company's revenue. A small number of employees may be affected itf these goals are not met. |

***Identify the Business, Technical Risks, and Vulnerability***

Business risks can impact business goals. For example, they can affect business reputation, revenue, and productivity. The identification of business risks helps to define and identify the most effective technical and managerial methods for measuring and mitigating these risks. In terms of technical risks, they are hard to find because they are often not actionable. They can be related to a system behaving in an unexpected way, violating its own design structures, or failing to perform as required.

When identifying the business and technical risks, three fundamental sources of threats should be taken into account: natural (e.g., floods, earthquakes, tornadoes); human, including unintentional acts and deliberate actions such as network-based attacks; and environmental threats, such as long-term power failures, pollution, chemicals. Also, these sources can be dividing into adversarial incidents and non-adversarial incidents. Adversarial incidents are these initiated by the adversary such as hackers or cyber-criminal organizations, while non-adversarial incidents occur due to environmental problems such as earthquakes, floods, system faults, or those initiated unintentionally by operators.

In this stage, technical, management, and operational vulnerability should also be investigated. Applying vulnerability sources, the performance of system security testing, and the development of a security checklists can help identify system weak points. After identifying risks and vulnerability, a ranking of risk indicators, impact of risks, and likelihood of identified risks must be created; see Tables 3 and 4. Risk indicators are signs and important tools within operational risk management that can monitor and measure to determine the risk status over time. The level of impact and the likelihood of occurrence would allow the analyst to evaluate the impact of business risk on different business goals, Table 5. In addition, this step involves discovering and describing technical risks and linking them to business goals.

Table 3. NIST risk likelihood description

| **Likelihood Value** | **Definition** |
|---|---|
| **High** | The threat is highly motivated and sufficiently capable, and controls to prevent the risk from occurring are ineffective. |
| **Medium** | The threat is motivated and capable, but controls are in place to impede its successful materialization. |
| **Low** | The threat lacks motivation or capability or controls are in place to prevent, or at least significantly impede, the risk from occurring. |

Table 4. NIST business impact scale

| **Business Impact Value** | **Definition** |
|---|---|
| **High** | 1. Very costly loss of major tangible assets or resources<br>2. Significant violation of, or harm or impediment to, an organization's mission, reputation, or interest<br>3. Human death or serious injury |
| **Medium** | 1. Costly loss of tangible assets or resource<br>2. Violation of, or harm or impediment to, an organization's mission, reputation, or interest<br>3. Human injury |
| **Low** | 1. Loss of some tangible assets or resource<br>2. A noticeable effect on an organization's mission, reputation, or interest |

***Synthesize and Prioritize the Risks***

In any system, a large number of risks always will exist. However, prioritization should be taken place. In this stage, the process must consider the most important business goals and identify which goals are immediately threatened. To understand and manage risks, analysts must establish relationships between the business goals, business risks, and technical risks. It is helpful to draw visual relationships between these three items. It is possible that an individual technical risk may impact multiple business goals at different severity levels. Additionally, analysts are strongly encouraged to prioritize these goals and risks in meaningful business terms, as in Table 5. In the third stage, synthesize and prioritize the risks

by producing a ranked set, analysts can develop the technical risk severity by examining how each technical risk impacts on business goals. To determine the severity level, likelihood of technical risk occurrence and business impacts must be assessed. So, based on all the information gathered so far, management team is able now to create an outline for a risk mitigation strategy.

Table 5. Level of risks

| Quality Values | Semi-Quantitative Value | Description |
|---|---|---|
| **Very High** | **10** | Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organization, or the nation. |
| **High** | **8** | High risk means that a threat event could be expected to have severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organization, or the nation. |
| **Moderate** | **5** | Moderate risk means that a threat event could be expected to have serious adverse effects on organizational operations, organizational assets, individuals, other organization, or the nation. |
| **Low** | **2** | Low risk means that a threat event could be expected to have limited adverse effects on organizational operations, organizational assets, individuals, other organization, or the nation. |
| **Very Low** | **0** | Very low risk means that a threat event could be expected to have negligible adverse effects on organizational operations, organizational assets, individuals, other organization, or the nation. |

### *Define Risk Mitigation Strategy*

A coherent strategy should be created for mitigating the risks in a cost-effective manner. All suggested mitigation strategies must take into consideration cost, implementation time, likelihood of success, completeness. and impact over the entire body of risks. Coherent strategies should be created taking into account their effectiveness. Also, the management team should answer the question, “How can the identified risks be managed?” Different mitigation methods should be proposed to choose the best and the most effective one that make sense economically and is applicable to many risks. The method that provides large risk coverage at low cost should be considered. Also, several issues should be taken into account when selecting mitigation methods such as legislation/regulation, organizational policies, and impact of method implementation on operations. After that, a completed risk analysis report should be ready to present for management team and peer review.

### *Carry Out Required Fixes and Validate Correctness*

This stage involves carrying out validation techniques, which provides confidence that risks have been properly mitigated and that strategy is working. Also, the mitigation strategy should be tested to make sure it is effective. It involves implementing the process and

applying validation techniques. Validation plan and instruments are different from one project to the other based on risks identified and methods chosen to address them.

### *Overall Assessment and Monitoring*

After carrying out the required solution, the teams of experts meet to continually evaluate and assess the outcome of the solution. Based on observations, the team decides whether the risk assessment meets the plan or not and what they should do next in each situation. If the assessment meets the plan, they can document the type of attack/threat and the effective solutions. They can then think of solution vulnerabilities and ways to fix them. Besides, alternative solutions can also be devised to increase readiness should the current solution fail for a similar attack. The experts can also evaluate the performance of the solution to see the effectiveness in meeting the goals of the business partners as well as securing the client confidence.

If the solution failed, the experts can assess why it failed and develop fixes. They can evaluate the extent of damage and come up with effective ways of counteracting any aftermath of attacks. They can also develop effective ways of restoring the confidence of their clients should the attack tamper with their data security or privacy information. This team of experts forms the backbone of cloud computing because their innovative thinking does not only provide robust mechanisms for combating known threats but also provides the platform for developing more effective and dynamic RMF. Since humans are potentially the most dangerous potential threat source, a team of humans performing continuous monitoring and creating combat procedures is indispensable to any reliable risk management framework.

## Conclusion

In recent years, cloud computing has gained much popularity in the IT industry. Cloud computing is a computing resource with deployment and service models that enables users to get computing resources and applications from any location via an Internet connection. The powerful characteristic of cloud computing is that no special devices or software are required for the service. A user only needs the Internet and remote servers to use cloud-computing services.

Cloud computing brings us both opportunities and challenges. Reduced coast, speed of deployment, scalability, less requirements for operating IT functions and other environmental benefits, such as less physical space, are among the advantages cloud computing provides. However, a large number of organizations and users in general do not use or adopt this new technology mainly because of security concerns and low trust. To prevent serious problems occurring with security aspect of cloud computing, we provided a risk management framework that can be applied for this purpose. The main goals are to raise trust between providers and users and to increase the number of users and adopters of cloud computing. To accomplish this, this paper has provided a comprehensive cloud computing risk management framework based on previous work. This risk management framework consists of six stages: (1) understand the business context, (2) identify the business technical risk, (3) synthesize and prioritize the risk, (4) define the risk mitigation strategy, (5) carry out required solutions

and validate that they are resolved, and (6) overall assessing and monitoring of the system is a novel idea for effectively combating threats both from adversarial and non-adversarial sources. The first five steps are the well-known risk management stages, but this research has adopted a more robust approach to each of them. This paper highlights the details of these approaches used in the first five steps as well as the explanation of the sixth step.

To clarify these steps, a scenario explaining a step-by-step approach to applying this risk management framework to a hypothetical cloud computing provider has been outlined. The advantage of this risk management framework lies in its flexibility because it can fit with small and large enterprises. Besides, the "RMF is not specific to security risks; it can be applied in non-software situations" [11].

**References**


[1] Qaisar, S., & Khawaja, K. (2012, January). Cloud Computing: Network/Security Threats and Countermeasures. *Interdisciplinary Journal of Contemporary Research in Business*, *3*(9), 1323.

[2] Han, Y. (2011, December). Cloud Computing: Case Studies and Total Costs of Ownership. *Information Technology and Libraries*, *30*(4), 198-206.

[3] Tan, X., & Ai, B. (2011). The Issues of Cloud Computing Security in High-Speed Railway. *International Conference on Electronic & Mechanical Engineering and Information Technology*. Heilongjiang, China: Harbin.

[4] Lui, W. (2012). Research on Cloud Computing Security Problem and Strategy. *2nd International Conference on Consumer Electronics, Communications and Networks*, 1216-1219.

[5] Jadeja, Y., & Modi, K. (2012). Cloud Computing—Concepts, Architecture and Challenges. *International Conference on Computing, Electronics and Electrical Technologies*, 877-880.

[6] Claycomb, W., & Nicoll, A. (2013). *Insider Threats to Cloud Computing: Directions for New Research Challenges*. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52379

[7] Hutchings, A., Smith, R., & James, L. (2013). Cloud Computing for Small Business: Criminal and Security Threats and Prevention Measures. *Trends & Issues in Crime and Criminal Justice*, no. 456. Retrieved from http://www.aic.gov.au/publications/current%20series/tandi/441-460/tandi456.html

[8] Peerson, S., & Yee, G. (eds.). (2012). *Privacy and Security for Cloud Computing*. London: Springer.

[9] Cloud Security Alliance. (2010, March). *Top Threats to Cloud Computing V1.0*. Retrieved from https://cloudsecurityalliance.org/topthreats/csathreats.v.10.pdf

[10] Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud Computing Implementation, Management, and Security*. Boca Raton, FL: CRC Press.

[11] McGraw, G. (2006). *Software Security: Building Security In*. Upper Saddle River, NJ:Pearson Education, Inc.

[12] Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., & Kanai, A. (2011). Risk Management on the Security Problem in Cloud Computing. *First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering*, 147-152.
[13] Xie, F., Peng, Y., Zhao, W., Chen, D., Wang, X., & Huo, X. (2012). A Risk Management Framework for Cloud Computing. *IEEE 2nd International Conference on Cloud Computing and Intelligent Systems*, *1*, 476-480.
[14] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica., I., & Zaharia, M (2010). A View of Cloud Computing. *Communications of the ACM*, *53*(4), 50-58.
[15] Bento, A., & Bento, R. (2011). Cloud Computing: A New Phase in Information Technology Management. *Journal of Information Technology Management*, *22*(1), 39-46.
[16] Brohi, S., & Bamiah, M. (2011). Challenges and Benefits for Adopting the Paradigm of Cloud Computing. *International Journal of Advanced Engineering Sciences and Technology*, *2*, 286-290.
[17] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi,A. (2011, April). Cloud Computing: The Business Perspective. *Decision Support Systems*, *51*(1), 176-189.
[18] Rimal, BP,. Jukan, A,. Katsaros. D,. & Goeleven Y. (2011, March). Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. *Journal of Grid Computing*, *9*(1), 3-26.
[19] Sadiku, M., Musa, S., & Momoh, O. (2014, February). Cloud Computing: Opportunities and Challenges. *IEEE Potentials*, *33*(1), 34-36.
[20] Stoneburner, G,. Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: NIST.
[21] Wang, H. (2011, January). Cloud Computing-Based IT Solutions for Organizations with Multiregional Branch Offices. *Proceedings of the European Conference on Information Management*, 435.
[22] Wang, X., Wang, B., & Huang, J. (2011). Cloud Computing and Its Key Techniques. *IEEE International Computer Science and Automation Engineering*, *2*, 404-410.
[23] Joint Task Force Transformation Initiative. (2012, September). *Information Security: Guide for Conducting Risk Assessments*. Special Publication 800-30. Gaithersburg, MD: NIST.
[24] Brodkin, J. (2008, July 2). Gartner, Seven Cloud-Computing Risks. *InfoWorld*. Retrieved from collegiatetimes.com/

## Biographies

IBRAHEEM KATEEB is currently at NCA&TSU as an assistant professor in the CST Department. His current research is on power and green energy, electronics and control/ robotics. In the last few years, he has published more than 40 journal and conference papers. Dr. Kateeb was recognized as the recipient of Academic Excellence Award from CARTS

International 2012 (Electronic Components Industry Association, ECIA) for one of his research studies.

MADALLAH SALAH ALMADALLAH is currently a graduate student at University of North Carolina Agriculture &Technology in the Master of Science in Information Technology (MSIT) program. He received his bachelor's degree in Computer Information System (CIS) from Elon University in NC, 2011. He is interested in cloud computing, security, and its management.