Unified Risk List for Electronically Stored Information Subject to eDiscovery in Cloud Computing

Jonathan Vargas-Rodríguez
jvargasrpr@gmail.com
Master in Computer Engineering
Alfredo Cruz-Triana, Ph.D.
Electrical and Computer Engineering and Computer Science Department
alcruz@pupr.edu
Polytechnic University of Puerto Rico

Abstract

Electronic discovery is the process of production of electronically stored information (ESI) for use in legal court or corporate investigations. When eDiscovery is performed over a cloud service, the amount of risks to the process increase. Therefore, the purpose of the project is to define the risks affecting ESI residing in a cloud environment that are subject to eDiscovery. This project also seeks to state which risks have the most impact and which are more likely to occur, and provide recommendations to mitigate these risks. To achieve this, a list of risks was compiled from different sources and the risks related to eDiscovery were selected. The risks were evaluated using a qualitative risk analysis to determine likelihood and impact. Vulnerabilities and control recommendations were established for the compiled risks and conclusions were drawn. Control recommendations provide a perspective on areas that require attention for risk mitigation.

Key Terms — electronic discovery, cloud computing, risk analysis, ESI.

Introduction

Electronic Discovery (E-Discovery or eDis-covery) is the discovery of electronically stored information (ESI) for use in court or corporate investigations. Without electronic discovery, inves-tigators wouldn't be able to obtain sets of data for their investigations. Today, ESI is treated with the same, if not higher, relevance as physical evidence. Due to the volatility of ESI, eDiscovery faces many challenges to this date.

One of these challenges is cloud computing. Cloud computing is the concept of deploying a network of servers such that the "cloud" is a centralized data storage and/or online provider for services or resources. Cloud computing has been used for data storage, virtualization and even software deployments, and has become part of the network solutions employed by businesses worldwide. Still, there is a set of threats to cloud computing which can potentially affect eDiscovery procedures over a cloud.

While eDiscovery over a cloud service presents a challenge, these challenges increase if the cloud doesn't implement any type of control to mitigate the risks associated with the service. Different researchers and organizations have presented their risks assessments on cloud computing, but none have presented the impact of these risks conjoined with the risks of eDiscovery over the cloud.

Definition of Concepts

- *Cloud computing*: centralization of data storage or services over a network connection.
- *Electronically stored information (ESI):* information that has been stored in an electronic/digital medium and is subject to deletion, modification or eDiscovery.

- *Electronic discovery*: also known as eDiscovery, is the process of producing a set of electronically stored information for use in litigation or corporate investigations.
- *Information technology (IT)*: applications of computers to create, store, alter or transmit data in business.
- *Meet and confer*: the process where the requesting party and the producing party of an eDiscovery process meet to establish aspects of the process, such as the format of production.
- *Risk analysis*: the process of determining the impact of effect of threat realization over vulnerabilities in a system or process.
- *Threat*: a person or process capable of inducing damage to a system or ESI.
- *Spoliation*: the act of altering or disposing of ESI relevant to the eDiscovery process.

Supporting Theory

Electronic discovery, or eDiscovery, is the process of producing, upon request, a set of electronically stored information (ESI). The eDiscovery process can be requested for legal court or for corporate investigations. In [1], LexisNexis provides insight in the best practices for performing eDiscovery and the requisites dictated by the Federal Rules of Civil Procedure (FRCP) from the United States. The FRCP has categorized ESI as important as physical data, so eDiscovery is very important for resolutions in court.

When eDiscovery is requested, the parties undergo into a process called the “meet and confer”. In this phase parties agree on what ESI must be produced and the format of the production. Both parties must agree on the process, so the requesting party takes into account the difficulty the producing party may undergo in order to produce the data in the requested format. Also, the producing party must make sure that they will produce a set of data in the format requested by the requesting party. If the producing party produces the data in another format that is not useful to the requesting party, then the court can order the producing party to re-produce the requested data in the correct format.

Electronic Discovery Reference Model

The eDiscovery Reference Model (EDRM) outlines a general process framework for the eDiscovery process. The EDRM is shown in Figure 1. The phases of the reference model are: Information Management, Identification, Preservation & Collection, Processing, Review and Analysis, Production, and Presentation. Each of these phases are described as follows:

- *Information management* includes all policies and procedures established by a company to preserve their data while minimizing risk and cost for an eDiscovery request.
- *Identification* is the process of identifying the ESI possessed and how it relates to the data being requested. Issues such as sensitive data or trade secrets are considered.
- *Preservation* is the process of ensuring that ESI is protected against spoliation and modification during the process of eDiscovery.
- *Collection* is the process of collection all identified ESI for processing.
- *Processing* deals with the determination of which identified data is relevant and which is not relevant to the request.
- *Review* is the process of evaluating the relevant ESI for appropriateness, relevance and other special considerations.
- *Analysis* is the process of determining the meaning of reviewed ESI and its contextual relation to the legal issue. It can include executive summaries.
- *Production* is the process of producing the ESI in the appropriate format agreed during the “meet and confer”.

- *Presentation* deals with the way ESI is presented, which depends on the content and the requesting party.

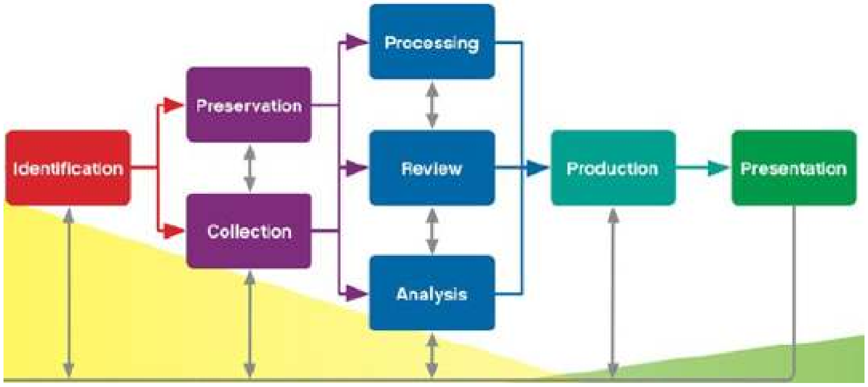

Figure 1: Electronic Discovery Reference Model

Cloud Computing

Cloud computing is an attractive solution today for centralized data storages for businesses. The concept of the cloud, as defined in [2], is used for a centralized service provided by a service provider to a customer organization or business. The cloud has a specific infrastructure that enables sharing of physical service, storage space and networking capabilities with another network. These provided services are provisioned dynamically, which means that they are provided as needed. These services require network access, which can be one disadvantage taking into account the degree of dependability on the cloud services and the availability of a backup internet service provider (ISP).

Cloud computing has different service models. The most used models are software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). The software as a service model provides the customer access to an application or service being hosted. Platform as a service provides a platform that allows the customer to deploy their own applications in the cloud, which can include restrictions because the customer doesn't manage the operating system. Infrastructure as a service gives more control to the customer, allowing them to manage the operating system, applications, storage and network.

Cloud services also possess different deployment models. A private cloud, which can be an in-house cloud or an outsourced cloud, is maintained and operated by the organization due to the privacy requirement. A public cloud is available from a cloud service provider and provided to customers. A community cloud is a type of cloud service that is shared among different companies or organizations that have similar requirements. The community cloud can also be operated in-house of can be outsourced. A hybrid cloud is a combination of both private and public clouds and can be used when a company must use a set of cloud services but also provide some (or other) cloud services. As stated in [3], private clouds can be considered by companies for long-term IT solutions, rather than employing a public cloud as a long-term solution, which is a short-term solution. A visual representation of the deployment models is shown in Figure 2.

Cloud computing has its benefits. By using cloud services an organization can reduce their expenditures of investing in information technology (IT). In this way, the cloud service provider also handles maintenance and is responsible for providing a reliable service and implementing good business continuity and disaster recovery plans. The cloud is designed mostly as a scalable and flexible service, which eliminates another problem for an organization in terms of IT upgrades and/or expansions.

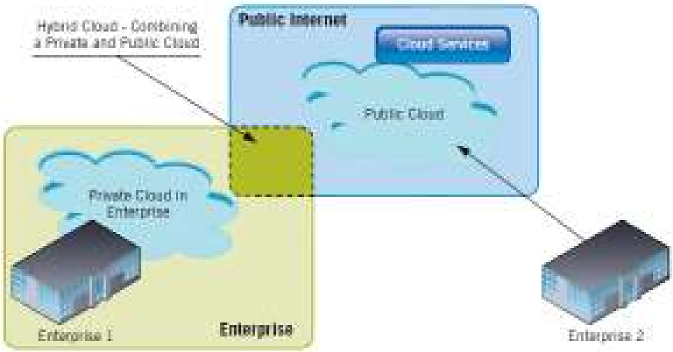

Figure 2: Cloud Service Deployment Models

Cloud computing also has a set of risks and challenges, but businesses have started driving the development of cloud computing for their ends. According to [4], organizations have invested resources in order to improve cloud computing cost structures, increase their productivity, provide fast and flexible cloud platforms and provide security for the cloud service platforms. The "status quo" of cloud computing states that while internet users widely accept and use the cloud, companies still proceed with caution due to the issues of security. In [3], the fourth myth states that all cloud security requirements are created as equals.

This is far from the truth, as private clouds (due to its very definition) will possess of controls to safeguard the privacy of data. Still, the companies caution is well-founded as private clouds and their controls are not perfect barriers against vulnerabilities and the realization of risks into threats. The fifth myth further discusses that there is not one way to do cloud computing; in fact, the cloud models discussed provide options to choose the option that is most relevant to the needed architecture. The third myth states that critical applications don't belong in the cloud, which is a half-truth: due to the "status quo", companies may not prefer to host their critical applications on the cloud due to different reasons, but efficient cloud service providers can still provide efficient availability to these critical applications by employing the correct measures of redundancy.

Risk Assessment

Risk assessment has been defined as the method of identification of vulnerabilities and threats and assessing possible impacts to a system or process and the indication on where to apply controls to mitigate the risk. This type of assessment can be conducted to perform cost-benefit analysis, select controls, determine what assets are at risk, why these assets are at risk and to comply with regulations and legal requirements. There are many different approaches, such as the NIST SP 800-30 approach discussed in [5]. The NIST SP 800-30 is the Risk Management Guide for Information Technology Systems and is the U.S. federal standard for risk analysis in IT.

According to the NIST SP 800-30 publication, the steps are:

- Characterization of the system.
- Identification of threats and vulnerabilities
- Listing of controls.
- Likelihood determination and impact analysis.
- Risk determination.
- Control recommendation and documentation.

When performing the risk analysis, two methods exist: quantitative and qualitative. In a quantitative risk analysis, monetary values are assigned to assets and the loss potential is calculated using the monetary value assigned and the likelihood of occurrence in a 12 month period. Therefore, the quantitative risk analysis is good when determining the cost of a threat and the cost of mitigation controls. The qualitative method is focused on impact, and maps the likelihood of a threat to its degree of consequence. The qualitative analysis doesn't provide monetary values, but is a great option when monetary values are irrelevant. Quantitative analysis can take a large amount of time without tools to perform the analysis, while qualitative analysis is subject to the opinion of the personnel performing the analysis.

Much work has been done around risk assessment and mitigation controls for cloud computing. In [6], risks are categorized as data security risks, logical access risks, network security risks, physical security risks, compliance risks and virtualization risks. The authors provide recommendations on controls to mitigate the risks. Ziluck, in [7], has also provided recommendations to mitigate a series of presented risks, but doesn't address the question of which risks are more likelihood to occur and which are the risks that have the strongest impact. Den Hoed, in [8], performs a qualitative risk assessment over the risks categorized as data location, deletion, leakage and segregation from a technological point of view. Other risks are also discussed in [9] and [10], and they present indispensable sources for risks on cloud computing. Then, these sources become extremely important in the development of a unified risk list for eDiscovery in the cloud.

Methodology

A unified risk list that targets data in cloud computing was compiled from different sources. Initially, a list of general risks to data and cloud computing services was compiled. This general list was compiled from [6] and [9]-[11]. From this list, the risks were analyzed in terms of their impact target. Those that target ESI or its accessibility were selected; the other risks were discarded. The list containing the risks that target ESI make up the "Unified Risk List".

Next, a qualitative risk analysis was performed over the unified risk list obtained. A qualitative risk analysis is subjective to the person performing the analysis, but provides a better measure of impact levels rather than providing monetary costs. The likelihood and impact ratings were obtained from the proposed sample sources for the most part; the risk involving steganography was estimated due to lack of data.

The impact and likelihood were determined subjectively using the proposed risk list over data subject to eDiscovery and residing in a cloud computing environment by assigning scores from statistics and reported impact from various sources. The risk analysis was based on ISO/IEC 27005:2008. Risk levels used based on the ISO standard present low risks with a score of 0 to 2, medium risk with a score of 3 to 5, and high risks with a score of 6 to 8. For likelihood and impact, levels are assigned as very low (0), low (1), medium (2), high (3) and very high (4). The risk score is the sum of the likelihood score and the impact score. The table used to conduct the analysis is shown below in Table 1.

Table 1: ISO/IEC 27005:2008 Risk Analysis Table

		Likelihood				
	Ratings	VL	L	M	H	VH
Impact	VL	0	1	2	3	4
	L	1	2	3	4	5
	M	2	3	4	6	6
	H	3	4	5	5	7
	VH	4	5	6	7	8

Finally, controls were recommended for each of the risks compiled in the. To provide the list of recommendations, the vulnerabilities of each risk were established first. Then, mitigation strategies and controls were provided for these vulnerabilities. The recommendations are not included in this paper. Still, a pie chart was used to show visually the distribution of these recommendations. The graph can help understand recommendations by classification to conclude which areas deserve immediate attention.

Unified Risk List

A list of 34 risks to data and cloud services was compiled. This initial risk list, dubbed the "candidate risk" list, contained risks that had impact to cloud services but not to the eDiscovery process, while others were redundant or modified. The resulting list, dubbed the “Unified Risk List”, contained 26 risks. The risks are defined as follows:

- *Data lock-in*: data lock-in includes the difficulty of migrating data to and from cloud services. The impact of the risk depends on the cloud service model in use.
- *Loss of governance*: this particular risk covers the issue when the customer loses control over their ESI in the cloud service.
- *Cloud service termination/failure*: if a cloud service provider goes out of business suddenly, decides to terminate the service or fails due to disasters, the effect on ESI is expected.
- *Supply chain failure*: if the cloud service provider has outsourced some of their services, the probability of failure to comply with eDiscovery requests increases.
- *Resource exhaustion*: if cloud services resources are exhausted, ESI can remain unavailable and disrupt the eDiscovery process.
- *Segregation failure*: failure to segregate or isolate ESI from one tenant to another tenant is a classic barrier to eDiscovery processes, especially when disclosure of ESI may be subject to penalties under law such as HIPAA.
- *Spoliation*: spoliation occurs when ESI is altered or covered to change the outcome of an eDiscovery process. This specific risk targets single employees acting within their access rights.
- *Cloud provider malicious insider*: an insider is an employee with the objective of obtaining information for the gain of a third-party not related to the customer or the cloud service provider. Insiders may cause spoliation over ESI or disrupt cloud services provided.
- *Management interface compromise*: the cloud services are accessed by an interface. If the interface is compromised, then access to ESI may prove difficult.
- *Interception of data in transit*: data intercepted in transit can be deleted or modified and sent to the cloud storage; this risk is another kind of spoliation.
- *Distributed Denial of Service*: a denial of service attack targeting a system can disrupt the cloud services and impede an eDiscovery process.
- *Loss of encryption keys*: if encryption keys are lost then encrypted ESI can’t be accessed. Encrypted ESI can include, but is not limited to, backups and other data stored in databases.
- *Use of multiple encryption schemes*: the use of multiple encryption schemes becomes a problem during the decryption process. This poses a threat to compliance with eDiscovery when dealing with encrypted ESI.
- *Rogue encryption*: ESI encrypted by employees presents another problem that may result in unrecoverable ESI due to key failure, loss or employees that won’t provide the encryption key.
- *Inefficient decryption procedures*: if policies and procedures for encryption don’t exist, then the decryption of ESI for production in eDiscovery may not comply with the established dates.
- *Steganography*: steganography, or hiding data inside data, may not be detectable by eDiscovery software. ESI covered in the scope of the eDiscovery process may exist, but the existence of such ESI can’t be proven or verified reliably.
- *Compromise of service engine*: the compromise of the cloud service engine affects the cloud service provider’s ability to provide the services to their customers, and can impede eDiscovery.
- *Jurisdiction*: jurisdiction can be a problem during eDiscovery. If the physical storage units of the cloud service are not in the country where the eDiscovery process has started then jurisdiction problems arise.

- *Privilege escalation*: similar in nature to malicious insider, but in this case an employee is the responsible for data spoliation or service disruption.
- *Social engineering attack*: this risk has many different vectors targeting both the cloud service provider and the customer; access to ESI can result in spoliation.
- *Loss of operational logs*: this risk doesn't affect most ESI directly but the loss of operational logs result in the loss of an audit trail; this counts as ESI spoliation.
- *Loss or theft of backups*: loss of ESI stored in backups that may be required for eDiscovery can disrupt the process.
- *Unauthorized physical access*: this risk targets the cloud service provider's facility specifically; this risk can result in service disruption or ESI spoliation.
- *Theft of equipment*: this risk targets the cloud service provider. Theft of equipment can negatively affect eDiscovery due to disappearance of ESI.
- *Natural disasters*: natural disasters can result in heavy losses of infrastructure that can delay or impede eDiscovery.

The aforementioned risk list was organized as a table with risk IDs, such that the ID starts with the letter R and is followed by a unique number. The risk list with IDs is shown in Table 2.

Risk Analysis

The risk list was organized in Table 3, a table similar to the table shown as Table 1. This table includes the risks from Table 2, but the risk IDs are used. The risk IDs with asterisks represent a variation of the same risk. Table 3 was used to determine which risks are the most likely to occur and which risks that produce the most impact to eDiscovery. These results also give insight on which risks must be mitigated first in order to assure compliance in eDiscovery and to provide proper conclusions.

Findings

Originally, such a low number of high probability risks was not expected. However, these results provide a guide on the existing risks and their levels of probability. Since most of the risks fall in medium (M) or lower (L, VL) likelihoods, focusing on the few risks with the highest (VH) likelihood can potentially decrease the amount of high risks from the Unified Risk List. If the initial focus is to decrease the likelihood of the very high (VH) and high (H) likelihood risks, the focus can then change to decrease the likelihood of the medium (M) likelihood risks that may or may not include the previous high (H) or very high (VH) likelihood risks.

Another finding, although expected, is the fact that every risk with a very high (VH) impact rating can affect the ability to acquire ESI permanently. These risks can result in the inability to comply with an eDiscovery request or ESI tampering and can result in penalties with monetary and reputation repercussions. Other risks rated as high (H) can also affect ESI permanently, while others target accessibility.

Table 2: Unified Risk List with IDs

Risk ID	Risk
R1	Data lock-in
R2	Loss of governance
R3	Cloud service termination/failure
R4	Supply chain failure
R5	Resource exhaustion
R6	Segregation failure
R7	Spoliation

R8	Cloud provider malicious insider
R9	Management interface compromise
R10	Interception of data in transit
R11	Distributed Denial of Service
R12	Loss of encryption keys
R13	Use of multiple encryption schemes
R14	Rogue encryption
R15	Inefficient decryption procedures
R16	Steganography
R17	Compromise of service engine
R18	Jurisdiction
R19	Privilege escalation
R20	Social engineering attack
R21	Loss of operational logs
R22	Loss or theft of backups
R23	Unauthorized physical access
R24	Theft of equipment
R25	Natural disasters

Table 3: Risk Analysis over Unified Risk List

		Likelihood				
Impact	Ratings	VL	L	M	H	VH
	VL	🟨	🟨	🟨	🟧	🟧
	L	🟨	🟨	🟧	🟧	🟧
	M	🟨	R2*, R4, R21	🟧	R1	R2*
	H	R23, R24, R25	R5, R11, R12, R19, R22	R10, R20	🟥	R18
	VH	R3	R6*, R13, R16, R17	R6*, R7, R8, R9, R15	R14	🟥

*R2 has likelihood L for SaaS model and VH for IaaS model *R6 has likelihood L for private cloud, M for public cloud

Risks of Highest Impact

The majority of the risks are rated as either high (H) or very high (VH). This outcome isn't surprising considering that the inability to produce ESI for an eDiscovery process can result in serious penalties. Therefore, only the risks rated as very high (VH) are considered for this answer.

The risks that have the highest impact are cloud service termination/failure (R3), segregation failure (R6, in both private and public clouds), spoliation (R7), cloud provider malicious insiders (R8), management interface compromise (R9), use of multiple encryption schemes (R13), rogue encryption (R14), inefficient decryption procedures (R15), steganography (R16) and the compromise of service engine (R17).

Risks of Highest Likelihood

Most of the risks established fall under very low (VL) or low (L) categories. Therefore, the risks with likelihood of high (H) or very high (VH) are the ones considered for this answer. The risks with high (H) or very high (VH) likelihood are data lock-ins (R1), loss of governance under IaaS service models (R2), rogue encryption (R14) and jurisdiction (R18).

Highest Risks

From Table 3, we can establish the issues that pose the highest risk. The highest risks have a rating of 6 to 8 and are covered in the red area of the table. These risks are loss of governance under IaaS service (R2), segregation failure (R6, in public cloud), spoliation (R7), cloud provider malicious insiders (R8), management interface compromise (R9), rogue encryption (R14), inefficient decryption procedures (R15) and jurisdiction (R18).

Controls

The risks shown in Table 2 were tabulated with their corresponding vulnerabilities. Then, controls were recommended to address the vulnerabilities and mitigate the risks.

From the risk list, 24% of risks (6 out of 25) require proper service-level agreements for mitigation. This means that cloud service providers have to step up and become a partner in eDiscovery compliance rather than being at the margin and only taking care of their service provision. The involvement of the cloud service provider should extend to help the company establish a model where they can comply with their eDiscovery responsibilities, and where the cloud service provider knows its responsibilities in helping their customer achieve this end.

Additionally, 28% of risks (7 out of 25) can be mitigated by the design of policies, followed by the cloud service provider, by the customer, or established in the service-level agreements. Some of these policies need to be enforced by using physical security and/or monitoring software. Additionally, there is one risk (4%) that combines both service-level agreements and policy solutions

The other percentage states that 24% (6 out of 25) of risks are reduced by software security, physical security and testing. Another 12% combines security and policies. The rest (8%) includes proper architecture design by the service provider and user training. Table 4 states what risks belong to each control type. Additionally, a pie chart distribution is shown in Figure 3. Figure 3 summarizes the distribution of recommended controls to mitigate the risks stated during the research process.

Table 4: Control Types over Risks

Control	Risks
Service-level agreement (SLA)	R1, R2, R3, R4, R18, R25
Policies	R5, R7, R12, R13, R15, R19, R21
SLA & policies	R8
Security & testing	R9, R10, R11, R17, R23, R24
Policies & security	R14, R16, R22
Architecture design	R6
User training	R20

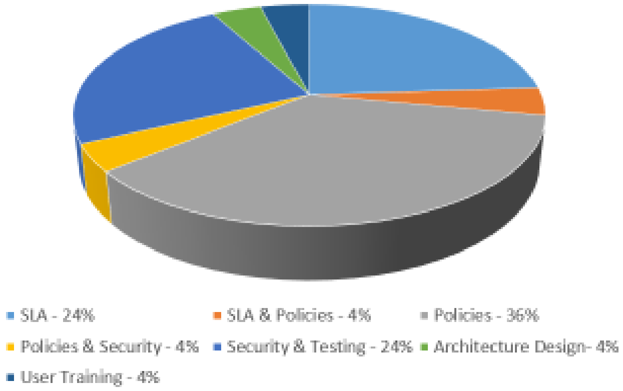

Figure 3: Distribution of Controls for Unified Risk List

Conclusions and Future Work

The mitigation of risks over ESI in cloud service environments requires a strategy that combines the establishment of good service-level agreements, establishment and enforcement of policies that guarantee a secure environment for ESI, user training to follow these policies and avoid becoming a vulnerability of a social engineering attack, and the use of software security and physical security to avoid or deter attacks with periodic testing. The current focus should be over service-level agreements to pressure the cloud service providers to become a partner in eDiscovery compliance rather than a provider and observer.

The establishment of good service-level agreements that addresses common loopholes and unclear roles between the customer and the cloud service provider is only the first step. Policies that promote secure processes and procedures realize the service-level agreements and must be well-thought in order to comply with the service level agreements. These policies should affect the implementation of physical, software and network security and how these configurations are success-fully tested. Furthermore, the policies should affect how users are trained to comply with the policies that realize the service-level agreements and how the cloud service provider has implemented the ser-vice provisioning architecture to assure compliance with eDiscovery processes.

This project has wide potential for improve-ment and development. In improvement, the acqui-sition and use of more statistics to better understand and/or correct likelihood and impact ratings for the qualitative risk analysis. Another area of improve-ment is the inclusion of other risks that may have not been included in the project but have an impact effect on the capability of eDiscovery over ESI stored in a cloud service. This includes previously not-known risks, or the re-evaluation of risks not included. Furthermore, the classification of the risks by type (i.e. technical, legal, procedural, etc.)

This project can also lead to development of an ESI governance model for eDiscovery compliance with cloud service storage. Such a model could be used in the cloud service acquisition process to understand where the risks are and how the service provider and the customer must work together to establish a compliance model. Furthermore, the project can also lead to develop a "checklist" used in the audit process to ensure that the organization has eDiscovery compliance in perspective and works actively to improve their compliance with their cloud service provider.

References

[1] LexisNexis. "Electronic Discovery Best Practices". [Online]. Available: http://www.lexisnexis.com/applieddis covery/lawlibrary/whitePapers/ADI_ImplementEDiscBestPractices.pdf. [Accessed: 09- Mar- 2015].

[2] Dialogic. "Introduction to Cloud Computing". [Online]. Available: http://www.dialogic.com/~/media/products/docs /whitepapers/12023-cloud-computing-wp.pdf. [Accessed: 19- Mar- 2015].

[3] Hewlett-Packard. “Five Myths of Cloud Computing”. [Online]. Available: http://www.hp.com/hpinfo/newsroom/ press_kits/2011/HPDiscover2011/DISCOVER_5_Myths_of_Cloud_Computing.pdf. [Accessed: 19- Mar- 2015].

[4] T-Systems. “Alternative Sourcing Strategy for Business ICT”. [Online]. Available: http://www.t-systems.com/pre page-whitepaper/whitepaper-download/1016440?ts_refBea nId=760948. [Accessed: 19- Mar- 2015].

[5] S. Harris. *CISSP All-in-One Exam Guide*, 6th ed. Berkeley, Calif.: Osborne, 2012, pp. 74-95.

[6] M. Carroll, A. Van der Merwe and P. Kotzé. “Secure Cloud Computing: Benefits, Risks and Controls”, ICSA Department of Computer Science, 2011. [Online]. Available: http://icsa.cs.up.ac.za/issa/2011/Proceedings/Ful l/13_Paper.pdf. [Accessed: 09- Mar- 2015].

[7] A. Ziluck. “Cloud Computing and the Implications for E-Discovery”, American Public University System, 2012. [Online]. Available: http://www.apus.edu/content/dam/onli ne-library/masters-theses/Ziluck-2012.pdf. [Accessed: 11- Mar- 2015].

[8] A. Den Hoed. “Technology Based Methods to Reduce the Risks of Cloud Computing”, Leiden Institute of Advanced Computer Science. [Online]. Available: http://www.liacs.nl /assets/Masterscripties/2012-12AntonDenHoed.pdf. [Accessed: 12- Mar- 2015].

[9] D. Catteddu and G. Hogben. “Cloud Computing: Benefits, Risks and Recommendations for Information Security”, European Network and Information Security Agency, 2009. [Online]. Available: https://www.enisa. europa.eu/activities/risk-management/files/deliverables/clo ud-computing-risk-assessment/at_download/fullReport. [Accessed: 19- Mar- 2015].

[10] W. Jansen and T. Grance. “Guidelines on Security and Privacy in Public Cloud Computing”, National Institute of Standards and Technology, 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf. [Accessed: 19- Mar- 2015].

[11] Symantec. “Enterprise Encryption Trends Survey: Global Results”, 2011. [Online]. Available: https://www4.syma ntec.com/mktginfo/whitepaper/SYM_2011_EncryptionPoll_revC_2011-11-28_cta56524.pdf. [Accessed: 09- Mar- 2015].