Return on Security Investment for Cloud Platforms

Nikolaos Tsalis Marianthi Theoharidou Dimitris Gritzalis

Information Security & Critical Infrastructure Protection Research Laboratory
Dept. of Informatics, Athens University of Economics & Business, Greece
email: {ntsalis, mtheohar, dgrit}@aueb.gr

***Abstract*—Cloud migration is a complex decision because of the multiple parameters that contribute for or against it (e.g. available budget, costs, performance, etc.). One of these parameters is information security and the investment required in order to ensure it. A potential client needs to evaluate various deployment options and Cloud Service Providers (CSP). This paper proposes a set of metrics focused on the assessment of security controls of a cloud deployment, in terms of cost and mitigation. Such an approach can support the client to decide whether she selects to deploy part of her services, data or infrastructure to a CSP, or not.**

Keywords—cloud security; metrics; controls; Return on Investment (ROI); Return On Security Investment (ROSI); cost-benefit analysis.

I. INTRODUCTION

A tenant decides to migrate part of his data, services, or infrastructure to a Cloud Service Provider (CSP) based on several parameters, such as expected benefits, adoption costs, performance, flexibility, business opportunities and others [1], [2], [3]. As in any new IT context, this decision requires a modified approach towards risk [4]. One deciding factor, not clearly depicted in existing literature, is whether the CSP offers security services and if so, the characteristics of these services, which signify both, varied levels of protection and cost. If the tenant anticipates higher probability of security events and/or substantial losses from potential security events, due to the lack of controls, she may not migrate to the cloud [2].

Each migration decision refers to a particular '*deployment profile*', which is defined in the context of this paper to include four elements: *deployed assets*, *cloud type* (i.e. service model [5]), *deployment model* [4] and a specific CSP. Due to the varied level of tenant control of each profile, different security services are required by the CSP. Higher protection on the CSP side is expected to increase deployment fees, while lower protection translates to more controls (and cost) on the tenant's side.

This paper focuses on the security aspect of cloud migration and proposes security metrics which can be used in order to weigh benefits and costs of security for a particular deployment profile. The ultimate goal is to adequately assess whether migration of assets (e.g. data, services, applications, infrastructures, etc.) to the cloud is a beneficial decision or not, both from an economic and security perspective. This means that the tenant needs to evaluate both the level of security offered by the CSP and the cost that such controls introduce. We assume that the CSP is cooperating and reveals the security services offered.

In this paper, we describe the logical process of such a decision (Section II), we define three categories of *cloud security metrics* (Section III), and we apply them on a comprehensive case scenario, described in Section IV. Section V compares our approach to other ones. The paper concludes with a discussion on limitations and future work.

II. MIGRATION DECISION PROCESS

The migration decision has two main inputs: the characteristics of the deployment profile and the required security and privacy controls [6], [7]. The latter can be either offered as a service by the CSP, or they may need to be implemented on the tenant side. Both options introduce migration costs, thus affecting the decision of the tenant.

Essentially, the tenant has to answer to the following question: *'Are the security controls offered adequate and efficient from an economic perspective?''*. The answer to this question may affect the decision to migrate to the cloud and it is usually co-examined with other business parameters [1].

The logical process of the decision follows four steps:

1. *Define deployment profile.* The tenant selects the migrated assets, the cloud type, and the deployment model, coupled with a CSP offering such a service.
2. *Define set of controls*, for the deployment profile. These may be offered by the CSP or implemented by the tenant (due to the cloud migration).
3. *Evaluate benefit and cost metrics*, for the assets of the deployment and for the implemented controls.
4. *Evaluate Return on Security Investment (ROSI)* for each combination of deployment profile-controls.

The last step results in the evaluation of the ROSI of one or more profiles and the tenant deciding whether he will migrate or selecting the CSP, the model, and the type of cloud that is more beneficial.

III. CLOUD SECURITY METRICS

In order to assess ROSI for a deployment profile [6], we identify metrics for the deployed assets and respective controls. *Damage cost* refers to the potential damage inflicted in each deployed asset by a security incident (e.g. loss of availability), while *control metrics* evaluate (i) the level of protection provided, and (ii) the cost of implementing security

978-0-7695-5095-4/13 $31.00 © 2013 IEEE
DOI 10.1109/CloudCom.2013.115

controls on the client side and/or acquiring security services by the CSP.

A. Damage

This metric quantifies the cost of a security incident, regardless of the presence of controls[1]. The metric is assessed based on: (a) the value of the affected asset *i*, i.e. direct losses (service downtime, hardware replacement, etc.) or indirect losses (loss of reputation, non-compliance, etc.) depending on the type of the asset, (b) the cost of recovering the asset *i* to its initial status. Recovery costs may include the man-hours spent for recovering a service, maintenance or service cost for hardware or software, etc. However, in realistic conditions a more complex depiction of recovery costs may be required, as some costs may be dependent or difficult to estimate in advance.

$$\mathrm{dmg_i} = \mathrm{value_i} + \mathrm{cost\_rec_i} \quad (1)$$

This metric is assessed on a per asset basis. In our analysis, we need to consider major security incidents (worst-case scenario) that affect availability, confidentiality or integrity of an asset [8], [9], so as to assess the maximum possible damage that can occur after migrating to a CSP. Cloud introduces both new and traditional threats to a tenant [10], [11], [12]. While performing a full risk assessment for the cloud deployment profile poses challenges [13], the tenant is capable of assessing the potential impact of such events, even if statistics for assessing the likelihood of these threats may be unknown or limited.

Thus, when multiple incidents occur at the same time or we consider incidents that affect all three security attributes, the overall damage to an asset i, is calculated as follows:

$$\mathrm{total\_dmg_i} = \mathrm{value_i} + \sum \mathrm{cost\_rec_i} \quad (2)$$

Note that the *value* of the asset *i* refers to the overall loss of the examined cases/scenarios.

Likewise, if we consider a scenario that affects several deployed assets the damage cost of the scenario is the sum of the damage costs of each affected asset.

B. Control cost

The implementation of a control *j* entails several costs: (a) implementation, (b) installation, (c) maintenance and (d) training. If the control is offered by the CSP it may be given at a flat rate, without been analyzed in detailed costs.

$$\mathrm{cost_j} = \mathrm{cost_{imp_j}} + \mathrm{cost_{inst_j}} + \mathrm{cost_{main_j}} + \mathrm{cost_{train_j}} \quad (3)$$

Each control may protect several deployed assets, so care should be demonstrated so as not to take into account this metric multiple times, when calculating aggregated values.

[1] A similar metric is Single Loss Expectancy (SLE) [14], which refers to the total cost of an incident assuming single occurrence. Herein, we propose a varied form of this metric that includes additional information, such as recovery costs.

C. Control mitigation ratio

A security control may be more effective than an alternative one, in respect to a specific threat scenario. We refer to the expected percentage (ratio) of protection offered by a control *j*, to an asset *i* as '$\mathrm{mitigation_j}$*(i)*'. This can be calculated as the percentage of incidents the control has mitigated in the past [14] or, if such information is not available, as the percentage of threats this control can potentially mitigate

D. Residual Damage

The impact of accepting some of the risks, thus leaving an asset *i* partially unprotected, is calculated as follows:

$$\mathrm{residual\_dmg_i} = \mathrm{dmg_i} * \left(1 - \mathrm{mitigation_j(i)}\right), \quad (4)$$

where *j* is the implemented control.

Note that a control may reduce the damage cost of a scenario either by inducing damages which lower than the value of an asset or by reducing recovery costs.

IV. ROSI METRICS

If we consider the simple case where each control protects only one asset and each asset is protected by one control, the following metric demonstrates the benefit acquired by implementing a control *j* to an asset *i* versus the cost of the control *j*.

$$\mathrm{B: C(j)} = \mathrm{dmg_i} * \mathrm{mitigation_j(i)} \,/ \mathrm{cost_j} \quad (5)$$

If the control *j* provides protection to more deployed assets, the previous formula is modified into the following:

$$\mathrm{Bs: C(j)} = \left.\sum_i \left(\mathrm{dmg_i} * \mathrm{mitigation_j(i)}\right)\right/ \mathrm{cost_j} \quad (6)$$

Note that the mitigation ratio for non-applicable assets equals to 0.

The Return of Security Investment (ROSI) for each pair of deployed asset *i* and control *j* is assessed as:

$$\mathrm{ROSI(i,j)} = \left.\mathrm{dmg_i} * \mathrm{mitigation_j(i)} - \mathrm{cost_j}\right/ \mathrm{cost_j} \quad (7)$$

However, in real scenarios it is highly unlikely that we will encounter the above case. Therefore, Return of Security Investment can be assessed from: (a) the asset perspective, (b) the control perspective and (c) the overall cost perspective of the examined CSP.

A. Asset Return on Security Investment (a-ROSI)

This metric calculates the ROI from a security perspective and on a per asset basis. A deployed asset is protected by one or more available security controls. So, for each scenario examined, e.g. total loss of availability, we have to take into consideration: (a) the maximum, potential damage that can occur to the asset *i*, (b) the mitigation ratio of each ap-

plied control *j* for each applicable asset *i*, and (c) the cost of each control *j*, as described above.

$$\text{aROSI(i)} = \frac{\sum_j\left(\text{dmg}_i * \text{mitigation}_j\text{(i)}\right) - \sum_j \text{cost}_j}{\sum_j \text{cost}_j} \quad (8)$$

B. Control Return on Security Investment (c-ROSI)

Similarly, a control implemented in a cloud deployment provides protection against one or more threats to one or several deployed assets. As a result, we need to calculate: (a) the mitigation ratio of the control *j* for each applicable asset *i*, (b) the overall potential damage of each protected asset *j* and (c) the cost of the control.

$$\text{cROSI(j)} = \frac{\sum_i\left(\text{dmg}_i * \text{mitigation}_j\text{(i)}\right) - \text{cost}_j}{\text{cost}_j} \quad (9)$$

C. Return on Security Investment (ROSI)

The overall ROSI refers to the evaluation of all implemented security controls and all the deployed assets of the particular deployment profile. For each deployed asset *i*, we calculate the overall mitigated damage by each relevant control *j*. The mitigation ratio for non-applicable controls equals to 0.

$$\text{ROSI} = \frac{\sum_i\left(\left(\text{dmg}_i * \sum_j \text{mitigation}_j\text{(i)}\right) - \sum_j \text{cost}_j\right.}{\sum_j \text{cost}_j} \quad (10)$$

The output of the introduced metrics is not a straightforward result, in terms of approving or declining cloud migration. The derived ratios need to be taken into consideration by the tenant according to the various business thresholds he sets. So, the tenant can either accept or reject the planned migration to the cloud, while being able to compare two or more CSPs to find the most appropriate one from a security-/cost perspective.

Furthermore, he can choose not to migrate assets that are too expensive to protect (or have high impact when damaged), or reject security controls because of their cost. In general, it is expected that the client will consider ROSI together with other business parameters, such as the ones described in [1], [2], [3].

V. CASE SCENARIO

Let's consider a case scenario of tenant Alice who considers whether to migrate assets (e.g. data, services, etc.) to a cloud deployment provided by CSP_A. CSP_A provides a *private cloud deployment* for Alice, while the available *offered service* is Infrastructure-as-a-Service (IaaS).

For the case scenario, we adopt the following assumptions:

- The currency used in the example is irrelevant, so we consider the values as plain numbers (e.g. 80).
- We assess damage and costs based on a worst-case scenario basis. In the example that follows we assess the scenario where the infrastructure experiences multiple incidents simultaneously, and as a result total unavailability, integrity and confidentiality are experienced. Other scenarios could include a major data breach or loss of data.

Alice's deployed *assets*, along with their properties, are depicted in Table 1. These include: server (A1), application (A2), network (A3), data (A4), Virtual Machine (VM) (A5).

TABLE 1. DAMAGE COSTS OF DEPLOYED ASSETS

Asset i	value_i	cost_rec_i	dmg_i
A1	60	40	100
A2	80	40	120
A3	50	30	80
A4	100	70	170
A5	80	50	130

CSP_A offers several *controls*, while Alice needs to implement some additional ones to complement them. The controls were selected based on the Cloud Control Matrix (v1.4), by the Cloud Security Alliance [15]. The scenario examines the following controls[2]:

- C1: encryption services (IS-18, IS-19)
- C2: vulnerability/patch management services (IS-20)
- C3: wireless security controls (SA-10),
- C4: data integrity controls (SA-05),
- C5: network security controls (SA-08, SA-09, SA-11, IS-31),
- C6: anti-virus/malicious software (IS-21) and
- C7: application security controls (SA-04).

Note that controls C4 and C6 are implemented by Alice, while the rest by CSP_A. The costs of the above controls are depicted in detail in Table 2.

As mentioned before, each control may protect one or more of the available assets (one-to-many approach). The *mapping* between controls and applicable assets they protect, along with the corresponding *mitigation ratios* are depicted in Table 3. This table indicates which assets are not protected, as well as their ratio of exposure for the particular threat scenario we examine.

As mentioned before, each control may protect one or more of the available assets (one-to-many approach). The *mapping* between controls and applicable assets they protect, along with the corresponding *mitigation ratios* are depicted in Table 3. This table indicates which assets are not protected, as well as their ratio of exposure for the particular threat scenario we examine.

[2] Each control is assigned a code (i.e. C_x), a description and the relevant CCM control ID(s) in parentheses.

TABLE 2. COSTS OF CONTROLS

Control j	$cost\_imp_j$	$cost\_inst_j$	$cost\_main_j$	$cost\_train_j$	$Cost_j$
C1	80	30	20	30	160
C2	60	20	20	10	110
C3	70	50	40	20	180
C4	0	30	20	20	70
C5	60	40	20	20	140
C6	0	30	20	10	60
C7	50	20	10	10	90

TABLE 3. CONTROL MITIGATION RATIO

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
A1	70%	60%	80%	-	70%	50%	60%
A2	50%	70%	-	-	-	80%	90%
A3	60%	-	70%	-	80%	-	-
A4	80%	-	-	50%	-	-	-
A5	60%	80%	-	60%	-	60%	70%

TABLE 4. RESIDUAL DAMAGE PER CONTROL

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
A1	30	40	20	100	30	50	40
A2	60	36	120	120	120	24	12
A3	32	80	24	80	16	80	80
A4	34	170	170	85	170	170	170
A5	52	26	130	52	130	52	39

Since none of these controls provides total mitigation, this means that each control leaves part of the risk of the examined scenario unmitigated. The resulting residual damages that may occur when controls are implemented individually are presented in Table 4.

An asset is protected by multiple controls, but these may mitigate the same threats or incidents. This means that although the sum of mitigation ratio may be more than 100%, the value may not be accurate if the ratio refers to the same incidents. The calculation of the total mitigation ratio may require a more in depth analysis of how various controls may interact towards mitigation. For simplicity reasons, we will assume that the controls mitigate threat independently and with different ways, so the sum operator can be used. For example, while encryption (C1) reduces the damage induced on data (A4) by a security breach in terms of confidentiality, change detection (C4) protects the data from unauthorized modification. The residual damage may refer to the lack of a control to ensure availability.

Table 5 presents the benefit value from applying controls (e.g. C3, C4) for every unit spent in order to apply the control. We observe that for the particular deployment profile, implementing control C3 is not beneficial, while C4 offers 2.32 units of benefit for each unit spent.

TABLE 5. BENEFITS TO COST RATIO FOR CONTROLS C3 & C4

Assets	**B: C for C3**	**B: C for C4**
A1	0.45:1	-
A2	-	-
A3	0.31:1	-
A4	-	1.21:1
A5	-	1.11:1
Total	**0.76:1**	**2.32:1**

In order to decide whether to migrate to the particular CSP based on the needed controls, Alice needs to calculate the following metrics:

a) ROSI of each asset (a-ROSI): It reflects whether it is beneficial to implement all applicable controls for a single asset,

b) ROSI for each control (c-ROSI): It depicts how beneficial is to apply a single control for all assets, and last,

c) Overall ROSI: It shows how beneficial (or not) is the particular set of controls for the defined set of assets.

TABLE 6. ROSI FOR CSP_A

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**aROSI**
A1	-0.56	-0.45	-0.55	-	-0.5	-0.16	-0.33	**-0.47**
A2	-0.62	-0.23	-	-	-	0.6	0.2	**-0.17**
A3	-0.7	-	-0.68	-	-0.54	-	-	**-0.65**
A4	-0.15	-	-	0.21	-	-	-	**-0.04**
A5	-0.51	-0.05	-	0.11	-	0.3	0.01	**-0.12**
cROSI	**1.45**	**1.25**	**-0.24**	**1.32**	**-0.04**	**2.73**	**1.87**	**0.92**

The values of the examined scenario are presented in Table 6. We observe that it is costly to implement multiple controls for individual assets (aROSI results). With the exception of controls C3 and C5, the implementation of the other controls provides collectively more benefit (the protection of the applicable assets) than the induced cost. For the CSP_A profile, there is some ROSI, but the tenant will most likely have to compare the results with other CSP offers. Alice can choose one of the following actions:

- *accept to migrate* to the CSP (based on the deployment profile described)
- *reject to migrate* to the cloud as the overall ROSI is not satisfactory,
- *select another deployment profile* (assets, model, types, controls) or
- *select another CSP* (and the set of controls offered).

Overall, Alice should take into consideration each above mentioned metric, so as to understand and evaluate all the involved aspects of the cloud migration decision. For example, she can reject some of the included security controls or

replace them with other equivalent ones, based on their Benefit to Cost ratio or c-ROSI. Thus, according to this example, she could reject controls C3 and C5 because they do not provide a positive ROSI. Finally, note that any possible tenant should also take into account the saved cost from the controls already deployed by her. For instance, Alice may not require additional costs for already implemented controls on her side.

A. Alternative CSP migration

Let's consider the same deployment profile, as described above, but for a different CSP. CSP_B offers the same set of controls (same mitigation ratio) but for a varied fee, shown in Table 7. The controls implemented by Alice, i.e. C4 and C6 are not depicted, as their cost does not vary.

TABLE 7. CONTROL COST FOR CSP_B

	C1	C2	C3	C5	C7
$\mathbf{Cost_j}$	180	90	200	160	170

The increased cost of the controls offered by the CSP_B is reflected in the resulting lower ROSI of the new deployment profile (where the only parameter changed is the provider and the cost of the offered services). While the decision is straightforward in the particular case, varied CSPs can modify the deployment profile more, offering different controls or even cloud type and model, making the decision process complex.

TABLE 8. ROSI FOR CSP_B

	C1	C2	C3	C4	C5	C6	C7	aROSI
A1	-0.61	-0.33	-0.6	-	-0.56	-0.17	-0.54	**-0.53**
A2	-0.67	-0.07	-	-	-	0.6	-0.23	**-0.26**
A3	-0.73	-	-0.72	-	-0.6	-	-	**-0.69**
A4	-0.24	-	-	0.21	-	-	-	**-0.12**
A5	-0.57	0.16	-	0.11	-	0.3	-0.35	**-0.21**
cROSI	**1.18**	**1.76**	**-0.32**	**1.33**	**-0.16**	**2.73**	**0.85**	**0.73**

VI. RELATED WORK

In the literature, both general security metrics and cloud-specific metrics can be found. Some of the work includes cost-oriented evaluations, in terms of proposing ROI formulas. To the best of our knowledge, none of the existing approaches proposes a set of metrics that focuses on ROI for security controls, applied in Cloud platforms.

There are several standards [16], [17], initiatives (i.e. CSA, NIST, ISACA, ENISA, OWASP, CIS, Microsoft, ISECOM, CISWG, etc.) [18], taxonomies [19], [20], frameworks [21], and models [22], [23] for security metrics. Some propose general metrics for security within an organization [24], [25], while others focus on information assurance and vulnerability [26], [27].

Security is considered as a deciding factor in the form of expected losses [1], [2], [3], based on the security level of each CSP. The need to design new security metrics, taxonomies and models for assessing cloud security has been identified in the literature [28], [29]. Such an approach suggests metrics for the evaluation of the CSP in terms of security [30]. These indicate the security level of the provider, by measuring the budget spent on security, the level of security maturity or quantifiable findings by audits and vulnerability assessments.

Cost is also assessed by a risk-oriented approach [31] that identifies threats and security requirements, and assesses impact in the form of metrics, such as mean failure costs. Two other approaches [32], [33] include ROI metrics in the cloud adoption decision process, but do not include security (ROSI) in their assessments.

A ROI metric is used in a similar sense on [34], but the decision is focused on business intelligence solutions on the cloud and not the adoption process. Approaches close to the proposed one, but not cloud-oriented, are included in [35] and [36]. Both of them describe metrics regarding ROI, but only the former is focused on the security aspect.

None of the above mentioned research covers the need for security-oriented metrics, specifically designed for assessing the controls offered by each CSP. Only a guide proposed from ENISA [14] provides a single metric for the ROSI calculation, but it is limited and suggested not for cloud clients but for CERT.

VII. DISCUSSION

In this paper, we have contributed in the migration decision process of a potential tenant. We focused on the assessment of benefit and cost that arise by migrating to a CSP, with regards to the security controls offered. More specifically, we proposed metrics that can assist a tenant to decide whether it is beneficial to migrate to a particular CSP from a security perspective, for a specific deployment profile. The proposed metrics can contribute towards the selection of a CSP by the tenant or can affect the decision to migrate entirely.

The assessment focuses on security controls offered by available CSPs in terms of both mitigation and cost. It does not assess threat likelihood but it assumes worst-case scenarios and their expected impact. Since it assesses expected mitigated damage by each examined control, it could be used as part of a wider risk assessment process performed by the tenant prior to migration [13], so as to comply with probabilistic approaches. Another limitation is that it does not deal with other parameters that affect the migration decision, such as performance or expected business benefit, but solely on security. However, the metric are comprehensive and could be incorporated in more general models.

Our future steps include the presentation of the above metrics, in a form which is compliant to existing standards and map them to existing information security metrics. We then plan to incorporate them in a risk assessment methodology [13] that would assist the tenant to quantify potential security risks that are introduced when migrating to various CSPs. An evaluation of the model is also required in order to assess how the assumptions of this model can be handled, such as the assessment of mitigation ratios or the lack of accurate information by the CSP. We will also examine how

such metrics can be translated in security requirements in SLAs between the tenant and the CSP [37].

ACKNOWLEDGMENT

This work has been partially funded by the 'SOLO Cloud Gateway' project, which is co-financed by the European Regional Development Fund and national funds, through the Greek Ministry of Education, and is part of the Operational Programmes 'Competitiveness & Entrepreneurship' and 'Regions in Transition'. M. Theoharidou has been supported by the Excellence and Extroversion Programme (Action II) of Athens University of Economics & Business.

REFERENCES

[1] B. Martens and F. Teuteberg, "Decision-making in cloud computing environments: A cost and risk based approach," *Information Systems Frontiers*, vol. 14, no. 4, pp. 871–893, 2012.

[2] M. Kantarcioglu, A. Bensoussan, and S. Hoe, "Impact of security risks on cloud computing adoption," in *Proc. of the 49th Annual Allerton Conf. on Communication, Control, and Computing*, 2011, pp. 670–674.

[3] B. Johnson and Y. Qu, "A holistic model for making cloud migration decision: A consideration of security, architecture and business economics," in *Proc. of the IEEE 10th Int. Symp. on Parallel and Distributed Processing with Applications,* 2012, pp. 435–441.

[4] M. Theoharidou, A. Mylonas, and D. Gritzalis, "A risk assessment method for smartphones," in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, Springer (AICT 267), 2012, pp. 428–440.

[5] P. Mell, T. Grance. (2011, Sept). The NIST Definition of Cloud Computing, *NIST Special Publication 800-145*. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[6] Joint Task Force Transformation Initiative. (2013, Apr). *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 (Revision 4). [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800

[7] D. Gritzalis, "Embedding privacy in IT applications development", *Information Management & Computer Security*, Vol. 12, no. 1, 2004, pp. 8–26.

[8] N. Virvilis, S. Dritsas, and D. Gritzalis, "Secure cloud storage: Available infrastructure and architecture review and evaluation," in *Proc. of the 8th Int. Conf. on Trust, Privacy & Security in Digital Business*, Springer (LNCS 6863), 2011, pp. 74–85.

[9] N. Virvilis, S. Dritsas, and D. Gritzalis, "A cloud provider-agnostic secure storage protocol," in *Proc. of the 5th Int. Workshop on Critical Information Infrastructure Security*, Springer (LNCS 6712), 2010, pp. 104–115.

[10] Cloud Security Alliance. (2013, Feb.). *The notorious nine: Cloud computing top threats in 2013* (v.1.0) [Online]. Available: http://cloudsecurityalliance.org/research/top-threats/

[11] ENISA. (2009, Nov.). *Cloud computing: Benefits, risks and recommendations for information security* [Online]. Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[12] M. Kandias, N. Virvilis, and D. Gritzalis, "The Insider threat in cloud computing," in *Proc. of the 6th Int. Workshop on Critical Infrastructure Security*, Springer, 2011, pp. 95–106.

[13] M. Theoharidou, N. Tsalis, and D. Gritzalis, "In cloud we trust: Risk-Assessment-as-a-Service," in *Proc. of the 7th IFIP Int. Conf. on Trust Management*, Springer (AICT 401), 2013, pp. 100–110.

[14] ENISA. (2012, Dec). *Introduction to Return on Security Investment* [Online]. Available: http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment.

[15] Cloud Security Alliance. (2013, Mar.) *Cloud Controls Matrix* (v.1.4). [Online]. Available: http://cloudsecurityalliance.org/research/ccm/

[16] *Information Technology-Security Techniques - Information Security Management - Measurement*, ISO/IEC Standard 27004, 2009.

[17] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, W. Robinson. (2008, Jul). *Performance Measurement Guide for Information Security*, NIST Special Publication 800-55 (Revision 1). [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/ SP800-55-rev1.pdf.

[18] R. Barabanov, S. Kowalski, and L. Yngstrom, *Information Security Metrics - State of the Art*, Stockholm University, Social Sciences, DSV, Tech. Rep. 11-007, 2011.

[19] R. Savola. "Towards a taxonomy for information security metrics," in *Proc. of the 2007 ACM workshop on Quality of Protection*, 2007, pp. 28–30.

[20] A. Wang, "Information security models and metrics," in *Proc. of the 43rd Annual Southeast Regional Conf.*, Vol. 2, 2005, pp. 178–184.

[21] J. Pironti, "Developing metrics for effective information security governance," *ISACA Journal*, vol. 2, pp. 1–5, 2007.

[22] D. A. Chapin, and S. Akridge, "How Can Security Be Measured," *ISACA Journal*, vol. 2, pp. 43–47, 2005.

[23] V. Kanhere, "Driving Value From Information Security: A Governance Perspective," *ISACA Journal*, vol. 2, 2009.

[24] J. Bayuk, "Security as a theoretical attribute construct," *Computers & Security*, vol. 37, pp. 155–175, Sept. 2013.

[25] Center for Internet Security (2010, Nov.). *CIS Security Metrics* (v1.1). [Online]. Available: https://benchmarks.cisecurity.org/ tools2/ metrics/CIS_Security_Metrics_v1.1.0.pdf.

[26] A. Wang, M. Xia, and F. Zhang, "Metrics for Information Security Vulnerabilities," *Journal of Applied Global Research*, vol. 1, no.1, pp. 48-58, 2008.

[27] R. Savola, "A Novel Security Metrics Taxonomy," in *Proc. of the 7th Annual Information Security South Africa Conf.*, 2008, pp. 379–390.

[28] L. Pavlova. (2011). *Challenges and Best-practices to Use Existing Security Metrics in the Cloud*." [Online]. Available: http://webmail.deeds.informatik.tudarmstadt.de/teaching/courses/SS11/smcc/reports/Challenges_and_Best-practices_to_Use_Existing_Security_Metrics_in_the_Cloud.pdf.

[29] J. Luna, H. Ghani, D. Germanus, and N. Suri, "A Security Metrics Framework for the Cloud," in *Proc. of the 8th International Conference on Security and Cryptography*, 2011, pp. 245–250.

[30] L. Hayden, and K. Stavinoha, "Measuring cloud security," *ISSA Journal*, vol. 11, no. 6, pp. 26–32, June 2013.

[31] L. Rabai, A. Aissa, and A. Mili, "An Economic model of security threats for cloud computing system," in *Proc. of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic,* 2012, pp. 100–105.

[32] ISACA. (2012, Jul.). *Calculating Cloud ROI: From the Customer Perspective*. [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI -From-the-customer -Perspective.aspx.

[33] V. Chang, G. Wills, R. Walters, and W. Currie, "Towards a structured Cloud ROI: The University of Southampton cost-saving and user satisfaction case studies," in *Sustainable ICTs and Management Systems for Green Computing*, IGI Global, 2012, pp.179–200.

[34] M. Mircea, B. Ghilic-Micu, and M. Stoica, "Combining business intelligence with cloud computing to delivery agility in actual economy," *Journal of Economic Computation and Economic Cybernetics Studies*, vol. 45, no. 1, 2011, pp.39–54.

[35] D. Rico, "Practical Metrics and Models for Return on Investment," *TickIT International Journal*, vol. 7,. no. 2, 2005, pp. 10–16.

[36] V. Kanhere. , "Driving Value From Information Security," *ISACA Journal*, vol. 2, 2009.

[37] V. Emeakaroha, I. Brandic, M. Maurer, S. Dustdar, "Low level Metrics to High level SLAs - LoM2HiS framework: Bridging the gap between monitored metrics and SLA parameters in cloud environments," *2012 Int. Conf. on High Performance Computing and Simulation*, 2010, pp.48–54.