A New Methodology for Security Evaluation in Cloud Computing

Sasko Ristov
Ss. Cyril and Methodius University
Faculty of Information Sciences
and Computer Engineering
Skopje, Macedonia
Email: sashko.ristov@finki.ukim.mk

Marjan Gusev
Ss. Cyril and Methodius University
Faculty of Information Sciences
and Computer Engineering
Skopje, Macedonia
Email: marjan.gushev@finki.ukim.mk

Magdalena Kostoska
Ss. Cyril and Methodius University
Faculty of Information Sciences
and Computer Engineering
Skopje, Macedonia
Email: magdalena.kostoska@finki.ukim.mk

***Abstract*—Cloud service providers (CSPs) and cloud customers (CCs) are not only exposed to existing security risks but to new risks introduced by clouds, like multi-tenancy, virtualization and data outsourcing. Several international and industrial standards target information security and their conformity with cloud computing security challenges. We give an overview of these standards and evaluate their completeness. As a result we propose a new extension to the ISO 27001:2005 standard including a new control objective about virtualization applicable for cloud systems. We also define a new quantitative metric and evaluate the importance of existing ISO 27001:2005 control objectives if customer services are hosted on-premise or in cloud. Our conclusion is that obtaining the ISO 27001:2005 certificate is not enough for CSP and CC information security systems, especially in business continuity detriment that cloud computing produces and propose new solutions that mitigate the risks.**

***Index Terms*—Information Security Management, Security Assessment, Security Standards, Virtualization**

I. Introduction

Cloud concept offers on-demand services, scalability, redundancy and elasticity compared to traditional on-premise computing. Furthermore, the concept of cloud offers several business continuity benefits: eliminating downtime, better network and information security management, disaster recovery with both backup management and geographical redundancy [1]. It also avoids or eliminates disruption of operations, increases service availability and mitigates DoS attack possibility.

Despite the benefits cloud produces several open issues. Interoperability among different vendor clouds and services is maybe essential. Information systems must be redesigned to exploit cloud advantages. In this effort all relevant data and applications are moving outside of company security perimeter and the security is probably the most important issue.

Business managers know that risks exist in spite of all the benefits each new technology or business model offers. A lot of regulatory violation, security, trust and privacy issues appear in clouds. Each company that moves into the cloud should evaluate the risks in comparison to the traditional solutions. A comprehensive analysis for business information system security in cloud computing is given in [2].

Security and privacy assessments are considered as best practice for evaluating a system or application for potential risks and exposures [3]. Traditional security assessments for on-premise infrastructure and applications, as well as compliance audits are well defined and supported by multiple standards. However, additional challenges arise when different tools are used to audit cloud environments [4].

The paper is organized as follow. In Section II we overview the security standards, guidance and best practices. We continue the analysis in cloud security standardization in Section III and the evaluation of ISO 27001:2005 completeness towards cloud security in Section IV. Section V presents several security challenges that ISO 27001:2005 does not cover. A lot of security risks that cloud arises are presented in Section VI along with new proposals how to mitigate them.

II. Background

Many international standards, guidance, and best practices cover security issues. We overview their domain and comment their conformity to cloud computing security challenges.

A. NIST's 800-53 R3 Security Controls

The NIST's special publication 800-53 R3 [5] refers to Security Controls for Federal Information Systems and Organizations as another security control based guidance. It provides guidelines for selecting and specifying security controls for information systems (ISs) supporting the executive agencies of the federal government to meet the requirements of FIPS 200 [6]. The guidance defines total of 205 controls grouped in 17 families of security controls for an information system and one family of program management controls to manage information security programs.

The standard focuses on managing risks aroused from information systems with risk management at the organizational level incorporated in NIST's Special Publication 800-39 [7].

B. ISO 27000 Standard series

ISO 27000 is series of standards specifically reserved for information security matters.

ISO 27001:2005 [8] certification for information security management system (ISMS) can be considered as best solution for securing information assets and also to establish customer's trust in CSP's services. Microsoft proves that information security is central to its cloud operations [9]. The standard

adopts the ”Plan-Do-Check-Act” model applied to structure all ISMS processes. The model ensures that ISMS is established, implemented, assessed, measured where applicable, and continually improved. The standard defines 133 controls grouped into 39 control objectives and 11 clauses. These controls shall be selected as part of the process to establish ISMS suitable to cover the identified requirements. They are not exhaustive and additional control objectives or controls may also be selected, or some can be excluded, but the prospective candidate must justify the exclusion.

ISO 27002:2005 [10] is complementary to ISO 27001:2005. It is a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

ISO 27005:2011 [11] provides guidelines for Information Security Risk Management (ISRM) in organization supporting the requirements of ISMS. ISRM process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review.

C. Audit and Assessment Standards and Guidance

A company must perform internal and external audits prior certification to obtain ISO 27001:2005 Certificate. There are several guidance and certifications for this purpose.

COBIT 4.1. Control Objectives for Information and Related Technology (COBIT) [12] developed by Information Systems Audit and Control Association (ISACA) provides a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. The structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment. COBIT version 5 is in preparation.

SAS 70 (Audit) Type II. SAS 70 [13], developed by American Institute of Certified Public Accountants (AICPA), does not specify a pre-determined set of control objectives or control activities that CSP must achieve, but it provides guidance to enable an independent auditor to issue an opinion on a CSP's description of controls through a Service Auditor's Report. SAS70 Type II certifies that CSP had an in-depth audit of its controls (including control objectives and control activities), which should relate to operational performance and security to safeguard CCs data. This helps the CSP to build trust with its CCs. CCs, on the other hand, with the Service Auditor Report from their CSP(s), obtain valuable information regarding the CSP(s) controls and the effectiveness of those controls. The standard SAS70 is now divided into parts and replaced by two new standards: (1) SSAE No. 16 for Service Auditors and (2) Clarified Auditing Standard for User Organizations. We have analyzed SAS 70 since many CSPs have SAS 70 compliance.

There are other security standards that cover specific areas. HIPAA [14] addresses the security and privacy of health data and intends to improve the efficiency and effectiveness of the health care system by encouraging the widespread use of electronic data interchange. PCI DSS V2.0 [15] is developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. At high level it has 12 requirements to protect cardholder data, which may be enhanced with additional controls and practices to further mitigate risks at acceptable level.

III. Cloud Security Efforts on Standardization

Although general security standards can help CSPs in implementing information security system, there is a need for more efforts for cloud security standardization. CSA identified top threats to cloud computing in [16]. In order to mitigate the risks of threats ENISA identified and assessed the risk level as a function of the business impact and likelihood of the incident scenario [17].

NIST discusses the threats, technology risks, and safeguards for public cloud environments and provides the insight needed to make informed IT decisions on their treatment [18]. The main emphasis is set on security and data privacy.

The CSA's initial report V2.1 [19] contains a different sort of taxonomy based on 15 different security domains and the processes that need to be followed in an overall cloud deployment. New candidate domains are proposed for version 3 [4] and are of the greatest interest to experienced industry consumers and security professionals. Core functionalities, optional features, services, addressed threats, and the challenges to be focused on are addressed for each candidate domain.

CSA puts a lot of efforts in its CSA GRC project [20]. A list of 98 controls grouped into 11 groups is defined in [21]. Each control is mapped into compliant control of other security standards or best practices.

A. Is any general security standard appropriate for Cloud Security Challenges?

The best solution for CSP's information security system is to cover and meet both the ISO standard and NIST guidance controls. But, it is not so simple. NIST's 800-53 [5] shows that a small number of controls are not covered in the other standard. Also, neither NIST's 800-53 security control subsumes ISO 27001:2005, nor opposite. There are many security controls with similar functional meaning, but with different functionality. Other security controls with similar topics are addressed in the same control objective (ISO) or family (NIST), but has different context, perspective, or scope. Another problem is that some controls from one standard are spread in several controls in the other standard.

The standards differ in their purpose and applicability, as well. While ISO 27001:2005 is general purpose and applies to all types of organizations, NIST's 800-53 is applicable for information systems supporting the executive agencies of the federal government.

The main concern here is: are the controls of both standards applicable to CSP and all cloud service layers? Do they cover all the traditional security challenges, as well as newly opened security issues in cloud? Are there any security challenges in cloud computing not covered with these controls?

CSP	Security Compliance
Amazon	PCI DSS Level 1, ISO 27001, SAS 70 Type II, HIPAA
Salesforce	ISO 27001, SysTrust, SAS 70 Type II
Microsoft	PCI DSS, HIPAA, SOX, ISO 27001, SAS 70 TYPE 1 and II
Google	SAS 70 Type II, FISMA
IBM	ISO 27001

TABLE I
EXISTING CSPS' SECURITY CERTIFICATION AND ACCREDITATION

#	Description
-1	Transfered partially to SLA and remain as Control Objective
0	Same importance
+1	Control Objective with increased importance

TABLE II
CONTROL OBJECTIVE IMPORTANCE METRICS

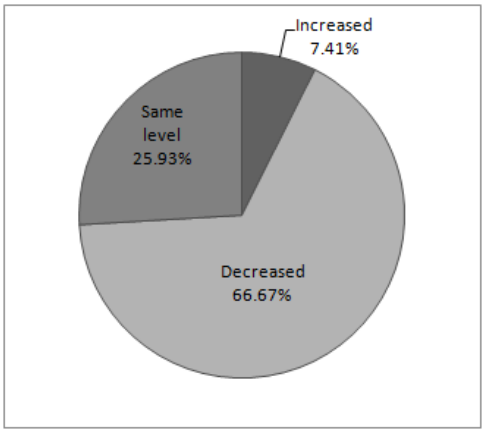

Fig. 1. Control objective comparison: On-premises computing versus cloud.

ISO 27001:2005 is a general purpose standard and therefore, its control objectives are conformable to CSP. But the question remains: Are they enough for CSP's ISMS? Our further research is going into two directions: first, we measure the CC efforts to be taken for each ISO 27001:2005 control objective if their services are hosted on-premise or in the cloud. And second, we analyze if there should be any other security control to be included in the ISO 27001:2005 controls.

B. CSPs' Efforts towards Security

Table I presents the evaluation of the security standards certification existing CSPs have. Most of CSPs are ISO 27001:2005 certified and in addition have one or more security certificates or compliances for their infrastructure.

In the next Section we evaluate ISO 27001 compatibility to cloud security challenges due to standard's generality and the fact that almost all main CSPs are ISO 27001:2005 Certified.

IV. ISO 27001:2005: ON-PREMISE VS CLOUD

In this Section we propose a model to measure the ISO 27001:2005 control objectives importance for both on-premise and cloud solutions. We assess and assign a quantitative metric for each control objective importance. With the qualitative and quantitative analysis we compare the applicability and importance of ISO 27001:2005 control objectives as a general purpose standard, and the fact that the cloud techniques subsume the on-premise ones.

As the CSP becomes an external party that CC relies, CC must transfer some security issues to CSP, but also to increase the domain in SLAs. We define three possible values for the importance of each control objective in ISO 27001:2005, both for on-premise and in the cloud. Table II shows the explanation of each importance. We omit particular control objectives that has no effect if the services are hosted on-premise or in the cloud, i.e. operational or management control objectives.

A. Evaluation of Control Objectives Importance

Comparison of the differences among cloud computing versus traditional on-premises computing can be carried through deducing which resources or services are executed by CC or CSP. Such comparison is given in [22]. The responsibilities for all parts of the IT services hosted on-premises are on the resource owner, i.e. the customer. Going from IaaS, through Paas to SaaS cloud service layer, more and more responsibilities are transferred from the CC to the CSP.

We evaluate each control objective importance on-premise and in cloud using the comparison and metric definitions in Table II. According to control classification in [5] for control objectives, management and operational control objectives do not depend if the company services are hosted on-premise or in cloud. For example, the company must define security policy, no matter of information systems' size and type.

B. Analysis of Control Objectives Importance

The results of the evaluation are presented in Table III. 18 control objectives depreciate their importance, 2 control objectives increase the importance and 7 control objectives retain the importance. We must emphasize that importance depreciation does not mean that a given control objective meaning is decreased or even irrelevant or that particular control objective should be excluded, but the control objective obligations are somehow be transferred to the CSP, and should be integrated (partially or all controls of a given control objective) into SLA agreement signed between CSP and CC. During the processes of establishing or reviewing ISMS and its improvement, the prospective CC can use this evaluation to select / exclude the controls and control objectives to cover the identified requirements, and to put more effort to control objectives with higher importance.

Fig. 1 presents the percentages of control objectives that increase, decrease or retain the level of importance in cloud solution compared to on-premise. We conclude that $2/3$ of control objectives are with depreciated importance in cloud and only 7.41% increased the importance when moving into the cloud. Also, the number of control objectives with depreciated importance is 9 times greater than the one with increased importance.

Control Objective	Value
External parties	+1
Third party service delivery management	+1
Responsibility for assets	-1
Information classification	-1
Secure areas	-1
Equipment security	-1
System planning and acceptance	-1
Protection against malicious and mobile code	-1
Back-up	-1
Network security management	-1
Media handling	-1
Electronic commerce services	-1
Monitoring	-1
User access management	-1
Network access control	-1
Mobile computing and teleworking	-1
Security of system files	-1
Technical Vulnerability Management	-1
Reporting information security events and weaknesses	-1
Compliance with sec. policies and standards, and tech. compl.	-1
Operating system access control	0
Application and information access control	0
Cryptographic controls	0
Management of information sec. incidents and improvements	0
Information security aspects of business continuity management	0
Compliance with legal requirements	0
Security in development and support processes	0

TABLE III
EVALUATION OF ISO 27001:2005 CONTROL OBJECTIVES

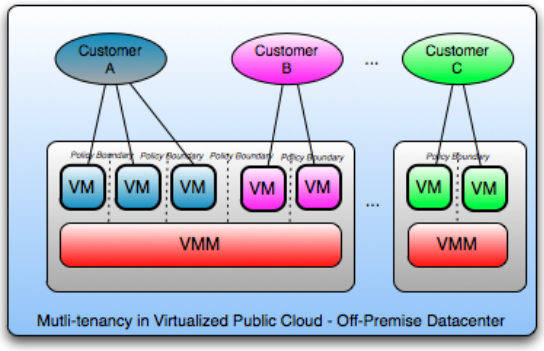

Fig. 2. Virtualized Multi-tenant Environment in IaaS and PaaS [19]

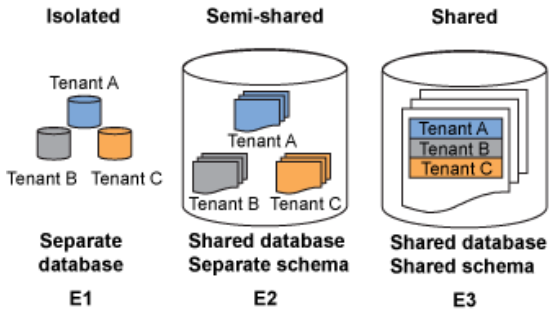

Fig. 3. Virtualized Multi-tenant Environment in SaaS [26]

V. ISO 27001:2005 (IN)COMPLIANCE FOR CLOUD COMPUTING

In this Chapter we analyze the ISO 27001:2005 requirements' conformity to cloud computing security challenges, particularly the new one, such as customer isolation, insider attacks, and security integration [23], due to cloud computing multi-tenancy, virtualization, and outsourcing the CCs' data and applications. We evaluated that almost all main CSPs are ISO 27001:2005 certified. Due to new security challenges we analyze if CSP' ISO 27001:2005 Certificate will be enough to generate trust for CCs that are secured in the rented infrastructure, platform or software.

A. Security Challenges due to Virtualization

Traditional on-premise data-centers security solutions do not comply with virtualized environment, because of the complex and ever-dynamic nature of cloud computing [24]. The virtualization by itself does not affect the security if it is used on-premise in a physical, logical and environmental isolated secured environment. IDS and IPS systems can secure the internal virtual and physical machines from the exterior environment, if they are into one autonomous system, that is, under same administrative governance. Figure 2 depicts multitenant environment where cross VM attacks is possible.

In cloud computing, especially in IaaS and PaaS, the resources are shared and rented to the different customers. Even more, the same physical machine can be shared to many different customers. The current virtualization is weak and can be easily attacked [25]. The security solutions for some flaws are found, but new security threats and vulnerabilities arise day by day. Thus, CSPs' security perimeter is broken from inside, making their IDS and IPS helpless. Therefore, CSPs must introduce effective isolation among the CCs, although allowing physical resource sharing.

Multitenancy exists In SaaS cloud service layer, as well. There are three degrees of data isolation for SaaS applications presented in Figure 3. In Isolated environment each tenant has its own database. Tenants in Semi-shared environment share the database using a separate schema and in Shared environment share both the database and the schema.

We found several security solutions for virtualization challenges. Hao F. et al [27] propose SEC2 solution which enables users to customize their security policy settings the same way they control their on-premise network. Ibrahim A. et al [28] propose Virtualization-Aware Security Solution CloudSec, which monitors volatile memory to detect and prevent for the kernel data rootkits.

Analyzing ISO 27001:2005 requirements and their controls we concluded that there is no control for virtualization. Clause 11 that covers access control and also many standard controls, even the whole control objective, assume that operating systems are on separate real machines. But in the reality, issues such as trusting the VM image, hardening hosts, and securing inter-host communication are critical areas in IaaS [29]. Therefore, we propose to include a new control objective for *virtualization management*, with two controls: *virtualization* and *virtual machines control*. For the former we propose: *Information involved in virtual machines shall*

be appropriately protected and for the latter: *Virtual machines shall be adequately managed and controlled, in order to be protected from internal and external threats, and to maintain information security in transit*. In addition to this, NIST defines the control SC-30 *Virtualization Techniques* in [5], which is not mapped to any control of ISO 27001:2005. NIST's control is far from enough to cover all security flaws due to multi-tenant virtualization in cloud computing.

B. Security, Data Protection and Privacy as-a-Service

Business does not fully accept cloud infrastructure, platform and software due to security, data protection and privacy, as well as trust issues. Combining the advantages of secured cloud storage and software watermarking through data coloring and trust negotiation, the authors in [30] propose reputation system to protect data-center access at a coarse-grained level and secure data access at a fine-grained file level.

Such systems and solutions supersede and subsume the traditional security systems, and thus CSPs should implement them. Therefore, offering *Security-as-a-Service* (SECaaS) and *Data protection and privacy-as-a-Service* will speed up cloud market growth, both for the providers' offers and clients, as well as cloud trustworthiness. CSA offers 10 candidate domains for SECaaS [4].

Data privacy is treated in two controls in ISO 27001:2005 requirements. The control 6.2.3 requires the client data privacy (CCs) and the control 15.1.4 requires from the CSP to ensure data privacy. These two controls obligate both the CCs and the CSPs to manage the data privacy with higher importance.

As shown in Table I, many CSPs are not only complained to some security standards, but they offer services to CCs to help them in their security standard compliance, as well. Thus, the risks that arise from multi-tenancy and virtualization will be mitigated, and mutual trustworthiness will be established among CSPs, CCs and end users.

VI. Security Risks in the Cloud

Cloud computing produces many open security issues to be assessed. Migrating company services into cloud moves their data and applications outside of the company security perimeter. This outsourcing opens new security issues and amplifies existing, thus increasing the company's security overall risk. Multi-tenancy, supported by virtualization, is another important security flaw producing new threats and vulnerabilities from inside, the co-tenants. The current isolation facility within clouds i.e. virtualization is weak and can be easily attacked [25]. The problem is even worse in the case of tenants are hosted on the same physical hardware. Thus, CSPs and CCs must ensure the customer data and applications are "really" secured and the risks are mitigated to the customer's acceptable level.

Business continuity and Disaster recovery are only one domain of all the domains for CSA's SECaaS [4]. In this section we analyze the security detriments cloud computing offers and are aware that some benefits will also produce detriments. We overview some of the main risks that impact the business continuity together with some solutions that mitigates the risks to acceptable level.

1) Multi-tenant environment: Although the cloud can offer better protection and defense for the same cost than traditional solutions it has a detriment as well. Different cloud tenants are serious potential threat in shared and multi-tenant environment and especially in the public clouds. This is not the case in the traditional in-house solution even if virtualization techniques are used. Each CSP should develop a methodology to evaluate the tenants and categorize them into categories with trustfulness purposes. This is especially important for IaaS and PaaS where a client can impact more to its own security, but also is threat to other tenants.

2) Heterogeneity, Complexity, Interoperability: Business continuity depends not only on the effectiveness and correctness of system components, but also on the interactions among them. Subsystem component heterogeneity leads to difficult interoperability. Number of possible interactions between components increases the system failure probability. Complexity typically relates inversely to security, with greater complexity giving rise to vulnerabilities [18]. Defining security standards for adapters, wrappers, transducers, and data transformation, as well as performance analysis can offer stable system solution and mitigate the risks.

3) Regulatory and Standards Compliance: A CSP must provide an evidence that meets the standards and regulatory a company needs. Each CSP should permit the regular audits by the CCs. A CC should assess the risks and include them into risk acceptance plan if acceptable. If not, the services with unacceptable risks should stay in-house. ISO 27001:2005 covers these issues well in several controls.

4) Loss of Control: A company must transfer some control of the assets, application, etc. to the CSP. CCs must assure that their CSP can meet SLA requirements, and if not, they must assess the risks and include them into BCP. Also, we suggest to CSPs regulatory to obligate CCs to concern about security in SLA agreement.

5) Disaster Recovery - RPO and RTO: Although the cloud can offer better RPOs and RTOs [1] we assume that maybe CSP had not defined these objectives or if defined they are worse than CCs would expect. The CCs must be ensured that CSP's RPOs and RTOs are defined in compliance with its own, as well as the CSP can satisfy such defined requirements.

6) Performance challenges: All cloud computing security solutions and techniques degrade cloud services' performance. Implementing identity and access management, web and email security, intrusion management, [4], as well as monitoring systems, data coloring, and other traditional security services, such as web service security produce data overhead and system latency. They must be considered due to their negative impact to server performance and thereby to the system availability.

7) Data Protection, Privacy and Location: Although replication produces security benefits in Disaster Recovery and system availability, it produces a security detriment. Thus, along with virtualization, it complicates the access control management and data privacy. Outsourcing only noncritical

applications and its data to cloud, if applicable, shall provide the client company with even better data protection and management compared to traditional solutions.

CSPs must ensure CCs into their operations and privacy assurance. Privacy-protection mechanisms must be embedded in all security solutions [29]. This risk directly impacts the regulatory compliance risk and company business reputation. Auditing and logging tenant's activities can reduce the risk of incidents, as well as including obligations in the SLA agreements. ISO 27001:2005 defines controls for audit and logging, but CSP must also include new controls we propose.

In some cases the applications and data might be stored in countries where their judiciary concern and lead to regulatory incompliance. Keeping them in-house or in a hybrid cloud with the appropriate SLA can mitigate the risk.

VII. Conclusion

Security challenges remain the main barrier to migrate the services and applications into the cloud. Introducing the trustworthiness among CSPs and CCs is essential. This paper concludes that the existing general purpose security standards, such as ISO 27001:2005, do not cover all cloud security challenges. We propose a new ISO 27001:2005 control objective, *virtualization management*, with two controls covering *virtualization* and *virtual machines control*.

In this paper we define a methodology to quantify the ISO 27001:2005 Requirements grouped in control objectives, comparing on-premise and cloud environments. The evaluation and analysis of ISO 27001:2005 standard result in the importance transfer from CC to CSP. Simultaneously CC must provide a huge effort to implement all control objectives with decreased importance in SLA with its CSP.

No paper so far has presented business continuity aspects in details about cloud computing and it challenged us to address the cloud computing model security detriments that depreciate the CC business continuity: performance and availability, data privacy, protection and location, regulatory and standards compliance, loss of control, heterogeneity, complexity, and interoperability, multi-tenant environment, and disaster recovery - RPO and RTO compliance and effectiveness. In this paper we introduce proposals to mitigate the probability of incident scenario for each detriment. These main risks can be assessed appropriately and mitigated to the acceptable level by applying recommendations in these proposals according to matrix for risk level as a function of the business impact and probability of incident scenario [11].

References

[1] S. Ristov, M. Gusev, M. Kostoska, and K. Kiroski, "Business continuity challenges in cloud computing," in *ICT Innovations 2011, Web Proceedings, Skopje, Macedonia*, 2011.

[2] S. Ristov, M. Gusev, and M. Kostoska, "Cloud computing security in business information systems," 2012, to be published in International Journal of Network Security & Its Applications (IJNSA).

[3] B. S. Kaliski, JR. and W. Pauley, "Toward risk assessment as a service in cloud environments," in *Proc. of the 2nd conf. HotCloud'10*. USENIX Ass., USA, 2010, pp. 13–13.

[4] (2011, Sep.) CSA security as a service v1.0. [Online]. Available: https://cloudsecurityalliance.org/research/working-groups/secaas/

[5] (2011, Sep.) NIST SP800-53 revision 3. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[6] (2011, Sep.) FIPS 200 minimum security requirements for federal information and information systems. [Online]. Available: http://csrc.nist.gov/publications/PubsFIPS.html

[7] (2011, Sep.) NIST SP800-39 managing information security risk. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[8] ISO/IEC 27001:2005, Information Security Management Systems - Requirements. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[9] (2010) Microsoft information security management system for microsoft cloud infrastructure. [Online]. Available: http://www.globalfoundationservices.com/security/documents/InformationSecurityMangSysfor/MSCloudInfrastructure.pdf

[10] (2011, Sep.) ISO/IEC 27002:2005, Code of Practice for Information Security Management. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[11] ISO/IEC 27005:2011, Information Security Risk Management. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56742

[12] (2011, Sep.) ISACA cobit 4.1. [Online]. Available: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[13] (2011, Sep.) AICPA SSAE 16. [Online]. Available: http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx

[14] (2011, Sep.) HIPAA. [Online]. Available: https://www.cms.gov/HIPAAGenInfo/

[15] (2011, Sep.) PCI DSS v2.0. [Online]. Available: https://www.pcisecuritystandards.org/security_standards/

[16] (2011, Sep.) CSA top threats to cloud computing. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[17] D. Catteddu and G. Hogben. (2009) Cloud computing risk assessment. [Online]. Available: http://www.enisa.europa.eu/publications/position-papers/position-papers-at-enisa/act/rm/files/deliverables/cloud-computing-risk-assessment

[18] (2011, Sep.) NIST SP800-144 draft guidelines on security and privacy in public cloud computing. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[19] (2011, Sep.) CSA security guidance for critical areas of focus in cloud computing v2.1. [Online]. Available: https://cloudsecurityalliance.org/research/initiatives/security-guidance/

[20] (2011, Sep.) Cloud security alliance group CSA-GRC stack. [Online]. Available: http://www.cloudsecurityalliance.org/grcstack.html

[21] (2011, Sep.) CSA cloud security alliance cloud controls matrix (CCM), v1.2. [Online]. Available: https://cloudsecurityalliance.org/research/initiatives/cloud-controls-matrix/

[22] C. Clayton. (2011, Sep.) Standard cloud taxonomies and windows azure. [Online]. Available: http://blogs.msdn.com/b/cclayton/archive/2011/06/07/standard-cloud-taxonomies-and-windows-azure.aspx

[23] R. Glott, E. Husmann, A. Sadeghi, and M. Schunter, "Trustworthy clouds underpinning the future internet," in *The future internet*, J. D. et al, Ed. Springer-Verlag, Berlin, Heidelberg, pp. 209–221.

[24] A. S. Ibrahim, J. Hamlyn-Harris, and J. Grundy, "Emerging security challenges of cloud virtual infrastructure," in *Proc. of the Asia Pacific Cloud Workshop 2010 (co-located with APSEC2010), Sydney*, 2010.

[25] Z. Afoulki, A. Bousquet, and J. Rouzaud-Cornabas, "A security-aware scheduler for virtual machines on iaas clouds," Tech. Rep. RR-2011-08. [Online]. Available: http://www.univ-orleans.fr/lifo/rapports.php?lang=en&sub=sub3

[26] M. Taylor and C. J. Guo. (2012, Jan.) Data integration and composite business services, part 3: Build a multi-tenant data tier with access control and security. [Online]. Available: http://www.ibm.com/developerworks/data/library/techarticle/dm-0712taylor/

[27] F. Hao, T. V. Lakshman, S. Mukherjee, and H. Song, "Secure cloud computing with a virtualized network infrastructure," in *Proc. of the 2nd conf. HotCloud'10*. USENIX Ass., USA, 2010, pp. 16–16.

[28] A. S. Ibrahim, J. Hamlyn-Harris, J. Grundy, and M. Almorsy, "Cloudsec: A security monitoring appliance for virtual machines in the iaas cloud model," in *Proceedings of 5th International Conference on Network and System Security (NSS 2011), Milan, Italy*, 2011.

[29] H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE J. of Security & Privacy*, vol. 8, no. 6, pp. 24–31, 2010.

[30] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Computing*, pp. 14–22, 2010.