Introducing the Information Security Management System in Cloud Computing Environment

Laslo Tot

Singidunum University, Danijelova 32, 11000 Belgrade, Serbia
E-mail: laslo.tot.10.dls@singimail.rs

Gojko Grubor

Sinergija University, Raje Baničića bb, 76300 Bijeljina, B&H
E-mail: ggrubor@sinergija.edu.ba

Takacs Marta

John von Neumann Faculty of Informatics, Institute of Applied Mathematics, Óbuda University, Bécsi út 96/b, 1034 Budapest, Hungary
E-mail: takacs.marta@nik.uni-obuda.hu

Abstract: Numerous organizations coordinate and certify their information security systems according to the Information Security Management System (ISMS) standard. Available Cloud Computing Services (CCSs) include new types of vulnerability (management, virtualization, sprawl, etc.) and differ in management requirements from other computational systems. Establishing a consistent security management framework (SMF) and information security management system (ISMS) in CC environment is a complicated, demanding and time-consuming process. Every experience from applying ISMS standard solutions is certainly useful, but not enough to entirely cover all security requirements of the customers and Cloud Service Provider (CSP). Attempts of establishing an integrated and consistent SMF and ISMS in CC environment have not been researched in-depth in recent available literature. In this paper, authors suggested a framework for an establishing quality management system (QMS) of CCSs, including CC SMF and CC ISMS, proactive digital forensic (DF), proactive and predictive security controls and corporate DF investigation process up to the level specified in Service Level Agreement (SLA).

Keywords: CC ISMS; CC SMF; Proactive Digital Forensic; Digital forensics; CCS QMS

1 Introduction

A manager of the clients' information security system should consider the nature of business, degree of information control and security risks within a Cloud Computing (CC) environment, in order to establish consistent and quality management system (QMS), and an information security management system (ISMS). Establishing ISMS in a CC system should gather all of the solutions and experiences in related technologies that are included in CC development. Establishing a Security Management Framework (SMF) and the methods of security risks management are basic requirements for designing all of the ISMS information systems, including a CC one. Establishing ISMS in a CC environment mostly depends on the model of the CC system and the type of the CC service. The greatest number of the ISMS specifications refer to the public CC system, which is, in fact, the subject of this paper. In the model of the public CC system and Software-as-a-Service (SaaS), multi-tenancy is the key to success. An effective and fully integrated simple template-based model transformation and synchronization approach has been proposed for the development of SaaS multi-tenant applications [14]. In the Platform-as-a-Service (PaaS) type of CC service, a user works with their data and with applications on hired platform from Cloud Service Providers (CSP). In the Infrastructure-as-a-Service (IaaS)-type of CC service, the infrastructure is entirely owned by CSP, and the user installs their applications on hired platforms. In most realistic scenarios, the end user is responsible for using hardware and software in the CC environment. In such cases, focus is on security specifications of the main data in the CC environment and on influence of the virtualization and management on establishing SMF and ISMS in CC environment including improvement of the CCSs QMS.

Related Works Review

According to the available references many authors focus their research on the technology solutions for data security of the clients in CC environment, such as: Distributed encryption system [13]; Multi-layer security (network, host and application levels) [1, 2, and 14]; Technical aspects of potential digital forensics in distributed Cloud environments by Dominik Birk, 2011; Possibility of digital signature application in the Cloud suggested by Doug Bannister, Omnivex Insight, 2011; Use of honeypot technology, its advantages and disadvantages and value to the Cloud security proposed by Nithin Chandra S. R and Madhuri T. M. in their article, Cloud Security using Honeypot Systems, International Journal of Scientific & Engineering Research Volume 3, Issue 3, 2012; Applications of end point security in virtualized environment written by Darren Niller, 2002; Detailed analysis of all aspects of CC security and lack of trust in the Cloud, regarding confidentiality, integrity and availability of information, privacy and auditability, and DF investigation, by authors Bharat Bhargava, Anya Kim, and Youn Sun Cho in their article, Research in Cloud Security and Privacy, 2012; Possibility of traditional DF investigation in CC environment suggested by Gartner group, in the

article, Assessing the Security Risks of Cloud Computing, in June 2008, etc. These are some of many technical solutions suggested for improvement of data and privacy security in the CC system.

Generally CC security refers to a broad set of policies, technologies and highly distributed security technical and procedural controls. After all, CC security is an evolving sub-domain of computer security, network security, cyber security and eventually information security. Authors of this paper contribute by assessing and collecting all relevant aspects of the CC system security, and by suggested CC SFM and CC ISMS including not only technical security controls (proactive and predictive), but also procedural controls and contractual obligations to overcome lack of trust in data security on both sides – CSP and customers. Vulnerabilities in virtualized CC environment are quite well described by IBM and many authors [4, 5 and 13], etc. The authors of this paper suggested a comprehensive framework of CC SMF and CC ISMS, including SMF and ISMS recommended by standards ISO/IEC 27001/2:2013, to improve CC management system and QMS of the CCSs and security and privacy of data, and to increase mutual trust in CC environment. Furthermore, the authors suggested the overall strategy of CC QMS including security best practice principles, real time managing risk, continuous monitoring, and proactive and predictive[1] security controls to increase security and enable DF investigation in CC systems up to certain level specified in the SLA.

2 Virtual Infrastructure Management

A basic driver in the development of a CC service is virtualization, which most usually refers to virtualization of computers' and networks' hardware and it is the basis of public CC system configuration. In this way, different applications could be applied on different virtual platforms, but on the same physical machine [12]. The complexity of the virtual infrastructure management includes the following:

- Mandatory control of availability and usage, and approach to the physical and virtual resources;
- Implementation of the solutions for special situations, and
- Security of the customers' virtual machines (VM), tasks, monitoring and reporting on the CC centre usage.

In practice, there is a lack of suitable tools and theory for discovering errors and performances analysis of the ISMS virtual infrastructure. Relative independence of the numerous created VMs from physical machines, results in so-called liquid

[1] Security control that includes artificial intelligence mechanism to detect, prevent and predict attacks.

computing, better known as the VM sprawl [19]. In order to avoid the security risks from VMs sprawl, a management tool limits the creation of new VMs by assigning authorizations. Further, it provides a strong monitoring system which reports about allocated, but unused VMs. Because of the requirements for balancing load of the physical machine in the CC centre, locations of the created VMs and evaluation of the virtualized CC centre efficiency are specific problems.

Consistent ISMS in a CC environment requires a strong monitoring system of the virtual infrastructure that includes monitoring of physical hosting servers, virtual machine monitors (VMM) or hypervisor, and VMs and applications that operate on them. Virtual machine Introspection (VMI), as the process by which the state of a VM can be observed from either the VMM or from other VMs, is a new security risk factor to customers' data. That is why VMM has full access to the resources of all VMs and if it is compromised the customers' data can be misused, too. This phenomenon remains an open research problem.

Monitoring of the physical servers is very important, because of hosting a great number of VMs, and the responsibility of the CSP. The CSP uses not only some of the known software tools, such as Open Manage and IT Assistant (Dell), Open View (HP) or Nagios (open code), but also their own hardware tools with better performances. There is no fundamental difference between the meaning of the terms of VMM and hypervisor. A VMM monitors and directs the VM, and the hypervisor refers to the function of a machine's kernel supervision, while in CC it means that the kernel supervises more than one VM (hypervisors). Therefore, in a CC system, the hypervisor/VMM could be considered the kernel of a virtual infrastructure. Some of the more famous hypervisors are VMware ESX, which includes web interface for ESX – MUI (Management User Interface) for monitoring and management of the current VMM usage, Hyper V in the server Windows 2008 R2, Windows 2012 OSs, etc. Usually, for the monitoring of applications on a VM and for applications on the physical machine, the same tools are used, but the difference is in the management of system usage from the application side.

3 Cloud Computing System Management

In theory, as well in practice of computer science, there are many definitions of service management [2], such as:

- The capacity of the organizations to deliver services to clients
- The set of special organizations' capacities for giving additional values to customers in the form of services
- More than a set of capacities, because it includes a professional team of experts with specific knowledge and skills.

The service delivery model in a CC environment refers to a set of more customers, assets, resources and capacities with flexible payment only, for what was used.

Management of the CC system services is an inherent vulnerability in a CC environment, not only because of the virtualization and accompanying vulnerabilities, but also because of certain other reasons. The main reason for the new approach to the CC system services management lies in the enormous increase of digital information in the world, and an ever-more difficult and more complex management of the so-called digital universe and big data. The organization IDS.com (Intelligent Document Solutions) predicted that the digital universe would grow from 1.2 million PB (petabytes, 1 PB = 1.000 GB) or 1.2 ZB (zeta bytes) in 2010, up to 35 ZB in 2020 [9]. As the CC is already becoming an integral part of the digital universe, more than 34% of the total digital data in the world will be stored or secured with CC services. Until 2020, CC services will become even more important, due to the following reasons [9]:

- They will be cheaper, and the economy of organizations will initiate innovative development
- They will become much more important for individual users because of mobile access possibility
- They will include advanced services (data compression, de-duplication, etc.) for easier management of the big data. They will become part of the solution for more efficient management of the digital universe. In a CC environment, management of the performances and errors should be entirely automated, sophisticated and analytical. The CC operator should adjust, integrate and coordinate management of the all CC functions. Management of the infrastructure change and configuration in the CC system requires fast reaction and the Configuration Management Database (CMDB) must be used for better performance. For the effective management of the CC server's change and configuration, the CMDB must be embedded in this process and integrated with other controlling operations.

The tools for management in physical, virtual and CC environment are comparatively shown in Table 1 [2].

Table 1
Main management activities in physical, virtual and CC environment

Functions of the management	Physical servers	Virtual servers	CC environment
Management of the performances and errors	Manual or procedural approach to the monitoring and management of the resources, based on the events	Greater automation Access based on models and focused on services and applications	Entirely automated, sophisticated and analytical Operator adjusts, integrates and coordinates management functions

Functions of the management	Physical servers	Virtual servers	CC environment
Management of the infrastructure: change and configuration management	Manual processes on demand and change management according to the plan	For better performance a CMDB could be used	Fast change management For better performance, a CMDB must be used
Management of the server: change and configuration management	Manual processes on demand Change management according to the plan	For better performance, a CMDB could be used	Change management requires speed For better performance, a CMDB must be embedded in the process and integrated with other controlling operations

3.1 Infrastructure Management in Cloud

Holistic method of the integrated management of the physical and virtual resources (Iaas) is the main problem of the CSP. The main goal of the CSP management is to secure dynamic and fast provisions of the resources for CC applications. For this purpose, there is a tool already in development, the so-called Manager of Virtual Infrastructure (VIM) [4], which is usually called CC OS (Operating System) [23] or CC engine[2]. This type of software resembles a traditional OS, but instead of managing just one computer, the VIM aggregates resources of numerous computers with a uniform view at users and applications. Two following categories of the tools for management of IaaS were suggested [2]:

- Tool sets for the CC system that provide a distant and secure interface for creating, controlling and monitoring the virtualized resources, but it is not as efficient for VIM as specialized tools.
- The VIM tools with automatic balance of load, consolidation of servers, but without an interface for distant access to the CC system.

Both categories of tools are basic tools for the CC ISMS, or management of VM's vital cycle, but they are not applicable for implementation into all CC systems. The main difference between these two categories of tools is that the CC tools have an interface for remote access and management of the great number of consumers' accounts.

[2] *Amazon Cloud Computing*, www.amazon.com

3.2 Relationship Management among Cloud Service Provider and Consumers

The concept of classic relationships of the CSP and consumers is shown in Figure 1 [2].

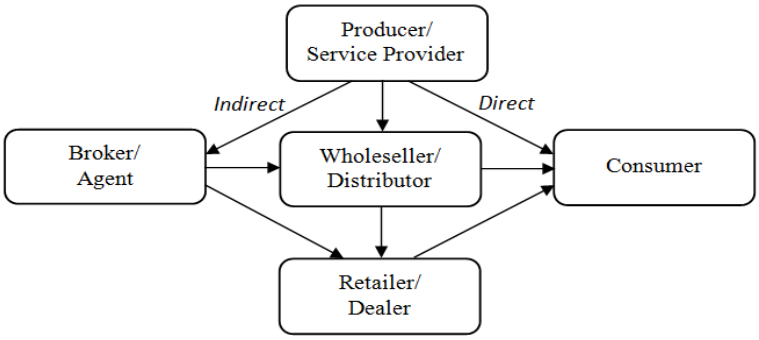

Figure 1
Diagram of classic relationship between the CSP and service consumer [2]

In the CC environment, the CSP performs many activities for service delivery, such as: defines the strategy, designs, invests, implements, transmits the data and operates within the CC infrastructure. The CC services increase the value of the customer's product that pays for what they use and they do not accept responsibility for expenses of service delivery and its risks. To ensure satisfaction of the customers with the quality of the CC services, a CSP must consider numerous factors, such as: nature of business and profiles of the target users, value of the CC services for users, form of use and payment for the services, security of the user's information, possibility of digital forensic (DF) investigation in the case of some incidents, etc. The CSP can increase the value of services on different levels, using different equipment, specialised technologies and additional services, etc.).

Quality of the CC service includes two basic elements: *benefit*, or what the customer gains, and *assurance* of the service delivery – available on time, with sufficient capacity, and continuous and secured. Service value for the customers is a combination of these two elements. Estimation of the CC service quality mostly depends on the two component perceptions: *expected value* – service level that the user expects, and *empiric quality* – experienced service level estimation of the user. There are various models for payment of the CC service, but payment for the used items are mostly applied (e.g. expenses for electricity and water bills, etc.), and subscription (e.g. on an annual level). Security of the user's information is the key factor of distrust in the CC systems. In practice, it is defined as the share of responsibility between the customers and the CSP, through the Service Level Agreement (SLA). In the case of incidents or crime in the CC environment, DF

investigation is naturally expected, but it is almost impossible to perform in practice. Implementation of the proactive forensics [7, 21, and 22] and the definition of some level of forensic investigation in the SLA and CC SMF documents are likely to yield solutions for the potential DF investigation in the CC system. They should be applied to the CC Service's Development Life Cycle (see Figure 2).

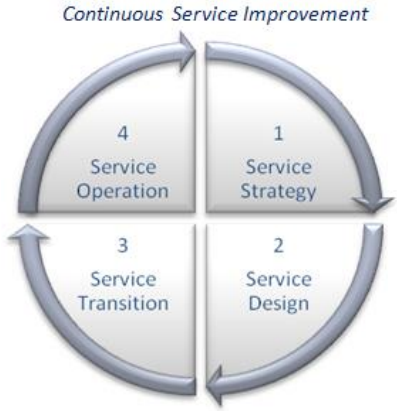

Figure 2
Development Life Cycle of the CC Services

3.3 The Importance of Introducing Proactive Forensics into CC SMF and CC ISMS

Proactive forensics could be defined as a preventive step for locating and collecting key forensically relevant data. In the CC system, with multi-tenancy VMs, the rate of overwriting data is much larger than in an ordinary computer. What the customers and CSP do, and who is responsible to collect forensic evidence proactively is the key question? Besides, it is doubtful whether classic (or post-mortem) DF investigation can be applied in CC system at all [11]? Generally, post-mortem forensic process has four phases: data access and identification, data acquisition, data analysis and evidence reporting. Access to the data sources and collection is the first step. Taking forensic images to the forensically sound media is the next step. In the analysis phase, the forensic image is installed by outside booting processes (usually from forensic tools) onto forensic computers for analysis. If a forensic image is booted onto a physical machine with different hardware configuration, the OS will discover those differences and try to install the missing drivers into image and contaminate it. Obviously, it is unacceptable according to the principles of the DF science. In the CC virtualized environment this approach, including even live forensics, is not sufficient to recreate the original environment. Actually, VM simulates some basic

hardware components and does not support a wide range of hardware devices. Therefore, a forensic image cannot be installed directly into a VM that requires some added files with information on the booted system. Some forensic tools could resolve this problem, including EnCase Physical Disk Emulator (commercial), ProDiscover family (commercial), Live View (free), and others [11].

A clause in the SLA, on some level of forensic investigation, could be a practical solution for the first time. It can provide an obligation for the CSP to proactively collect forensically relevant data. But the question is: who is to be trusted with discovering and collecting data, and identifying the nature of the incident? The security team, without forensic techniques, tools, knowledge and experience may compromise the evidence. Hiring of a third-party consultant could be unacceptable, too. A well-trained forensic investigator in the organization's security team can provide the following services:

- Electronic information discovery
- Forensic and technical consulting
- Storage media forensic investigation
- Proactive network digital forensic
- Internet forensics
- E-mail and other messaging systems forensics
- Incident nature identification
- Data collection and registration
- Malware risk reduction.

Generally, proactive forensics, included into CC SMF and CC ISMS, is a promising concept. It provides protection to an organization's responsibility, competency advantages and forensic evidence collection for future forensic investigations. In the CC ISMS, a strong monitoring system should be a mandatory proactive measure, including monitoring of the CC centres, CCSs availability, access and usage of VMs, data security, security emergency solution, flexibility for new VMs and new task additions. It is a good protection from VMs sprawl vulnerability, too. Monitoring of the VMs in the CC system includes physical servers, VM monitors or hypervisors and applications running on the VMs. Proactive forensic processes of the CC monitoring system include the generation, collection, analysis and reporting of the forensically relevant events instead of huge volumes of security events. It means that security problems could be stopped before critical escalations [11].

In general, computer incidents' proactive forensics in an organization includes proactive identification and collection of digital traces, investigation and malware

risk mitigation. Eventually, in the CC system, security monitoring has a much greater importance since, it simultaneously provides a real-time security monitoring alarms, reliable CC and security system functioning, and fast reaction against incidents. Defining and setting forensic evidence selection criteria is the main challenge in the networks and Internet forensics, including Cloud forensics, too. In the CC environment, Cloud forensics [13] means an application of the DF investigation as a subset of the CC system, computer forensic, and network and Internet forensic (Figure 3).

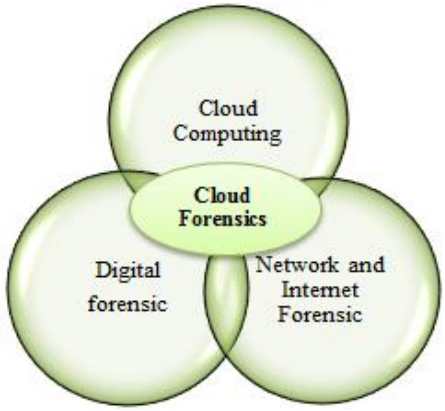

Figure 3
Place and role of cloud forensic

The summary of the critical success factors (CSF) of Cloud forensics is shown in Table 2 [11].

Table 2
Summary of the *Cloud forensics* critical success factors

Cloud forensics CSF	**Descriptions**
Management quality	Provide all of the stakeholder with cooperation and support to the DF investigation [9]
SLA	Oblige CSP on certain level of DF service in the CC systems [15]
Proactive forensics	Provide the traces of malware and direct attacks collection to the CC systems log files of network and security devices [22, 1 and 11]
Anti-forensic tools	Disable anti-forensic activities in the CC systems [11 and 9]
Managers' responsibility	Use ISMS standard (ISO 27001) to assess individual mangers' responsibilities [13]
Data source quality verification	Develop method and criteria for forensic incident data source quality evaluation [8]
Mobile devices forensic	Provides specific requirements for mobile devices forensic and balance them to the requirements for privacy protection [11]

Monitoring the key CC service performances indicators requires metrics establishing in the design phase (see Figure 2) [6]. Examples of the metrics are as follows:

- Service performances according to business and strategic plans
- Financial gain to the business
- Monitoring of the key ICT processes supporting CC services
- Reporting on the level of services Customers' satisfaction, etc.

The final criteria that require many activities to achieve wanted quality of the CC service management must be implemented before service delivery. They include investigation of the CC services acceptance against overload, users' activities, error tolerance, data recovery, network delay, and payment process.

3.4 Management of the SLA Agreement

Agreement between the customers and CSP on the SLA is the main document. It is based on the users' information security requirements and needs for DF investigation of computer misuse or criminal activities in the CC environment. In current practice, potential DF investigation in the CC environment requires a detailed SLA contract between the customers and CSPs that compels the CSPs on forensic investigation services up to the specified level. In this way, the customer knows what to obtain, or not, in the case of a DF investigation. Requests of the customers for this CC service should become a standard part of the SLAs to secure their vulnerable information into the CC system. This implies that the CSP should implement security controls that could enable proactive digital evidence collection and DF investigation later on [22]. Proactive forensics means taking precautionary steps that do not include the need for locating key evidence ("smoking gun") in the DF investigation process. Some CSPs have already offered DF investigation up to the certain level, as a CC service [18].

3.5 Management of the Anti-Forensic Tools and Activities

Legal processes for the DF investigation are increasingly becoming mandatory services in the ISMS systems [10 and 17]. Generally, computer criminals use numerous activities, techniques and tools to disrupt DF investigation process. Apart from classic hacking techniques for erasing of digital traces generated by computer (such as PC Cleaner, Evidence Eliminator, etc.), setting of time bombs, applications of the users for shut-down, etc., some anti-forensic techniques are also popular, including those mentioned in [23 and 16]:

- Modification of the time seal
- Header change and file extension, extracting hash password values without leaving a trace

- Data mule types of attacks on the reserved sectors by the system on hard disk
- Generating random file names (detection based on discovery of file signature is avoided), etc.

3.6 Human Resources Management in Cloud Environment

Quality management of the human resources and cooperation of all stakeholders are the most important factors in the CC system management and for successful corporate DF investigation. Management of the CC system that includes the CSP and customers must explicitly support teams for corporate DF investigation [17]. The organisations of the CSP and customers must establish security policies and procedures for managing computer incidents and corporative DF investigations. In the case of braking into the CC security system, DF forensic expert has to lead DF investigation process and harmonise functions of the team combined by programmers, administrators, engineers of network equipment, etc. Digital forensic experts must provide professionals with various skills, job procedures and protection of digital evidence integrity in the chain of custody. All participants who have access to the forensic data and evidence must maintain records for every activity in these procedures [15].

Carelessness of the managers and neglect of security events are common reasons for numerous court cases. It is particularly easy to prove consequences of carelessness and neglect of the plan and conduction of the technologies management strategy. Documented international ISMS standards, ISO/IEC 27001:2013 and ISO/IEC 27002:2013 provide necessary instructions regarding organization, methods, tools, security controls and procedures for the potential CC ISMS. These standards should be supported by newly developed (or in development process) set of standards for DF investigation, such as ISI/IEC 27033, ISI/IEC 27034, ISI/IEC 27035, ISI/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC 27043. They should be used for the ISMS implementation into the processes of CC information security systems, including DF investigative procedures, due to increasing forensic needs for estimating individual responsibility of the security technologies managers.

3.7 Functional Model of Introducing ISMS into CC system

For the reliable identification of the computer incidents, an uninterrupted verification of data source signs and indicators of incident is required [3]. Some standards of good practice in proactive detection of incidents in computer networks recommend the following activities [5]:

- Data users should develop and document the method and criteria for evaluating quality of incident data information source;

- Users and / or the CSP should verify information on an incident before importing them into the database or in a program for incident management, but without the process flow being delayed;
- Information on an incident should be in correlation with external services, refilled and filtrated in order to prevent event duplication, but without the process flow being delayed;
- If the source of information implements mechanisms of return links, the users should use it in the case of request for quality improvement of incident information;
- Data sources for threats and attacks (CERT/CIRT), should develop its sensor networks for malware detection and other incident indicators, implement honeypot and sandbox technologies at customer's side and, if it is possible, implement passive scanners for DNS monitoring [19].

In CC environment expected level of the company security and business continuity management may be achieved by real-time business risk assessment and by compliance to a wide range of security expectations, not only to recommendations of the information security international standards [21]. The basic principles of good practice for introducing SMF and ISMS into CC system are suggested by authors and summarized in Table 3.

Table 3
Basic principles of the SMF and ISMS best practices in CC system

Category	Basic principles of ISMS good practice in cloud system
Risk management	Key factor of the CC security, including identification, location, assessment and security risk mitigation, by choice and implementation of the best practice security controls in the CC environment (from the business point of view).
Information security policy	Includes security risk management methodology, scope and limits that change with the type of CC service and may be overlapping among SaaS, PaaS and IaaS policies; it should be updated and supported by standards, procedures and guides.
Control and change management	Includes procedural controls for configuration management (CM) and change control (CC); CM and CC automation is required in the CC environment.
Audit	Proves standards and security policy conciliation and effectiveness of security controls. Detects new vulnerabilities and requires both automated tools and manual procedures.
Vulnerability scanning	Includes all CC managing platforms, servers and network devices and identifies all new software, hardware and configuration vulnerability. Uses tools like Nessus, Back Track (Kali), etc.
Duty separation	Limits user privileges according to the "need-to-know" principle for duty performance.
Information assets	All information assets, including people, hardware, software

Category	Basic principles of ISMS good practice in cloud system
management	and network devices that make CC system infrastructures, must be protected.
Symmetric and asymmetric cryptography	Key management and digital certificates secure CSP infrastructure protection, but it is not applicable in the CC system.
Cryptography on demand	Proposed solution where customers are obliged to require cryptographic key from CSP before communication with the CCS.
Security of data storage	Identifies the need for encrypted protection of data storage and recognizes that some users need the special data storage's.
End point security	Secured by protection of the CC system resources, end points and access restriction to protocols and device types.
Network security	Secured by network traffic protection on the network devices and data package levels
Proactive forensic	Provides network incident prevention and strong real time monitoring, but lack of expensive and matured technologies, tools and knowledge are its limitations.
Access control and authorization	Secured by policy, strong authentication and effective access control implementation, depends on defined identity, role and privilege of the CCS users
Choice of the CSP	Should be based on CSP relations to the security and complementary security solutions with current organisational security practice.
Transparency	Choice of the CSP should be based on its readiness for transparency in key security items, including DF processes.
Security controls	CSP should implement proactive and predictive security controls to be acceptable and to fulfil user and legal requirements.
Security standards and practice	For the CCSs users the best practice is to define a comprehensive security program or CC SMF, including security polices for all CC service life cycle activities.
Network isolation	To provide isolation among different user services and network information flows, a CSP should separate the controls and flow of the network information.
Use of CMDB	It is most important for CC maturity and effective resources and automated CC system processes management.
Configuration integrity	Provided by software installation for the CC system configuration check and identification of system file platform, non-authorized modification is prevented.
Identity management	CSP must implement scalable and robust identity and access management systems, which establish strong identity authentication, authorization and user platforms management.

Introducing ISMS into CC system is more complex process than doing that in LAN or distributed computer network under full control of the users. However, best practice and experience from information security management system

(ISMS) according to the standards ISO/IEC 27001&2: 2013 could be used. Using system engineering knowledge and process approach, CC users can apply some process model such as PDCA (Plan, Do, Check, and Act), Six Sigma, CMMI, etc. The authors suggested PDCA model due to its simplicity and broader use in the many ISO standards. Implementation of the CC ISMS is the main purpose of the PDCA process model application. Functional model for ISMS implementing into CC environment, suggested by authors, is shown in Fig. 4.

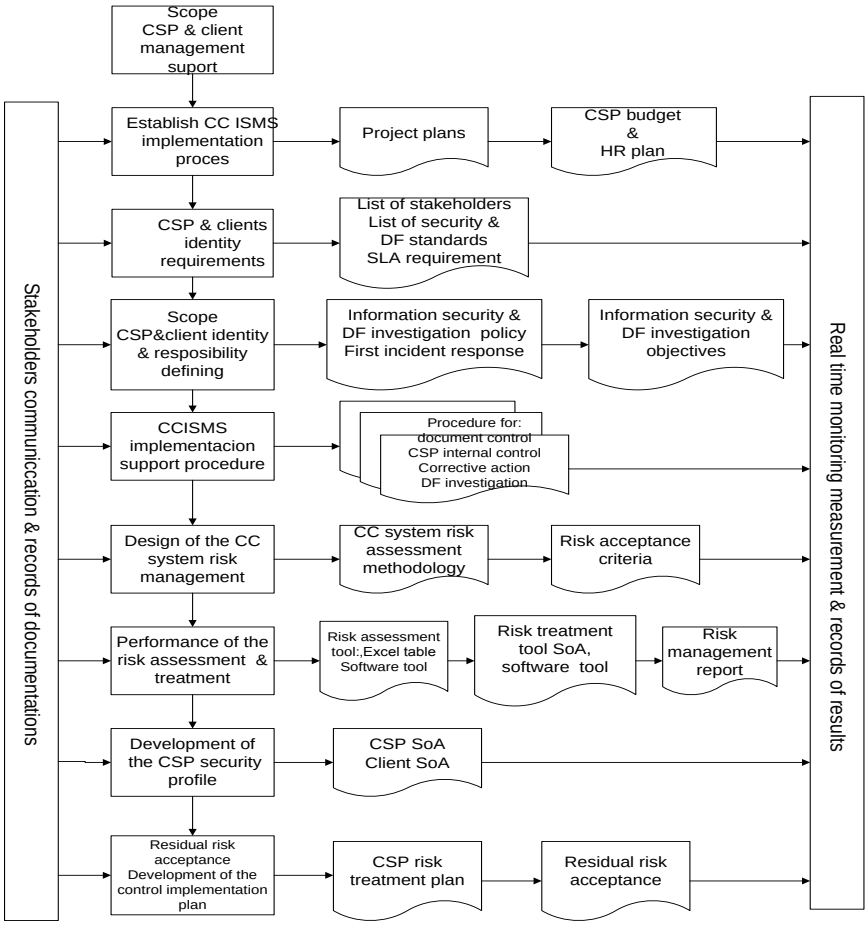

Figure 4
Functional model of the CC ISMS implementation (Part 1)

In Fig. 1 the CC system consists of the CC centre and part of the client ICT system that use service of the cloud service providers (CSPs), such as SasS, PaaS or IaaS. The detailed and completely new form of the SLA document is probably the most important concept in this model. The SLA document must include all

agreed upon activities by the clients and CSPs, throughout every step of the CC ISMS implementation process. In practice, the CSPs, as a rule, design and form SLA document, leaving more responsibilities for information security on the client side and without any word about possible incident, loss of the clients' information and potential digital forensic (DF) investigation. Many authors and organizations (such as Gartner group, NSA, Norton Symantec, etc.) suggested that the DF investigation in CC system has become almost impossible mission. The CSPs usually claims that security posture in CC centre is at highest level of the efficiency and effectiveness in the CC centre. However, attacks and penetration into CC system must be supposed, although there is no much information about that. That is why clients and CSPs must cooperate closely to prevent cloud services misuse, including stealing information of the clients. Functional model of the CC ISMS implementation process (see Fig. 4) is adapted by the authors from best practice standardized ISMS (ISO/IEC 27001:2013). Many phases, steps and activities must be accomplished by consensus of the clients and CSPs, such as: Scope determination and management support; Identity and responsibilities requirements; Establishment of the CC ISMS implementation process and project budget; Development of many documents, e.g. security policy and procedures, including level of the proactive DF infrastructure, etc. Most likely, closest collaboration should be in intention and responsibility defining, including information security and digital forensic policies, objectives and both side responsibilities and obligations. The main problem in this process could be the level of the potential DF investigation in CC system, in case of clients data lost in virtualized CC environment. As a first step a CSP can agree upon some level of DF investigation in CC system in the SLA document (Fig. 5). Implementing real time monitoring system and proactive network DF infrastructure can help to convince clients in highest level of the CC information security system. In developing security profile both sides must align their Statement of Applicability (SoA) documents, at least regarding residual risk acceptance.

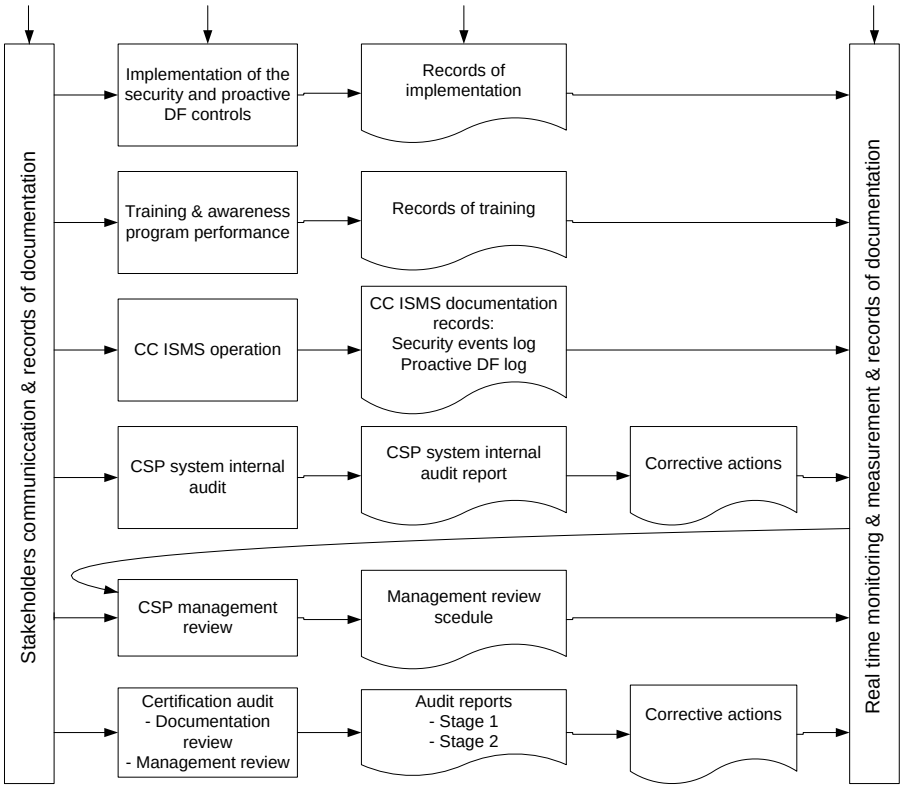

Figure 5
Functional model of the CC ISMS implementation (Part 2)

All other steps in Fig. 5 such as training and awareness, ISMS operation, and internal, management and certification audit, could be performed separately and independently at both side locations. Finally, certified ISMS on both sides could be a starting point to increase trust among clients and a CSP.

Conclusion

The CC system (CCS) is a modern computational type, including informative, human, legal, business, philosophical, and many other aspects. New types of CC vulnerabilities require abandoning the traditional container type protection concept. In the CC environment, especially for specific requirements, management of the CCSs life cycle, including the CC SMF and CC ISMS, must be established and implemented. In order to establish CC ISMS and CC SMF, principles and recommendations of the ISMS standards (ISO/IEC 27K) should be adapted and included in CC management system, and the traditional security management framework (SMF) should be enhanced by proactive and predictive security controls, proactive forensic infrastructure and mandatory DF investigation process

that is specified up to the certain level in the SLA. Quality of the CCSs could be provided by implemented both CC SMF and CC ISMS. Those are especially important due to further ISMS and security field investigations in the CC environment, open up new branches of smart grid computing [8] that uses more efficient network computational power, but requires enhanced information security, and proactive and even predictive protection from potential cyber-attacks. Therefore, security system in CC environment should be embedded, and DF investigation of computer crime in the CC environment should be enabled. Cloud forensic introduces a new approach to the traditional DF investigation methods and applications of the forensic tools and techniques. In this paper, a new framework of CC management system and potential use of proactive and predictive security controls, standardized ISMS and SMF, proactive forensic, and cloud forensic service embedded in the CC SMF and CC ISMS is suggested, in order to improve the QMS of the CCSs and to increase mutual trust in data security between CSPs and customers. Except of the CC security and management systems state-of-the-arts overview, comprehensive security principles and components suggested for establishing and implementing CC SMF, CC ISMS, and CCSs quality management system, are the main contribution of this paper. They are supposed to embed not only well-known security controls, but also some new ones, such as strong authentication, uninterrupted real-time monitoring, proactive network forensic, proactive and predictive security controls, embedded DF investigation infrastructure, etc.

The detailed process model and data flow information of the CC ISMS and CC SMF implementation process suggested by authors, should be subjected to the further research. A new system of legal and quality CC SMF and CC ISMS security policy and procedures should be formally described and defined, and standardized for more trusted, effective and efficient CC systems.

References

[1] Bradford, P. G., Hu, N: A Layered Approach to Insider Threat Detection and Proactive Forensics, 2005

[2] Buyya, R., Broberg, J., Goscinski, A., et al, Cloud Computing: Principles and Paradigms, John Wiley & Sons, Inc., 2011

[3] Cichonski, P., Millar, T., Grance, T. and Scarfone, K., Computer Security Incident Handling Guide, NIST Special Publication 800-61, Rev. 2 Recommendations of the National Institute of Standards and Technology, 2012

[4] ENISA (European Network and Information Security Agency) Report, Cloud Computing Information Assurance Framework, http://www.enisa.europa.eu, 2009

[5] ENISA (European Network and Information Security Agency) Report, Proactive Detection of Network Security Incidents, http://www.enisa.europa.eu, 12.07. 2012

[6] ENISA (European Network and Information Security Agency) Insecure magazine, str. 14-19, no. 35. www.insecuremag.com, September 2012

[7] Erickson, T., IDS, Digital Universe Study for EMC Corp., SearchStorage.com, The Security Help Net News, 2012

[8] Gorzelak, K., et al., Proactive Detection of Network Security Incidents, ENISA, 2011

[9] Gottlieb, J., Key Challenges in Proactive Threat Management, CEO of Sensage, The Security Help Net News, 2012

[10] Grance, T., Chevalier, S., Kent. K. and Dang, H., Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response, NIST Special Publication 800-86, 2005

[11] Grubor, G. & Njeguš, A., An Application of Proactive Digital Forensic in Cloud Computing Environment, International conference TELFOR. Belgrade, 2012

[12] Hoopes, J., Virtualization for Security, Syngress, ISBN: 1597493058, 2012

[13] Krutz, R. L. and Vines, R. D., Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, http://23510310jarinfo.files.wordpress.com/2011/08/ebooksclub-org_cloud_ security_a_comprehensive_guide_to_secure_cloud_computing.pdf, 2010

[14] Kun Ma, Bo Yang and Ajith Abraham, A Template-based Model Transformation Approach for Deriving Multi Tenant, Acta Polytechnica Hungarica, Journal of Applied Sciences, Vol. 9, No. 2, 2012

[15] Leibolt, G., The Complex World of Corporate Cyber Forensics Investigations, Springer's Forensic Laboratory Science Series, 2010

[16] Milosavljević, M. and Grubor, G., Digitalna forenzika računarskog sistema, Univerzitet Singidunum, 2010

[17] Milosavljević, M., Grubor, G., Istraga kompjuterskog kriminala, Univerzitet Singidunum, 2011

[18] MMSC – Morrison Maierle Systems Corp., Norman ASA, 2011

[19] Nacionalni CERT, Cloud computing, NCERT-PUBDOC-2010-03-293, www.cert.hr, 2010

[20] O Gara, M., Virtual srawl, Virtualization Magazine, irtualization.ulitzer.com, 2010

[21] Pál Michelberger Jr., Csaba Lábodi, After Information Security – Before a Paradigm Change (A Complex Enterprise Security Model), Acta Polytechnica Hungarica, Journal of Applied Sciences, Volume 9, Issue Nr. 4, 2012

[22] Taylor, P., Proactive Forensics in the Workplace, Litigation and Forensics, Data Recovery Services, Inc. www.legalforensics.com, 2010

[23] Zimmerman, S., Glavach, D., Cyber Forensics in the Cloud, The Newsletter for Information Assurance Technology Professionals, Vol. 4, No. 1, pp. 4-7, 2011