Cloud Standards in Comparison

Are New Security Frameworks Improving Cloud Security?

Carlo Di Giulio
University of Illinois at Urbana Champaign
cdigiul2@illinois.edu

Charles Kamhoua
Air Force Research Laboratory
charles.kamhoua1@us.af.mil

Roy H. Campbell
University of Illinois at Urbana Champaign
rhc@illinois.edu

Read Sprabery
University of Illinois at Urbana Champaign
spraber2@illinois.edu

Kevin Kwiat
Air Force Research Laboratory
kevin.kwiat@us.af.mil

Masooda N. Bashir
University of Illinois at Urbana Champaign
mnb@illinois.edu

***Abstract*— The increasing relevance of information assurance in cloud computing has forced governments and stakeholders to turn their attention to Information Technology (IT) security certifications and standards. The introduction of new frameworks such as FedRAMP in the US and C5 in Germany is aimed to raise the level of protection against threats and vulnerabilities unique to cloud computing. However, our in-depth and systematic analyses reveals that these new standards do not bring a radical change in the realm of certifications. Results also shows that the newly developed standards share much of their basis with older, more consolidated standards such as the ISO/IEC 27001 and hence the need for determining the added value.**

In this study, we provide an overview of ISO/IEC 27001, C5, and FedRAMP while examining their completeness and adequacy in addressing current threats to cloud assurance. We question the level of protection they offer by comparing these three certifications alongside each other. We identify weaknesses in the three frameworks and highlight necessary improvements to meet the security requirements indispensable in relation to the current threat landscape.

Keywords*— *FedRAMP; ISO; C5; Certification; Standard; Framework; Cloud; Privacy; Security.

I. INTRODUCTION

In the last decade, information assurance in cloud computing has captured much attention from governments and the Information Technology (IT) industry. Increasing resources and efforts have been devoted to fighting against cyber-threats in cloud environments [32]. On the one hand, the research of effective protection against new vulnerabilities has forced the creation of innovative security techniques. On the other hand, to effectively measure the security level guaranteed by Cloud Service Providers (CSPs), thus enabling cloud tenants evaluating the most suitable provider for their security needs, has required standardization of attestation and certification processes. We refer to "standard" as a structured approach to address IT security built on measurable indicators represented by controls, such as a checklist, or general yet unequivocal requirements, such as clauses or principles.

Among the most used IT security standards, the ISO/IEC 27001—which defines requirements and procedures for the implementation, maintenance, and improvement of Information Security Management Systems (ISMSs)—has offered IT security certification since 2005, and a 2013 revision brought it up-to-date with new technologies [27].

In the US, the Federal Government has turned to cloud services to improve IT efficiency while maintaining high security standards and reducing extremely high expenditure [28]. The creation of the Federal Risk Authorization Management Program (FedRAMP) in 2011 represents an important step toward information assurance in the cloud. The program builds on inspection, assessment, and authorization procedures to guarantee security and privacy of information held by Federal Agencies in public cloud. The program differentiates three security baselines (low, moderate, high) according to the sensitivity of data processed in cloud systems, and relies on a selection of controls from NIST SP 800-53.

Last in the timeline, the *Bundesamt für Sicherheit in der Informationstechnik* (BSI–German Information Security Office), presented its Cloud Computing Compliance Control Catalogue (C5) in February 2016. The C5 embeds cloud-specific security and privacy controls. Although BSI presented C5 as a mere guideline for Cloud Service Providers (CSPs) to build upon other certifications, what C5 does is add another element to the already crowded landscape of standards for IT providers. Like other frameworks, C5 relies on security controls organized in control domains. C5 prescribes a set of basic requirements which are mandatory for Clouds to be considered compliant with the standard. Additional requirements are specified to assure higher security level, where applicable. The large diffusion of existing IT security standards such as the ISO/IEC 27001 questions the necessity of creating new frameworks rather than focusing on the improvement of existing ones. Fostering further complications, rivalry between multiple standards often creates expense for the CSPs, since those CSPs already certified against one standard often need multiple certifications to satisfy statutory, or legislative requirements.[1]

Approved for Public Release; Distribution Unlimited: 88ABW-2016-6154, Dated 30 Nov 2016

[1] FedRAMP, for instance, is required to CSPs providing services to the Federal Government

2159-6190/17 $31.00 © 2017 IEEE
DOI 10.1109/CLOUD.2017.16

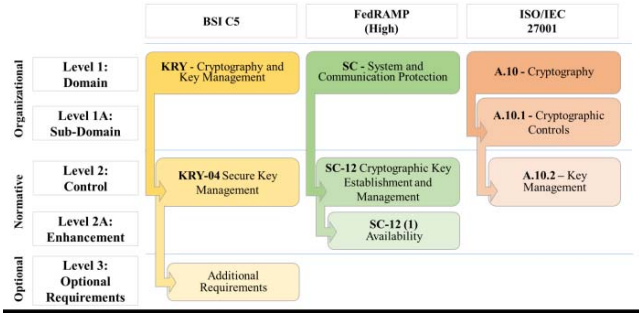

Figure 1: Structure of the three standards

This paper addresses questions of whether new certifications such as FedRAMP or C5 add to existing requirements: how effective are IT security measures and frameworks based on certifications against these standards? Are the newer standards better than the old ones at protecting information assurance in cloud environments, and if so, how? Is it worth investing in new cloud security standards rather than focusing on the improvement of old ones?

This paper aims to respond to these questions and define the effectiveness of C5 and FedRAMP compared to ISO/IEC 27001 in addressing information assurance in cloud computing. The results of our observations clarify the impact of C5, FedRAMP, and ISO/IEC 27001 (henceforth referred as "ISO") on the vast landscape of IT security standards.

We offer a comprehensive review and analyses of their completeness and adequacy. We point out missing controls and control domains in the three standards and suggest their impact in cloud assurance by showing how potential threats can exploit the missing security measures. We identify weaknesses in human resources management and mobile security measures for two frameworks, and more potential threats stemming from gaps in access and credential management. Our conclusions can be used to improve the effectiveness of further versions of these frameworks.

A. Structure of the Standards and Differences

The three standards oversee the secure implementation of IT systems by prescribing security measures, defined as "controls," organized in control domains. Each of the standard lists a variable number of controls, identified by a code. For example, FedRAMP prescribes security measures on management of cryptographic keys in a control titled "Cryptographic Key Establishment and Management." This control is the twelfth control in the domain named "System and Communication Protection." The same control is further developed in control enhancements, providing more details on the nature of the security measure, and prescribing further actions to achieve cloud assurance (Figure 1). The other two standards, C5 and ISO, do not prescribe control enhancements, but follow a similar structure in that security controls are organized in domains. C5 specifies additional controls as optional, thus not required to achieve full compliance with the standard. ISO is organized in domains, a sub-level that we defined as "sub-domain," where the letter of the standard does not specify accurately any security measures, and last the control level, where the standard details the security measures. FedRAMP is built on 421 controls and enhancements in 17 domains. ISO has 13 domains, and a total of 114 security measures. C5 has 18 domains and 118 controls, of which 54 are accompanied by optional additional requirements.

B. Previous Work

An extensive body of academic and non-academic research literature investigates IT security standards and guidelines. In this section, we include comparisons among IT security frameworks, detailed analyses of standards, and classifications of threats to cloud security.

Part of the literature has analyzed existing standards either comparatively [19][35][20][1][14][15][24] or limiting the observation to a specific framework [6]. In most of these studies, the authors highlight gaps in the certification process, or provide support to the choice of tenants or CSPs among a variety of certifications. These studies, however, are often based on outdated frameworks—such as ISO/IEC 27001:2005—or offer limited suggestions for the improvement of existing standards. The work of the Cloud Security Alliance (CSA) [13] is also based on the observation of existing standards, but goes beyond observation by creating a new framework. CSA has reviewed existing standards since 2008, collecting the results on a matrix (Cloud Control Matrix) that relates the existing frameworks through a list of detailed cloud assurance controls. CSA bridges the gap between common industry and government standards by offering its own framework of consolidated standards. Similarly, some studies promote improvements to the current status of cloud security by remodeling the analytical framework around security assessments. They either suggest the definition of security metrics on a case-by-case basis rather than building on existing frameworks [3][4][6] or limit their scope to suggesting the inadequacy of existing standards deeming them unable to keep pace with innovation and too expensive for small firms, thus eroding competition [36].

In our analyses we also considered the body of literature that focuses on threats and issues to cloud security. Security standards and threats to cloud assurance have a strong correlation, because confidentiality, integrity, and availability of information managed in the cloud may suffer from a number of causes of endogenous and exogenous origin. Knowledge on these issues helps identify weaknesses and flaws in the adopted system, thus improving existing protection measures. Part of this body of literature focuses on specific threats, circumscribing the observation to single threats or a classes of threat. These studies consider attacks in IaaS, PaaS, and SaaS, including mobile environments [24][25][28][38][17]. Another branch of literature draws from results of existing studies, building comprehensive reviews and classifications, either limiting their scope to threats [18], or as part of a larger review of topics on cloud computing [2]. Three studies by CSA fit into this area of work. CSA has addressed cloud-specific menaces to information assurance, publishing white papers and studies on the issue [8][9][10]. The most recent publication is "The Treacherous Twelve: CSA's Cloud Computing Top Threats in 2016". Building on the results of a survey of 271 IT experts worldwide, CSA offers a nuanced comparison of twelve security issues in cloud computing, ranking them according to the severity of risks, and commenting

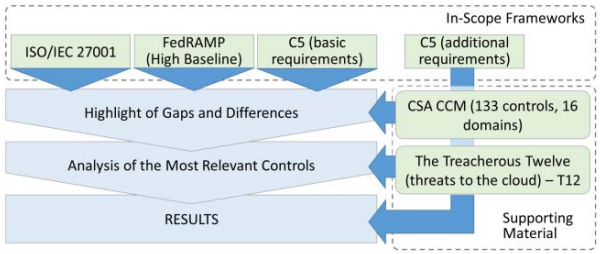

Figure 2: Methodology

their impact on cloud assurance. An important feature of CSA's collection of issues is the connection with other work, such as the Cloud Control Matrix (CCM). Issues and controls in the matrix are matched to highlight the areas with higher impact and possible security measures to implement accordingly. CSA has conducted a wide exploration of issues in cloud computing. Unlike the CSA effort, existing security standards are not connected with potential threats, thus leaving gaps and flaws unaddressed.

C. Our Contribution

The literature we have reviewed has observed existing standards as multiple frameworks either to be considered alongside each other, or focusing on one at the time. Such analysis, however, is quickly outdated by the release of newer versions of the analyzed standards, or misses systematic observation of controls and control domains. Previous work sought threat and security issues, either from a higher perspective (collectively examining cloud assurance issues) or from a lower one (dissecting how a specific threat can exploit security flaws to endanger cloud assurance). In contrast, we review the impact of known threats in terms of their consequences in the current security landscape and the level of protection guaranteed by existing certifications and standards.

Previous research has shown differences in how FedRAMP and ISO can have an impact on cloud assurance [15]. However, that study was centered on clarifying effectiveness and completeness of the standards, justifying their characteristics in an historical perspective. Our work focuses on a systematic review of FedRAMP rev. 4 and C5—which are recent standards released by Government Agencies—and ISO/IEC 27001:2013, a well-established benchmark for information assurance. We look at how missing controls in current standards may result in security flaws and leave potential threats undiscovered; we contextualize our analysis to suggest a measurement of resiliency and adequacy of current standards; we gauge the impact of new standards in the context of cloud assurance and evaluate their complementarity.

II. METHODOLOGY

Our methodology is based on a three-step analysis. We collect and match the controls in the three standards against a third-party framework; we select the most relevant missing controls according to their adequacy at addressing current threats; and we analyze the missing controls in context, evaluating their effect on the threat landscape (Figure 2).

We compare FedRAMP at a high baseline, which includes the controls from the moderate and low baselines, and focus on

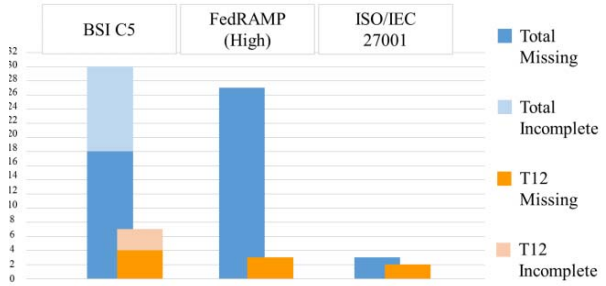

Figure 3: Missing Controls and T12 Selection

the basic requirements in C5. As mentioned in previous section, although BSI's catalogue includes additional requirements, compliance with the standard is achieved by implementing the basic list of controls. We include considerations for those controls in C5 that satisfies only in part the requirements in our analytical framework, or provide full coverage if supported with the additional requirements. Only one possible baseline is considered for ISO/IEC 27001.

In the first step, we collect the controls in the three frameworks—C5, FedRAMP, and ISO—and classify them according to the requirement they prescribe to the CSPs. To organize the controls, we adopt as the analytical framework the most recent CSA's CCM, version 3.3.1, published in January 2016. We match the requirements in the three standards to the controls in the CCM and verify the fulfillment of CCM provisions. Like the analyzed standards, this version of the matrix is organized in controls and controls domain, and includes a full matching with the controls in ISO/IEC 27001. In November 2015, CSA released a candidate mapping of FedRAMP rev. 4 at a medium baseline on the CCM [12]. We add the result of the mapping to our framework. However, since the document has not been officially released as an update to the CCM, and since its scope is limited to the FedRAMP moderate baseline, we use the content referring to FedRAMP rev. 4 as a mere guideline, and reinforce the observation with further considerations. In addition to FedRAMP rev. 4, we also match the controls in C5 against the CCM, thus obtaining a complete comparison of the three standards. We highlight the controls missing from the matching with the CCM.

In the second step of our analysis, we select the most relevant controls based on their impact on the issues listed among CSA's Treacherous Twelve (T12). The twelve issues identified by CSA are matched over the CCM. Out of 133 controls in the matrix, 82 are connected with one or more issues and 51 are not. Matching the T12 with the three standards on the CCM, we obtain a direct reference to the impact of the three standards on the issues considered by CSA as prominent in cloud security.

In the third step, we draw conclusions from the quantitative (number of controls missing from the comparison) and qualitative (type of controls and controls domain missing) results of the first two steps. To better understand the impact of the missing controls in the face of the current threat landscape, we present an attack model considering the distribution of missing controls among the three standards.

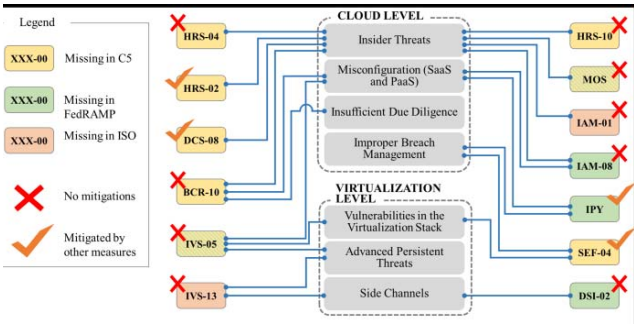

Figure 4: Attack Model. C5, FedRAMP, and ISO/IEC 27001

III. FINDINGS

The result of matching the controls in ISO/IEC 27001:2013, FedRAMP rev. 4 high baseline, and C5 on CSA CCM shows important quantitative differences (Figure 3). Looking to the total missing controls, BSI's C5 is the standard showing the highest number with 30 missing matches on the CCM, followed by FedRAMP, with 28, and ISO with 3. However, the number of controls missing in C5 drops to 18 if we exclude from the count those controls providing incomplete fulfillment of CCM controls or being fully adequate only when including additional requirements.

The gap between the three standards reduces considerably if we consider the relevance of the missing controls, measured in our second step on the basis of their impact on at least one of the T12. The introduction of this variable allows us to focus only on the most significant controls missing from the count.

After the selection, the fulfillment of 7 controls in CCM is missing in C5; 3 are partially covered by the standard or fulfilled implementing the additional requirements. The number of controls missing in FedRAMP drops drastically to 3, and ISO reduces the number from 3 to 2.

Interestingly, two entire control domains—accounting for a total of 25 controls—do not impact any of the T12. *Interoperability and Portability* (IPY), built on a total of 5 controls, counts 5 controls missing in FedRAMP; *Mobile Security* (MOS) counts the highest number of missing controls in C5 and FedRAMP (14 each). This consideration partially explains the drastic drop after the selection in the second step of our analysis. In addition, C5 does not cover 4 controls in the domain of *Human resources* (3 of which are relevant for the T12).

IV. DISCUSSION

The model we use for our analysis is built on two main blocks according to the origin of the attack: virtualization technologies or cloud provider. This is a reasonable approach as virtualization technologies introduce new attack vectors that must be considered in the standards creation process. Additionally, the standards must consider the second class of attacks stemming from the outsourcing of operations; these may or may not stem from the addition of new technologies, but must be considered nevertheless. Each level is subject to more than one threat. In the model, we define the threats created by the omission of controls and control domains in the three standards,

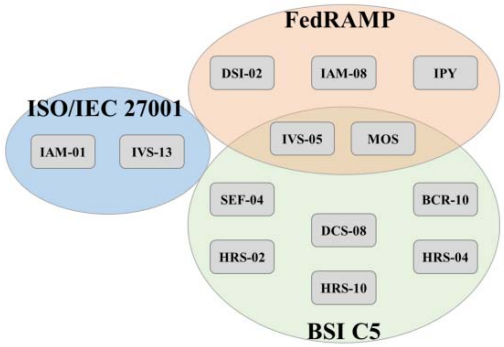

Figure 5: Distribution of missing controls in C5, FedRAMP, and ISO/IEC 27001

and we connect each threat with the control that is meant to protect against it (Figure 4). In building our attack model, we consider the missing controls included among the T12. Although MOS and IPY are two domains not impacted by the T12, we choose to include them in the analysis. We believe that their relevance should not be overlooked, and further considerations on their impact are necessary. The results of our analysis are presented in relation to the controls missing in each standard to conclude with the controls missing in FedRAMP and C5 (figure 5).

A. BSI C5

Six controls are omitted in C5. According to our attack model, the most recurring risks created by the omissions in C5 are at a cloud-level, and are insider threats.

The first control missing in C5 is named *Human Resources - User Responsibility* (HRS-10) and requires awareness of procedures and policies, supported by proper training to the CSP employees. Lacking training and information on internal procedures, employees could be the origin of unwanted security breaches and vulnerabilities regardless of employee intention. An example is the replacement of a password to access the personal workstation, compromised after an event known only by the employee, such as loss of a note where the password was written. Although considered secure according to general principles (e.g. the password is complex and has been regularly changed every 3 months), an employee not properly trained could still represent a threat for the CSP.

Two other controls relate to the maintenance of a security baseline in identity management. *Human Resources - Background Screening* (HRS-02) requires the background screening to be proportional to the sensitivity of information accessed in the system. The absence of this control can cause the employee to bypass access restrictions, thus generating a security flaw. Information with higher sensitivity requires the CSP to apply additional caution, and background checks might be useful to reveal personal conditions of the employee, such as conflict of interest, which may suggest restrictions on some of his or her access privileges. The security measures in C5 prescribe background screenings in the basic requirements, but adds the principle of proportionality, thus becoming fully compliant with HRS-02, only in the additional requirements.

Another omission leading to insider threats is that of *Datacenter Security - Unauthorized Persons Entry* (DCS-08), missing in C5. The standard fully mitigates the omission only by including the additional requirements. The control requires monitoring of service areas to prevent intruders from moving undetected within datacenters and processing facilities. C5 includes measures for access control, but isolation of service areas and data storage is missing, thus causing a possible security flaw.

In addition, *Human Resources - Employment Termination* (HRS-04) is another control missing in C5. It requires a clear definition of policies and procedures in case of termination or change of function of the CSP's employees. The omission might generate insider threats if, for example, an adjustment in access privileges does not follow a termination event or a change of function. Without that countermeasure, the subject can obtain unauthorized access to restricted information. The omission could eventually lead to a misconfiguration if, for instance, the employee does not transfer his or her knowledge to the person succeeding in the role, thus creating an information gap. However, that consideration only applies if documentation on the configuration of the systems is not adequately maintained by the CSP, and does not directly relate to the omission of HRS-04 among the security controls.

Similar considerations apply to the omission of *Business Continuity Management & Operational Resilience – Policy* (BCR-10) in C5. The control requires the creation of clear policies and procedures to guarantee appropriate IT governance and adequate training supporting the implementation of those policies. Although C5 includes the creation of governance policies among its requirements, what is missing is the detailed definition of roles, responsibilities, and training support, which is only offered to the employees for generic security aspects. In the same vein of HRS-04, the risks for this omission are insider threats, but also misconfigurations and insufficient due diligence. The difference between HRS-04 and BCR-10 is that the former refers to transferred or terminated employees, the latter refers to current employees. Misinformed employees, for example, could delay or fail in adequately responding to discovered vulnerabilities (insufficient due diligence), or be unaware of their responsibilities in that they should apply mandatory updates or changes to the system (misconfiguration).

The last control missing in C5 could generate two different threats: improper breach management, and vulnerabilities in the virtualization stack. That control is *Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation* (SEF-04). The absence of this control mostly impacts the transparency between CSP and the tenant and the possibility for the latter to take countermeasures in the event of a security incident. The absence of this control precludes the participation of the tenants in forensic procedures and might affect proper response to security breaches. In case of incident, failing to apply the required countermeasures leaves a vulnerability open, and potentially exploitable. Active participation of tenants in forensic procedures is precluded among the basic requirements in C5, but is contemplated in the additional requirements.

As result of our analysis on six controls missing in C5, four omissions can affect the CSP creating insider threats. Two of those controls (HRS-02, DCS-08) are mitigated by additional requirements in the standard. However, the additional requirements are not necessary to be C5 compliant and their absence cannot be overlooked. The absence of BCR-10 is particularly alarming, since it could lead to three different class of threats: insider threats, misconfigurations and insufficient due diligence. Last, SEF-04, only mitigated by the additional requirements, can lead to improper breach management and vulnerabilities in the virtualization stack.

B. FedRAMP

The second standard in our analysis is FedRAMP, which omits one individual control and an entire control domain protecting against vulnerabilities at the cloud level, and one control operating at the virtualization level.

The first control is *Identity & Access Management - Trusted Sources* (IAM-08), which requires the adoption of the least privilege rule to handle identity access information, and policies and procedures granting that the rule is applied. FedRAMP does not include this provision, and it could trigger vulnerabilities allowing for account hijacking, or the presence of malicious insiders [10]. Through the escalation of privileges, malicious attackers could obtain access to information or functions for which they are not authorized. We must notice that FedRAMP does not include controls from the Program Management section in NIST SP 800-53 (Appendix G), including potential countermeasures such as the creation of an insider threat handling team, that would reduce the impact of this vulnerability. At the same time, the absence of policies and procedures may result in easier misconfiguration of privilege rules. Although there is not a data loss or disclosure directly related to the misconfiguration, it still represents an exploitable vulnerability.

In addition, we notice the absence of controls in the *Interoperability and Portability* (IPY) domain from FedRAMP, which could be a possible source for misconfiguration, as well as generating improper breach management. In the event of a security breach, vendor lock-in may impede the tenant or the CSP to migrate their applications to different platforms, thus leaving the security flaw poorly managed, or making harder to patch existing applications due to proprietary software. The US Government, however, gives directions to Federal Agencies on the specific issue of interoperability and portability management through NIST SP 500-293, thus reducing the impact of the absence of this control domain from FedRAMP.

The omissions in FedRAMP could also facilitate "side channel" attacks, which leverage the shared infrastructure to target information belonging to co-hosted tenants [26][30][38][39]. One control is missing in FedRAMP that would be effective in prevention of that kind of attack. It is *Data Security & Information Lifecycle Management - Data Inventory/Flows* (DSI-02). Inferring information on the usage of the CPU in co-scheduled systems, an attacker can determine the nature of the information processed in the system by other tenants. Detailed documentation is thus important to allow the CSP to implement stronger security measures in high-risk environments. The purpose of DSI-02 is to assure full documentation of data flows in the system for the entire information lifecycle. Full documentation on data flows can help

the CSP to determine the usage of computing resources in the system, their distribution and schedule, thus helping to prevent side channel attacks.

In sum, the two controls missing in FedRAMP are relevant in protecting against two different threats: insider threats, and side channel attacks. The control domain missing in FedRAMP (IPY) mitigates the effect of misconfigurations and improper breach management. Its absence, however, is softened by federal regulations that oversee characteristics of products and services provided to the US Government in terms of interoperability and portability.

C. ISO/IEC 27001

ISO is the third standard, the last in number of controls missing from the CCM. Insider threats, advanced persistent threats, or side channel attacks are all threats deriving from the omissions of two controls.

ISO does not include protection as required in *Identity & Access Management, Audit Tools Access* (IAM-01). The control prescribes restriction in the access to and segregation of audit tools to prevent tampering of log data. The flaw can be exploited by an attacker in the aftermath of a security incident, for example, to remove or modify event logs, thus allowing the event to go undetected. In addition, ISO does not include security measures from the control in CCM named *Infrastructure & Virtualization Security, Network Architecture* (IVS-13). This control refers to the production of network architecture diagrams helping to identify high risk environments, and the implementation of defense-in-depth techniques against network-based attacks. There are two risks associated with the omission of that control. The absence of security measures, such as re-scheduling of processes, aimed at preventing co-hosted tenants from inferring information processed in the system, could open a vulnerability exploitable by side channel attacks. At the same time, the absence of IVS-13 could lead to overlooked advanced persistent threats (APT). A clear view of the CSP's network architecture is necessary but not sufficient if not supported by detailed analysis and the application of countermeasures [5][37]. ISO includes requirements for detailed documentation, but does not require specific measures in protection of high-risk environments, thus failing to cover the requirement in relation to side channel attacks and APT.

Of the two controls omitted in ISO, the absence of IAM-08 increases the chances of insider threats. The other missing control, IVS-13, could be effective to protect the virtualization level against ATP and side channel attacks.

D. Controls missing in two standards

Surprisingly, only one control relevant for the T12 is missing across multiple standards. The provisions in *Infrastructure & Virtualization Security - Vulnerability Management* (IVS-05) are not fulfilled in FedRAMP and C5. The control requires the security assessment service used by the CSP to accommodate the virtualization technology in use. The absence of virtualization awareness might cause vulnerabilities to go unnoticed [10], since application requirements are different in cloud environments, and the virtualization technology itself needs to be audited. Insufficient attention in detecting threats in cloud environments can easily let advanced persistent threats to go undiscovered, as well as other vulnerabilities in the virtualization stack that can cause perpetrators to target other tenants through the CSP [33] as well as obtaining direct access to data belonging to other tenants by escalating access privileges [23]. The absence of IVS-05 could also result in misconfigurations. If the results of the audit are misleading, changes that would be deemed necessary using virtualization aware tools could be ignored, and hence the correct configuration of cloud services be altered.

Although not considered determinant on the issues included among the T12, the absence of multiple controls from the domain of *Mobile Security* (MOS) in FedRAMP and C5 deserves specific attention. The possibility of targeting a CSP through its employees is directly connected to the ability of the CSP to implement high protection for the devices in use by the workforce, including mobile phones. Recent examples of attacks exploiting mobile devices are the "Stagefright" exploit, using MMS to infect other devices [17][31], or the exploitation of vulnerabilities in Android [32][21] to gain access to restricted network resources. Because Android is Linux based, then vulnerabilities such as the recent "DirtyCOW" may mean that exploited devices are on CSP premises [21]. FedRAMP and C5 show flaws in the determination of policies on admissibility and usage of devices belonging to the employees, and it can be source of vulnerabilities as a compromised device can be used as a vector for attacks to the CSP, creating insider threats.

The results of our analysis on controls and domains missing in C5 and FedRAMP suggest that the absence of one control could have consequences at a cloud level, causing misconfigurations, and at a virtualization level, being source of APT and vulnerabilities in the virtualization stack. The missing domain, that of mobile security, could generate or facilitate insider threats.

E. Additional Considerations on the Standards

C5 shows the highest number of omissions among the three standards. Still, for the great majority of the missing controls the consequences are insider threats, and the gaps are about documentation, training, and workforce monitoring. Not only are the omission in C5 treacherous by their own nature, but they could concur in facilitating a security incident. For example, the absence of proportional background checks to the workforce (HRS-02) could create an authorization gap. That can be amplified by the absence of segregation between environments, some of which are potentially hosting sensitive information (DCS-08). In addition, scarce security training on IT governance (BCR-10) might result in unattended devices in restricted areas, making them easily accessible to the intruder. Those factors could all contribute to a successful and disruptive attack by a malicious insider. In a different scenario, the absence of clear policies on reassignment of employees to different roles (HRS-04), and the absence of adequate training on responsibilities and security in the workplace (BCR-10) may result in unawareness and lack of preparation of the employees in case of a security incident, thus making the CSP unable to provide a timely response and minimize the consequences of the incident.

FedRAMP shows similar weaknesses, especially if an attack is driven through the CSP's workforce. The absence of clear

policies on mobile security, associated with loose controls on insider threats, and the possibility of escalating privileges to access confidential information, all create the ideal ground for external attackers targeting the workforce, which represents the weaker link of the security chain. Although FedRAMP prescribes a baseline security training to CSP's employees, the existence of exploitable weaknesses having workers as the object of the attack questions whether the current training is sufficient to guarantee information security.

Last, although insider threats represent a vulnerability in ISO for unsecure access to audit tools, the critical aspect does not relate to prevention, but rather to the response in case of security incidents. Scarce reactiveness to security events could represent a problem in attacks at the virtualization level, such as APT or side channel attacks. Although ISO requires complete documentation on system architecture, data flows, policies, and procedures, its response to incidents and defense techniques needs to be clarified. The consequence of that defect is that, once an attack results successful against an ISO certified CSP, the threat agent can act undisturbed for prolonged periods of time.

V. Conclusion and Future Work

The need for a strong security baseline for cloud services has pushed governments and stakeholders to create new certification frameworks, trying to tackle cloud security issues and vulnerabilities in recent years. FedRAMP, issued in 2011 by the US Government and reinforced with a high baseline in 2016, and C5, issued by the German Government in 2016, are two example of new frameworks. Both aim to improve security standards in cloud environments by leveraging on third party assessments and a checklist of stringent controls. FedRAMP and C5, however, share their intent with existing, older standards. One example is the ISO/IEC 27001, first issued in 2005 and updated in 2013, with which they concur in the attestation of CSP security.

In our study, we have compared the three standards with the support of a third-party framework to shed light on the necessity of a new standard to define cloud security requirements. We have analyzed the most security-sensitive measures missing in the three standards organizing them in an attack model. We have determined that the absence of a single control could generate multiple threats, exposing security gaps in the three standards.

We have obtained important results highlighting the insufficiency of all of the three standards to completely guarantee cloud security by our analytical framework. ISO, however, has shown best performances when compared to the other two. The complementarity of the three standards stands out: only one of the controls impacting the T12 is missing in more than one standard, whereas the other ten are distributed among ISO, FedRAMP, and C5.

Insider threats represent the most important class of threats stemming from the omissions of the three standards. Higher attention to training and definition of security policies managing the workforce are required to improve the answer of C5 and FedRAMP to current security needs in cloud environments. Conversely, ISO lacks of responsiveness in the event of a security incident, thus requiring improvements in detection of threats and their removal.

Future research could expand the research to other industry and government standards, thus offering a more comprehensive view on complementarity and adequacy of existing standards. More attention could be given to controls not belonging to the list of T12, thus expanding the gap analysis and the analysis on the adequacy of the standards as a consequence. A more specific analysis of threats stemming from the absence of controls in the analyzed security frameworks could help gauge the attack surface of each standard, suggesting further improvements and integrations.

Acknowledgment

This material is based on research sponsored by the Air Force Research Laboratory and the Air Force Office of Scientific Research, under agreement number FA8750-11-2-0084. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

References

[1] Adobe. 2015. Adobe Security and Privacy Certifications. White Paper. Adobe Systems Incorporated. Accessed June 1, 2016. http://www.adobe.com/security.html

[2] Ardagna, C.A., Asal, R., Damiani, E., Vu, Q.H. 2015. From Security to Assurance in the Cloud: A Survey. ACM Computing Surveys. 48:1. Article 2.

[3] Bayuk, J. (2011). The Utility of Security Standards. IEEE International Carnahan Conference on Security Technology (ICCST), 2010. 341-345

[4] – – –. (2011). System Security Engineering. IEEE Security & Privacy. (9) 72-74

[5] Brewer, R. 2014. Advanced persistent threats: minimising the damage, Network Security, Volume 2014, Issue 4, April 2014, Pages 5-9, ISSN 1353-4858

[6] – – –. (2015). Cloud Security Metrics. Proc. of the 2011 6th International Conference on System of Systems Engineering, Albuquerque, New Mexico, USA.

[7] Beckers, K., Côté, I., Faßbender, S., Heisel, M., Hofbauer, S. 2013. A pattern-based method for establishing a cloud-specific information security management system. Establishing information security management systems or cloud considering security, privacy, and legal compliance. In Requirements Engineering for Security, Privacy & Services in Cloud Environments. 18. Springer. P. 343-395

[8] Cloud Security Alliance (CSA). 2010. Top Threats to Cloud Computing V1.0. Accessed May 23, 2016. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[9] – – –. 2013. The Notorious Nine Cloud Computing Top Threats in 2013. Accessed May 24, 2016. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[10] – – –. 2016. 'The Treacherous Twelve' Cloud Computing Top Threats in 2016. Accessed May 23, 2016. https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/

[11] – – –. CSA STAR: The Future of Cloud Trust and Assurance. Web page. Accessed May 31, 2016. https://cloudsecurityalliance.org/star/

[12] – – –. FedRAMP Cloud Controls Matrix v3.0.1 Candidate Mapping. Accessed June 1, 2016. https://cloudsecurityalliance.org/download/fedramp-cloud-controls-matrix-v3-0-1-candidate-mapping/

[13] – – –. Introduction to the Cloud Control Matrix Working Group. Web page. Accessed May 21, 2016. https://cloudsecurityalliance.org/group/cloud-controls-matrix/

[14] Cloud Standards Customer Council. 2013. Cloud Security Standards: What to Expect & What to Negotiate. Accessed May 23, 2016. http://www.cloud-council.org/resource-hub.htm

[15] Creese, S., Goldsmith, M., Hopkins, P. 2013. Inadequacies of Current Risk Controls for the Cloud. In Privacy and Security for Cloud Computing. Springer. P. 235-255

[16] Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R., Bashir, M. 2017 (Forthcoming). Cloud Security Certifications: A Comparison to Improve Cloud Service Provider Security. Paper Accepted to the 2nd International Conference on Internet of Things, Data and Cloud Computing (ICC 2017), Churchill College, Cambridge, UK. March 22-23, 2017.

[17] Drake, J. 2015. Stagefright: Scary Code in the Heart of Android. Researching Android Multimedia Framework Security. PPT Presentation. Black Hat USA, 2015. Accessed October 15, 2016. https://www.blackhat.com/docs/us-15/materials/us-15-Drake-Stagefright-Scary-Code-In-The-Heart-Of-Android.pdf

[18] Fernandez, D.A.B., Soares, L.F.B., Gomes, J.V., Freire, M.M., Inácio, P.R.M. 2014. Security Issues in Cloud Environments: A Survey. In International Journal of Information Security. 13. Springer. P. 113-170

[19] Gikas, C. 2010. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Information Security Journal: A Global Perspective. 19. 132–141.

[20] Gleeson, N., Walden, I. 2014. 'It's a jungle out there'?: Cloud computing, standards and the law. European Journal of Law and Technology. 5:2. 1-22.

[21] Goodin, D. 2016. Android phones rooted by "most serious" Linux escalation bug ever. *ArsTecnica.* Accessed October 28, 2016. http://arstechnica.com/security/2016/10/android-phones-rooted-by-most-serious-linux-escalation-bug-ever/

[22] Goodin, D. Google confirms critical Android crypto flaw used in $5,700 Bitcoin heist. 2013. Accessed June 8, 2016. http://arstechnica.com/security/2013/08/google-confirms-critical-android-crypto-flaw-used-in-5700-bitcoin-heist/

[23] Goodin, D. Xen Patches 7-Year-Old Bug That Shattered Hypervisor Security. 2015. Accessed October 9, 2016. http://arstechnica.com/security/2015/10/xen-patches-7-year-old-bug-that-shattered-hypervisor-security/

[24] Hendre, A., Joshi, K. P. 2015. A semantic approach to cloud security and compliance. Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015, 1081-1084

[25] Huang, W., Ganjali, A., Kim, B.H., Oh, S., Lie, D. 2015. The State of Public Infrastructure-as-a-Service Cloud Security. ACM Computing Surveys. 47:4. Article 68.

[26] Inci, M. S., Gulmezoglu, B., Irazoqui, G., Eisenbarth, T., Sunar, B. (2015). Seriously, get off my cloud! Cross-VM RSA Key Recovery in a Public Cloud. Cryptology ePrint Archive, Report 2015/898. Accessed October 9, 2016 http://ia.cr/2015/898

[27] ISO. 2013. New version of ISO/IEC 27001 to better tackle IT security risks. Accessed May 29, 2016. http://www.iso.org/iso/news.htm?refid=Ref1767

[28] Lamps, J. Palmer, I., Sprabery, R. 2014. WinWizard: Expanding Xen with a LibVMI Intrusion Detection Tool. 2014 IEEE 7th International Conference on Cloud Computing.

[29] Kundra, V. 2011. Federal Cloud Computing Strategy. Accessed May 27, 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

[30] Liu, F., Yarom, Y., Ge, Q., Heiser, G., Lee, R. B. 2015. Last-Level Cache Side-Channel Attacks Are Practical. 2015 IEEE Symposium on Security and Privacy. 605-622.

[31] MITRE. 2015.CVE-2015-1538. Common Vulnerabilities and Exposures. Online database. Accessed October 15, 2016. http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2015-1538

[32] Office of Management and Budget. 2016. *Strengthening Federal Cybersecurity. Meeting Our Greatest Challenges: The President's Fiscal Year 2017 Budget.* Fact Sheet. Last accessed May 31, 2016. https://obamawhitehouse.archives.gov/omb/budget/key-issue-fact-sheets

[33] Ormandy, T. 2007. An Empirical Study into the Security Exposure to Host of Hostile Virtualized Environments. http://taviso.decsystem.org/virtsec.pdf

[34] Perception Point. Analysis and Exploitation of a Linux Kernel Vulnerability (CVE-2016-0728). Accessed June 8, 2016. http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/

[35] Rasheed, H. 2014. Data and Infrastructure Security Auditing in Cloud Computing Environments. In International Journal of Information Management. 34. Elsevier. P. 364-368

[36] Sunyaev, A., Schneider, S. 2013. Cloud Services Certification. How to address the lack of transparency, trust, and acceptance in cloud services. In Communications of the ACM. February 2013. 56:2. 33-36.

[37] Virvilis, N., Gritzalis, D. 2013. The big four - What we did wrong in advanced persistent threat detection? Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013, art. no. 6657248, pp. 248-254.

[38] Zhang, Y., Juels, A., Reiter, M. K., Ristenpart, T. (2012). Cross-VM Side Channels and Their Use to Extract Private Keys. In CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security. ACM New York, NY. 305-316

[39] – – –. (2014). Cross-Tenant Side-Channel Attacks in PaaS Clouds. In CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM New York, NY. 990-1003