2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

IT Security and Privacy Standards in Comparison

Improving FedRAMP Authorization for Cloud Service Providers

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*—To demonstrate compliance with privacy and security principles, information technology (IT) service providers often rely on security standards and certifications. However, the appearance of new service models such as cloud computing has brought new threats to information assurance, weakening the protection that existing standards can provide.**

In this study, we analyze four highly regarded IT security standards used to assess, improve, and demonstrate information systems assurance and cloud security. ISO/IEC 27001, SOC 2, C5, and FedRAMP are standards adopted worldwide and constantly updated and improved since the first release of ISO in 2005. We examine their adequacy in addressing current threats to cloud security, and provide an overview of the evolution over the years of their ability to cope with threats and vulnerabilities. By comparing the standards alongside each other, we investigate their complementarity, their redundancies, and the level of protection they offer to information stored in cloud systems. We unveil vulnerabilities left unaddressed in the four frameworks, thus questioning the necessity of multiple standards to assess cloud assurance. We suggest necessary improvements to meet the security requirements made indispensable by the current threat landscape.

Keywords-FedRAMP; ISO; SOC; C5; Certification; Standard; Framework; Cloud; Privacy; Security.

I. INTRODUCTION

The adoption of cloud technology in the last decade has represented a great innovation in the information technology (IT) industry. Access to virtually unlimited and scalable resources has revolutionized IT service offering, and the best practices in IT management for vendors (cloud service providers, or *CSPs*) and clients (*tenants*). However, with the creation of new service models, new vulnerabilities have made their appearance, creating new threats to information assurance. As the growth of cloud investments does not show any sign of slowing down[1], threats and vulnerabilities are becoming an increasing concern among IT specialists.

Approved for Public Release; Distribution Unlimited: 88ABW-2017-0523, Dated 08 Feb 2017

To reassure tenants on the level of security guaranteed by their clouds, CSPs often use certifications or attestations resulting from trusted third parties' extensive audits of their systems and internal procedures. When standards are not adopted on a voluntary basis, governments could impose required standards on CSPs that host particularly sensitive information, to guarantee a certain security baseline.

Compliance with a standard alone, however, might not be enough. If the requirements and technical controls in a standard are not up to date and capable of dealing adequately with newer threats and vulnerabilities, the system being certified could still have undetected flaws, even at the end of a detailed assessment. Thus, the efficacy of a standard in guaranteeing cloud assurance cannot be judged based simply on the depth of the assessment it requires or on the detail with which the controls are explained, but rather on its adequacy to cope with cloud-specific threats.

Among the standards available for attesting cloud assurance, ISO/IEC 27001 (henceforth also referred to as "ISO") and SOC 2 are among the most commonly used. ISO defines requirements for "Information technology - Security techniques – Information security management systems." Its first release, from 2005, was reviewed in 2013 to include protection against new threats and keep pace with newer technologies [24]. ISO has a general scope, being focused on IT service security regardless of the deployment model (e.g., in the cloud or on-premises). There are more than 27,000 ISO certifications worldwide, of which more than 1,200 are in the United States [28]. ISO is built on a set of controls that are organized in different "families" that guide auditors in performing assessments of CSP systems. Like ISO, SOC 2 was not conceived specifically for cloud assurance. It derives from SAS 70 reports by the American Institute of Certified Public Accountants (AICPA), which were designed to support the examination of organizations' financial statements. The widespread use of those reports' findings in the assessment of IT systems, however, pushed AICPA to

[1] According to Gartner [23], investments in public cloud services grew 17.2% from 2015 to 2016, such that by the end of 2016 they accounted for 43% of worldwide investments in Infrastructure as a Service (IaaS).

978-1-5090-6611-7/17 $31.00 © 2017 IEEE
DOI 10.1109/CCGRID.2017.137

release a new set of standards, including SOC 2, to assess security and privacy measures in service organizations [1]. Audits performed in accordance with SOC 2 guidelines are based on the Trust Services Principles and Criteria (TSPC), which were also issued by the AICPA. Specifically, SOC 2, first adopted in 2011, is based on the TSPC issued in 2009. The TSPC were updated in 2014, at which time the principles and criteria were reorganized into more organic categories, and then again in 2016, when a dedicated section on privacy criteria was added.

Two other standards have been created specifically for attesting cloud assurance. These are the Federal Risk Authorization Management Program (FedRAMP) and the Cloud Computing Compliance Control Catalogue (C5). Any CSP that provides cloud services to federal agencies is required to have a FedRAMP Authorization to Operate (ATO). FedRAMP is based on a selection of controls from NIST Special Publication (SP) 800-53, organized in three tiers: low, medium, and high. The first two tiers have been part of FedRAMP since its first release in 2012. Its controls were updated after it was reviewed in 2015, following an update of NIST SP 800-53. FedRAMP's "high" baseline was created in July 2016, and improved the program with controls for systems processing data with higher sensitivity. A total of 77 systems in the US are FedRAMP authorized, 4 of which have obtained ATOs corresponding to the "high" tier [17]. C5 was issued in February 2016 by the Bundesamt für Sicherheit in der Informationstechnik (or *BSI*, the German Information Security Office). It is organized as a set of basic criteria and a more detailed group of additional requirements. The standard was conceived as a guideline that CSPs could use to improve their cloud systems, and can be used either as a complement to existing certifications, or as a standalone framework to assess cloud assurance.[2]

ISO, SOC 2, FedRAMP, and C5 made their appearance over a span of eleven years, and the older certifications have remained widely used in spite of the appearance of newer ones. The creation of new certifications often puts an additional burden on CSPs, if they are required by law to be certified (as with FedRAMP) to provide their services. But even when a certification is not required, it can still offer CSPs value as a mechanism for demonstrating their attention to information assurance, and serve as a marketing tool to promote their services,[3] thus pushing the CSPs to achieve multiple certifications at the same time.

The existence of multiple standards, all updated over the years and aimed at guaranteeing information security, raises the question of whether there is any need to have different frameworks aimed at the same goal. Are there differences in their function and focus? What is the purpose of creating new certifications such as FedRAMP if frameworks such as ISO already exist and have been widely adopted around the world?

To understand the reasons for their coexistence and explain their functions, we need to understand their complementarity, their redundancies, and what protection they offer against cloud-specific threats and vulnerabilities. In this paper, we offer a detailed review of ISO, FedRAMP, SOC 2, and C5, comparing them to unveil their fallacies and weaknesses and, ultimately, to address their adequacy to promote information assurance in cloud environments. We identify their overlaps and the gaps between them. We suggest improvements for the standards and integrations necessary to guarantee cloud assurance.

Our conclusions aim to improve the effectiveness of future versions of these frameworks and help CSPs and their tenants understand their differences, strengths, and weaknesses.

A. Previous Work

The study of IT security standards has flourished in recent years in the form of guidelines on the adoption of specific frameworks [5][6][35][43][37] or comparisons of multiple standards [7][14][19][20][24][42]. However, these studies have often been based on outdated versions of standards (such as ISO/IEC 27001:2005) or provided only general guidelines for the adoption of security frameworks. Most of these studies have been limited to a comparison of general features found in different frameworks, and did not consider their controls, their omissions, or how they complement or overlap each other. Even when overlaps and gaps have been specifically considered [1], there has not been in-depth explanation of the limitations and shortcomings. The Cloud Security Alliance (CSA), on the other hand, has done more detailed work. Since 2008, CSA has consistently worked on structured observation of IT security standards [12], including the most recent version of FedRAMP in 2015 [11], and has even created its own certification scheme, called the Security, Trust, and Assurance Registry (STAR) [7]. The STAR certification is based on a proprietary set of controls listed in the Cloud Control Matrix (CCM). The matrix is built on cloud-specific controls organized in control families. In parallel to its study of standards, CSA has also worked extensively on threats and vulnerabilities in cloud security. Three studies [7][8][9] published in 2010, 2013, 2016 address the most critical vulnerabilities in cloud environments, listed in order of relevance according to surveys of IT experts. Notably, CSA studies of threats are strongly connected with the CCM. Each of the studies has a reference to controls in the CCM that can provide enhanced protection against specific threats in the list, thus creating a direct correlation between controls and vulnerabilities. CSA, however, does not go beyond listing the controls in the CCM, and does not explain the cloud assurance consequences of lacking one control or another. Similarly, the large body of literature exploring threats and vulnerabilities in cloud environments is missing a direct

[2] For the purpose of this study, we refer to "certification" as the result of a detailed third party assessment. SOC 2 and C5, however, are respectively referred to as reporting standard or guideline. Not resulting in a certification, comprehensive data on their adoption by CSPs are not available.

[3] Nickell and Denyer [38] refer to the marketing function as one of the misuses of SAS70 that led the AICPA to create the SOC reports.

reference to IT security standards. Part of the literature builds on classification of threats in cloud environments [4][18], while numerous other studies explore the characteristics of selected attacks in the three main cloud service models (IaaS, PaaS, and SaaS) [24][25][33][44]. Studies on threats will be critical to improving existing security measures. However, without reference to applicable controls or a connection to existing frameworks, it will be harder to improve existing standards, and raise and update their baseline protection.

B. Our Contribution

Previous work on cloud assurance has contributed to the understanding of threats and security issues in cloud environments, either by collecting and ranking existing threats, or by deepening the analysis of specific threats, showing how they can endanger information residing in clouds. Those studies, however, lack a direct connection with IT security standards, so they have made only a limited contribution to the creation of baseline controls. At the same time, existing studies of IT security standards have also been limited by the release of newer versions of the analyzed frameworks, resulting in outdated findings, or by their lack of detail in dissecting standards, failing to address particular controls and their functions. Previous research has demonstrated differences in the impact of FedRAMP and ISO on cloud assurance [15]. However, that study was limited to establishing the effectiveness of the two standards, rather than relating them to the current security standards landscape.

Our work concentrates on four of the most relevant standards used to build and maintain cloud assurance, namely FedRAMP, C5, SOC 2, and ISO/IEC 27001. We consider their evolution over time, and concentrate on the most recent available version of each. We analyze their benefits and limitations by looking at the controls required in each framework; we measure their complementarity and assess the overlaps; and we gauge the effectiveness and adequacy of each standard in protecting against current threats and vulnerabilities.

II. Methodology

All four of the standards in our study are based on controls organized in groups or "families." However, not all the standards are built on extensive documents that explain the controls. FedRAMP, for instance, refers to a selection of controls in NIST SP 800-53. We limit our observation to the controls relevant for each version of FedRAMP (2012 and 2015), and to the highest security level common to the two releases. The FedRAMP high baseline was released only in 2016, and hence cannot be found in 2012. Therefore, we limit the comparison to controls included in the medium baseline. SOC 2 is based on TSPC. Although the TSPC were first published in 2006, the first version referenced in SOC 2 was from 2009. We also include observations on the two most recent reviews, in 2014 and 2016. C5 is organized in two levels: a set of basic requirements, and a set of additional requirements. Since implementation of the basic requirements is sufficient to be compliant with the standard, we draw our numerical data from observation of the basic requirements.

Our study has three steps. First, we collected the controls in the standards and compared them against a third-party framework, the CSA CCM. The CCM offers the advantages of being focused on cloud security and being easily comparable with the other standards because of its structure, which is based on controls and control families.

Second, we analyze the differences in the numbers of controls from the CCM that are omitted in each of the four standards. That allows us to build a quantitative comparison among the standards, highlighting their shortcomings. We compare all the available versions of the standards to obtain an historical perspective on their adequacy in addressing cloud security.

In the third and last step, we narrow down the analysis to the most relevant controls, selected from those having a direct impact on the particularly critical risks the CSA identified as the "treacherous twelve" [9] (henceforth referred as T12). In this step we focus our observation on the most recent version of each framework, explaining in detail the impact of each omission relevant for cloud assurance.

III. Findings

In this section, we detail the mismatches, and their evolution over time, in the mappings between the available versions of FedRAMP, ISO/IEC 27001, and TSPC on the CCM. C5, released in March 2016, is observed in its only available version in comparison with the most recent publications of the other three standards.

The three versions of TSPC, published in 2009, 2014, and 2016, show 43, 47, and 39 omissions, respectively, out of 133 controls in the matrix. In proposing its own matching over the CCM, CSA presents 48 controls omitted in TSPC 2014. However, the control *Identity & Access Management, Credential Lifecycle/Provision Management* (IAM-02), which prescribes adequate identity management policies, is in our opinion satisfied in TSPC 2014 and identical controls in TSPC 2016 (Section CC5 of the two frameworks). FedRAMP rev. 3, released in 2012, shows 45 omissions. In contrast, the CSA's matching claims that there are only 44 omissions in total. However, after a careful review, we believe that the CSA was mistaken in concluding that the control *Data Security & Information Lifecycle, Data Inventory/Flows* (DSI-02) is fulfilled by FedRAMP rev. 3. In our observation, the control signaled as adequate in FedRAMP, titled "Virtualization Techniques" (SC-30), does not relate to DSI-02.

Compared to its older version, the 2015 release 4 of FedRAMP shows a significant improvement. However, it still omits 30 controls from the CCM. ISO/IEC 27001 satisfies all but 43 and 3 controls in its 2005 and 2013 releases, respectively (Figure 1).

C5, although building on the ISO certification and TSPC to define its own set of criteria, shows as many as 30 omitted controls across multiple control domains.

Interestingly, two control domains are completely or substantially omitted in most of the frameworks we analyzed. The first domain is *Mobile Security* (MOS).

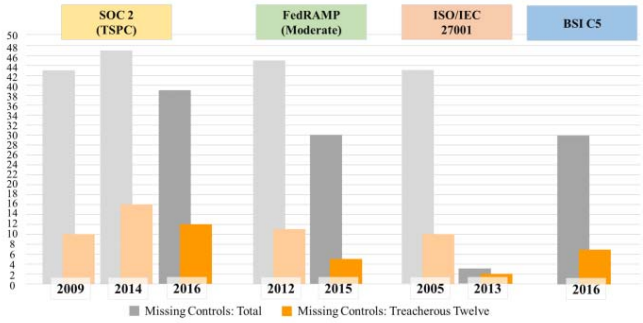

Figure 1: Missing controls and T12 selection

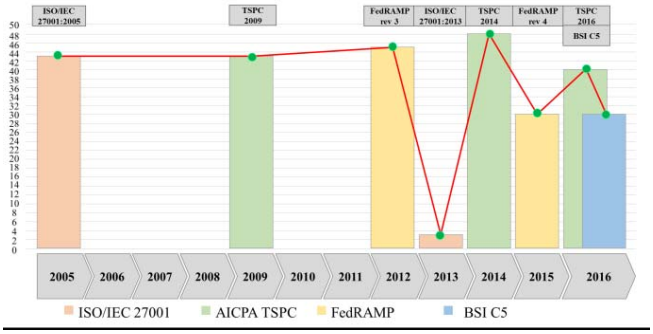

Figure 2: Evolution of omissions in a timeline

ISO/IEC 27001:2013 is the only framework that addresses it in its entirety. The 2015 release of FedRAMP and C5 satisfy only six out of twenty controls from that domain. None of the other frameworks include measures from MOS. The second domain is *Interoperability and Portability* (IPY). ISO/IEC 27001:2013 includes all the controls from that domain, and C5 omits only one control. None of the other frameworks include any of the controls from IPY.

In the control domain *Supply Chain Management, Transparency and Accountability* (STA), the referred frameworks show significant gaps, except for ISO/IEC 27001:2013 and C5, which cover all security requirements, and TSPC 2016, which omits only 2 of them.

The number of gaps and omissions indicated thus far, however, is substantially reduced if we consider the relevance of the omitted controls according to their impact on at least one of the T12. We can thereby focus on the most significant controls to obtain a more realistic view of the impact of each framework in terms of the security and privacy of information hosted in the cloud.

Once we apply that selection, the average drop in the number of omitted controls is close to 68%, with a peak of nearly 83% for FedRAMP rev. 4, which goes from 29 omitted controls to only 5. ISO/IEC 27001:2013 registers the lowest decrease, 33%, in going from 3 to 2 omitted controls. ISO/IEC 27001:2005 and FedRAMP rev. 3, with a drop of slightly more than 75%, still omit 10 and 11 controls respectively. FedRAMP and ISO show lower numbers of omitted controls in their newer versions. TSPC, on the contrary, show a fluctuation suggesting that the older version (from 2009) offers better protection than the newer ones. The TSPC from 2009, 2014, and 2016 omit 10, 16, and 12 controls, respectively. C5 shows an almost 76% decrease, dropping the number of omitted controls from 30 to 7.

When we focus on the controls relevant for the T12, the absence of controls in the MOS and IPY domains largely accounts for the drop in numbers of missing controls. The same absence justifies the limited variation in ISO/IEC 27001:2013 that covers both domains.

Last, if we narrow our observations to the most recent version of each framework, there is an absence of significant overlap among all four standards with respect to the omitted controls that concern T12. Certainly, the small number of omissions in ISO (2 controls) reduces the possibility of overlap. However, if we limit the observation to TSPC, FedRAMP, and C5, we find that only one control is missing in the area of virtualization security. Two controls are missing in both TSPC and FedRAMP in the area of virtualization security and information lifecycle management. One control is missing in both ISO and TSPC in the area of virtualization security.

IV. Discussion

Observing the results of our analysis, we notice how the different versions of the four frameworks have been released at different times, with different frequencies, over the span of eleven years since 2005 (Figure 2). In its first issue, ISO/IEC 27001, the first of the four to be published, shows results comparable to those of all the other standards. While at first we found 43 omitted controls, when we narrowed the selection based on the T12, the number went down by over 75%. The improvement between the first and last versions of ISO is particularly noticeable, ending in a total of only 3 omitted controls. This improvement must be attributed primarily to the inclusion of controls on mobile security and interoperability, which help fulfill the requirements in the MOS and IPY domains, with a combined total of 25 controls. The same improvement cannot be seen in the other standards, which are unable to cover the mentioned control domains thoroughly, even in their newest versions. At the same time, the newness of a standard does not necessarily play a role in the reduction of omitted controls and improvement of coverage against threats and vulnerabilities. While ISO is a clear example of improvement over time, and FedRAMP also shows good progress, the TSPC are an exception. In the same vein, the introduction of C5 in 2016 did not bring a drastic improvement, especially compared to the progress made three years earlier with the revision of ISO.

A good improvement in TSPC can be found in the transition between the 2014 and 2016 versions by looking at both the total omitted controls and only the ones relevant to T12. AICPA introduced a new set of privacy criteria in the last release, thus providing a more accurate set of criteria and controls. What is startling, however, is the regression of TSPC from 2009 to 2014, and how the improvement with the 2016 publication was not enough to restore the good performance of the 2009 version, especially with respect to the T12-relevant controls (12 missing in 2016, versus 10 in

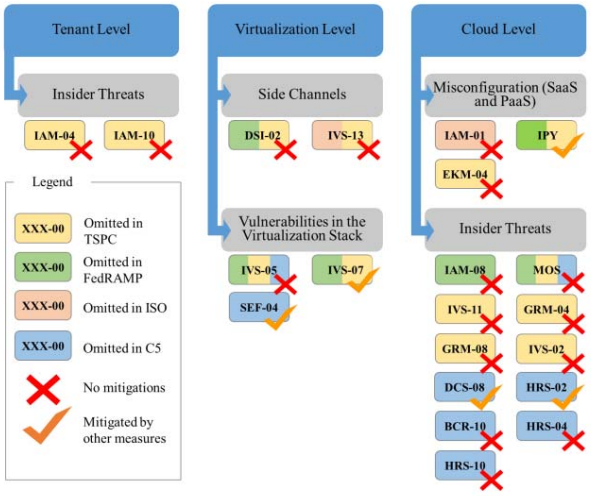

Figure 3: Attack Model. C5, TSPC, FedRAMP, and ISO/IEC 27001

2009). The reason might be the radical reorganization of the framework in its 2014 release, which made the content of the criteria more general and abandoned well-defined details that had matched the controls in the CCM.

If we narrow down the observation to the current version of each framework, and focus our attention on the most relevant security issues with respect to the T12 selection criteria, we isolate nineteen controls in the CCM that are not addressed by any of the frameworks. Two controls are omitted in TSPC, FedRAMP, and C5; two controls are omitted in TSPC and FedRAMP; and one is omitted in TSPC and ISO. As noted earlier, two control domains, MOS and IPY, although not considered relevant for the T12, are missing or considerably affected by omissions in C5, TSPC, and FedRAMP. As we consider the controls in MOS and IPY extremely relevant for information assurance, in spite of their absence among the controls involved in the T12 selection, we include consideration of their omission in our detailed analysis.

Our threat model accounts for the omitted controls and organizes them according to the vulnerabilities they may generate in cloud environments. At a higher level, three main possible sources of the threat specify the level at which the attack can be perpetrated: tenant, virtualization, or cloud. At a lower level, omitted controls are distributed according to the threat they are meant to restrain (Figure 3).

A. Hardware-Level Attacks

The first group of attacks is perpetrated through traditional vectors. In this category, an attacker can target information processed and stored in cloud environments or through on-premises hardware and software with no distinction. An example is unauthorized physical access into a data center hosting confidential information. The attacker acts directly on the hardware components of the system regardless of the service model (cloud or non-cloud). Other than physical security, threats belonging to this class typically stem from software vulnerabilities of single virtual machines (VMs), thus falling under the responsibility of the tenant. An example is security measures offered by vendors, including, but not limited to, malware detection to improve security of the single VMs. Although these measures are the subject of an extensive body of work [29][30][31][33][38], such work has not achieved sufficient stability to be included as part of a standard. For that reason, we chose not to consider this area of study in our research. Identity management is another problem. Two controls omitted in TSPC are *Identity & Access Management, Policies and Procedures* (IAM-4), and *Identity & Access Management, User Access Reviews* (IAM-10). These controls may facilitate the circumvention of access privileges, thus generating a flaw. The two controls oversee the management of tenants' identities used to authenticate to the cloud services, in terms of their storage, attribution, and updates of access privileges associated with them. One of the possible consequences could be the exploitation of misattributed access privileges by a tenant's employee—thus, insider threats—to obtain unauthorized access to data stored in the cloud.

B. Virtualization-Level Attacks

In the second group, we find attacks perpetrated at the virtualization level. An example is attacks that leverage sharing of infrastructure to access or infer information belonging to other co-hosted tenants. "Side-channel" attacks are one instance in which, in spite of lacking direct access to (or authorization to access) information being processed in the system, an attacker could infer that same information by analyzing the CPU usage of the system by other tenants [24][34][42][45]. To protect against such attacks and adopt effective countermeasures, a CSP must be aware of the information flows within the system, and thus be able, for instance, to identify recurrent traffic patterns and reschedule some activities to mitigate peaks in usage and consequently reduce the risk of undesired detection of particular activities. At the same time, the identification, documentation, and analysis of data flows allow the CSP to identify high-risk environments where more specific countermeasures can be applied. These security procedures are specified in two controls omitted in TSPC. One of them is also missing in ISO, and the other in FedRAMP. *Data Security & Information Lifecycle Management - Data Inventory/Flows* (DSI-02), omitted in FedRAMP and TSPC, requires the CSP to document data flows in the system for the entire information lifecycle. The control omitted in ISO and TSPC is *Infrastructure & Virtualization Security, Network Architecture* (IVS-13), which refers to the adoption of defense-in-depth techniques against network-based attacks. The absence of these two controls in ISO and FedRAMP reflects the nature of the two standards, with ISO being more oriented towards integrity of procedures and processes, while FedRAMP is more detailed in the use of technical measures to assure information confidentiality, integrity, and availability. Conversely, TSPC misses both aspects and does not include either documentation or technical measures, thus opening up important vulnerabilities.

Side-channel attacks directly target a co-hosted fellow tenant, but are not based on direct access to third-party information; rather, the exploitation of vulnerabilities in the virtualization stack allow an attacker to gain direct access to information belonging to other tenants. Information can be obtained through a direct attack on the CSP, as in the case of APTs [17], or escalation of access privileges [39]. Of the controls in the CCM, three would mitigate those vulnerabilities. *Infrastructure & Virtualization Security, Vulnerability Management* (IVS-05), which is missing in C5, TSPC, and FedRAMP, requires virtualization awareness of the assessment tools used by the CSP. Since the application requirements in cloud environments are different from those in non-virtualized systems and the virtualization technology itself needs to be audited, virtualization awareness is necessary to guarantee detection of existing vulnerabilities [5]. The second control, which is missing from FedRAMP and TSPC, must be read in context, and applied on a case-by-case basis; it is *Infrastructure & Virtualization Security OS Hardening and Base Controls* (IVS-07), which requires the implementation of technical controls and hardening techniques to protect each operating system. It can be seen as mainly a concern of the tenant, in that the provider maintains responsibility only for guaranteeing a security baseline, including a range of tools and applications to allow the tenant to meet the security requirement. However, in specific situations, the implementation of the control could be fully the responsibility of the provider, rather than the tenant. For example, that would be the case if PaaS applications were used to manage computing resources automatically, independent of the code supplied by the tenant [1]. If the tenant is held responsible, the omission of such a control in FedRAMP is mitigated by other federal measures (external to FedRAMP), such as the Federal Information Security Management Act (FISMA). FISMA requirements, which are generally applicable to federal information systems, also apply to external cloud services and the operating systems used in cloud environments. TSPC, however, were not designed specifically for federal agencies, and their shortcomings are not necessarily mitigated by complementary FISMA requirements. If there is a SOC 2 audit based on TSPC, a more careful evaluation of the distribution of responsibilities, and of the measures implemented to maximize security of the VM hosted on the cloud, must be done.

The last control in this first class, which is omitted only in C5, is *Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation* (SEF-04). This control relates to forensic analysis after a security incident, and requires the involvement and participation of the victimized tenant. The main impact of this control is on the transparency of the CSP towards tenants, enabling them to take adequate countermeasures when a security incident occurs. This requirement is not among the basic controls in C5, but other requirements in the standard compensate for its absence.

C. Cloud-Level Attacks

Two classes of vulnerabilities are part of the last group of threats in our model: SaaS and PaaS misconfigurations, and insider threats.

The class of SaaS and PaaS misconfigurations includes configuration flaws exploitable by an attacker to gain access to information stored in the cloud, bypass existing security measures, or remove the signs of an attack to remain undetected by the CSP. *Identity & Access Management, Audit Tools Access* (IAM-01) requires restricted access to audit tools to prevent disclosure of and tampering with log data. The omission of this control in ISO could generate a flaw in the review and analysis of security incidents. If log data are tampered with, violations could go unnoticed, and necessary repairs not done. The absence of one control in TSPC could enable undesired access to cloud data. *Encryption & Key Management, Storage and Access* (EKM-04) refers to the use of adequate data-encryption and secure management of encryption keys, and imposes a technical measure for information assurance enhancement. The absence of this control would open up a vulnerability that could be exploited by generic attackers to obtain encryption keys, and would be a risk with respect to insider threats as well. If keys are stored at a cloud level, a CSP employee could obtain access to them, thus breaking security measures implemented by the tenant.

Last in the class of misconfigurations, the absence in FedRAMP and TSPC of controls in the *Interoperability and Portability* domain could be a significant source of vulnerabilities. The omission, however, must be contextualized in the scope of each standard. FedRAMP, which is aimed at assuring a secure cloud for the U.S. government, is complemented by other regulations and frameworks, such as NIST SP 500-293. NIST SP 500-293, which is applicable to U.S. federal agencies, regulates interoperability and portability issues and thus mitigates the absence of the IPY domain in FedRAMP. TSPC, on the other hand, are not similarly complemented by other frameworks, and their effectiveness must be evaluated on a case-by-case basis.

The second class of vulnerabilities consists of insider threats. An attack could be perpetrated directly by a CSP's employee, or an employee could be the vehicle by which information hosted by a CSP is targeted. Among the controls useful for giving protection against such threats, *Identity & Access Management, Trusted Sources* (IAM-08) requires the adoption of the least privilege rule to access user identities and is omitted in FedRAMP. Two of the possible consequences of this omission are account hijacking, and the presence of malicious insiders [5]. In addition, among the provisions of NIST SP 800-53, FedRAMP does not consider Appendix G. Countermeasures outlined in that section, including the use of an insider threat handling team, would reduce the risk deriving from the omission of IAM-08, but are not included in the standard.

Similarly, the control *Infrastructure & Virtualization Security, Hypervisor Hardening* (IVS-11) is missing in TSPC. This control requires stricter control of access to all

the hypervisors, and its absence—which is not compensated for by other measures in the standard—may facilitate unauthorized access by CSP employees to applications and data. In addition, *Governance and Risk Management, Management Program* (GRM-04), *Governance and Risk Management, Policy Impact on Risk Assessments* (GRM-08) are also missing in TSPC. Those two controls require the creation of an Information Security Management Program and detailed security policies (GRM-04), and mandate constant updates of those policies following periodic risk and security assessments (GRM-08). Their absence, although not directly causing a loss or disclosure of data, can weaken the protection framework implemented by the CSP through the absence of security updates to the internal procedures and periodic checks to their effectiveness. Procedural flaws and missing updates to internal procedures following technical changes to a system could be exploited by a malicious insider to remain undetected. In a similar vein, the absence of *Infrastructure & Virtualization Security, Change Detection* (IVS-02) from TSPC could enable tampering with data. If changes to the VM images are to be made, adequate notice to the tenant must be given and archiving of logs performed by the provider. Failure to perform the notification could result in failure of necessary patches in an application or integrations to the VM, resulting in undetected vulnerabilities. An example could be a malware injection from a malicious insider that, in the absence of updates, could go undetected [32].

C5 shows five omissions relevant to the class of insider threats, and three of them are related to screening procedures involving CSP employees and clearance to enter CSP facilities. First on the list is the control *Datacenter Security - Unauthorized Persons Entry* (DCS-08), which oversees circulation of people between different areas within the CSP facilities. Although the control is mitigated by the inclusion of an additional requirement in C5, the baseline control does not require isolation of service areas and data storage, hence opening a flaw in physical access authorization. Once a subject has been authorized to access the service area, he or she could have access to the data center as well, potentially causing a security incident. Although the absence of this control could be disruptive if malicious attackers introduced themselves into the CSP facilities, access control and screening mechanisms are in place in C5, reducing the impact of the absence. Still, CSP personnel should be authorized to enter only the areas of a facility that are relevant to their areas of competence. Second on the list is a control on identity management. *Human Resources - Background Screening* (HRS-02) requires that background screening of employees be adequate and proportional to the sensitivity of information accessed in the system. If this control is omitted, employees could maliciously bypass access restrictions, and act on the system beyond the boundaries for which they are authorized. Background checks are included in C5, but proportionality is included only among the additional requirements. The third missing control is *Human Resources - Employment Termination* (HRS-04). C5 does not clearly specify policies and procedures for the event that an employee is terminated or his or her functions are changed. Following such an event, an adjustment in access privileges and restrictions must be applied; otherwise, the benefits of implementing precautions based on access level differentiation could easily be vanquished. The fourth control omitted in C5 is *Business Continuity Management & Operational Resilience – Policy* (BCR-10). It requires the CSP to set detailed IT governance policies and to train employees on the requirements imposed by those policies. Although C5 includes provisions on governance policies, it does not clearly define roles and responsibilities, nor does it mandate training for employees following the release of IT governance policies. The absence of such a requirement is made worse by the omission in C5 of another control, namely *Human Resources - User Responsibility* (HRS-10), which is generally oriented towards CSP employees' awareness of procedures and policies. The resulting information and awareness gap suffered by the employees could become the origin of violations and the cause of vulnerabilities.

Last, the absence in FedRAMP, C5, and TSPC of multiple controls from the domain of *Mobile Security* (MOS) cannot be overlooked. Attackers can target CSP employees' mobile devices by exploiting vulnerabilities in the mobile devices' operating systems. For example, the "Stagefright" exploit can use MMS to infect other devices [15][23]. At the same time, specific vulnerabilities in Android can be exploited to access restricted corporate network resources [17][38]. Further, mobile devices based on Android, a Linux-based operating system, are vulnerable to recently discovered flaws such as the "DirtyCOW" [38]. FedRAMP, C5, and TSPC show some important omissions in Bring-Your-Own-Device (BYOD) policies, and the lack of prudent controls on employee-owned mobile devices can be a source of vulnerabilities for a CSP.

D. Additional Considerations

With respect to the 133 controls required in the CCM, our comprehensive study of four standards used to assess cloud security shows considerable gaps, which have been filled only in part by updates that patched these standards over the years. When we narrowed our study to the 82 most relevant controls—which we selected for their ability to defend against common threats and vulnerabilities in cloud environments—we count up to nineteen omissions, only four of which are missing in more than one standard. That brings us to a first important consideration on the nature of the standards, which is their redundancy. As long as 63 of the most relevant controls in the CCM (or roughly 77%) are addressed in all of the standards, we affirm that there is not a radical difference in their substance. All four of the frameworks are aimed at providing information assurance in IT systems through a similar set of baseline controls. At the same time, these numbers lead to a second important consideration, which is the complementarity of the standards. On the one hand, the four frameworks overlap significantly, making them (to some extent) interchangeable when it comes to cloud assurance. On the other hand, a total of nineteen controls are missing from at least one standard; of those, only four are missing from more than one standard.

That highlights some relevant differences in the standards' approaches to IT security, which can also be seen through examination of their diverse sources and evolutions. First, FedRAMP, designed to assure security of information processed by contractors of the federal government, can balance its omissions by relying on other provisions that CSPs must comply with. As shown in the case of IVS-07, FedRAMP does not include measures that fall into the competence of the contracting agency, since FISMA also applies. At the same time, as proven in the case of side-channel attacks, the more technical and specific nature of FedRAMP gives high attention to technical countermeasures to threats and vulnerabilities, but lacks equal attention to internal policies supporting security of information. Conversely, ISO is more general in its scope and demands strong policies and procedures rather than detailed technical measures. Yet ISO tends to offer a set of well-articulated controls, especially after 2013, when its review focused on the existing threat landscape; that made the standard resilient, and well suited for cloud technology. C5 is very specifically designed for cloud environments. It is well structured and provides good protection, especially as it includes the additional requirements suggested in the standard. Notably, C5 compensates for the only two omissions in ISO: protection against side channel attacks and misconfigurations. However, C5 has important shortcomings with respect to human resources and identity management, thus increasing the risk of insider threats. If it is conceived as a complement to the ISO certification, C5 can be considered effective. If C5 is used as a standalone certification, however, additional controls will be required in order to ensure the best protection. Lastly, SOC suffers from being too general in the specification of the assessment criteria, performing well as an initial guideline for security audits, but not as a definitive standard. Our study of TSPC found a set of diffuse vulnerabilities to multiple threats, especially insider threats, on both the CSP and tenant sides. In particular, the adequacy of TSPC to assess cloud environments did not benefit from its 2014 review and the reorganization of its content into more general categories.

Our comprehensive assessment of the four standards reveals that all of the frameworks have limitations, and thus do not on their own provide full protection against current threats to cloud environments. However, the four standards provide complementary features and therefore in combination offer improved protection against threats and vulnerabilities; thus, the existence of multiple frameworks is justified. At the same time, our analysis highlights the limited number of omitted controls in each standard, and perhaps the addition of these few missing would be sufficient to allow individual standards to function on their own, potentially eliminating the need for multiple standards.

V. Conclusion

In the IT security landscape, four frameworks can be considered as the leading standards for assessment and attestation of information assurance in cloud environments. Two of the standards—SOC 2, created by AICPA based on TSPC, and ISO/IEC 27001—focus on IT systems, with no specification of the deployment model. The other two, FedRAMP and C5, are more recent and were created specifically for the cloud. We have compared these four frameworks, looking at their changes over the span of eleven years from 2005 (the year the first version of ISO was released) to 2016, when C5 and the last update of TSPC were released. We have drawn important conclusions from our observations of the evolution of the four standards and their completeness and adequacy in addressing cloud threats and vulnerabilities. To measure their performances, we have compared them against a third-party framework issued by CSA that is specifically designed for cloud assurance. We narrowed down our observation to the controls relevant to preventing common threats and vulnerabilities in cloud environments, selected from CSA's study "The Treacherous Twelve" [9]. This examination allowed us to identify gaps and omissions more precisely, and gauge how much risk the standards are unable to protect against in cloud systems. CSPs might benefit from our completeness and adequacy assessment of each standard to determine which framework is the most appropriate to evaluate their cloud security. We have determined that the examined standards are not completely interchangeable, but rather complementary. On the one hand, that finding justifies the existence of multiple standards, as they can be used in combination to guarantee cloud assurance. Since each of them proposes a slightly different approach to assessment and auditing, and focuses on different aspects of IT security, compliance with more than one framework allows a CSP to perform a more comprehensive and nuanced audit of its systems. On the other hand, little effort would be required to improve the standards, adding missing measures to prevent more vulnerabilities or threats. In our study, we have highlighted those missing measures, thus suggesting possible improvements. Among the standards in our study, ISO has shown better performance than the others. FedRAMP could be improved with greater attention to information management policies and procedures. C5 could benefit from improvements on identity and human resources management. Finally, TSPC suffers from being based on overly general criteria, showing gaps and weaknesses in the controls adopted for the assessment.

Additional attention must be given to mobile security, which is a flaw in three of the four standards. ISO, after the improvement made in its last review in 2013, is the only framework that gives full coverage of the control domain. Clarity in the definition of bring-your-own-device policies is the main issue in this area, since the absence of well-defined rules could generate (or amplify the magnitude of) insider threats.

VI. Future Work

Standards are a valuable tool in providing baseline security to support cloud assurance. Improvements to, and constant updating of, the existing leading standards are necessary to maintain adequate protection of the information stored and processed in cloud systems.

First and foremost, the areas left unprotected must be covered with additional controls and precautions.

Second, it is necessary to keep current standards up to date by maintaining the study of threats and vulnerabilities as a priority, and these studies must be used to suggest new measures for improving the security frameworks. The appearance of new threats is often associated with the appearance of new technologies or service models interacting with cloud environments, as with, for example, the Internet of Things. That phenomenon implies the need for additional effort in discovering, detecting, and finding solutions for vulnerabilities, while at the same time working to make existing security frameworks adequate, or create new ones.

Third, the current certification landscape needs better integration to avoid unnecessary repetitions and simplify the assessment process, once one or more certifications have already been obtained by a CSP. Since the great majority of needed controls already exist in four standards, we must question the need for having multiple assessment processes, instead of promoting mutual recognition of the existing standards.

Future research might consider the implications of unifying multiple standards under a common assessment process versus multiple concurrent security assessments, highlighting benefits and disadvantages of each model.

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] AICPA. 2011. New SOC Reports for Service Organizations Replace SAS 70 Reports. AICPA Communications, February 7, 2011.

[3] Amazon Web Services. 2016. AWS Lambda. Product Details. Webpage. Accessed October 15, 2016. https://aws.amazon.com/lambda/details/

[4] 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

[5] 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. Requirements Engineering for Security, Privacy & Services in Cloud Environments. 18 (4). Springer. P. 343-395

[6] Calder, A. 2005. The case for ISO 27001. Ely, U.K.: IT Governance Pub.

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

[8] – – –. 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

[9] – – –. 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/

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

[11] – – –. 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/

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

[13] 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

[14] Creese, S., Goldsmith, M., Hopkins, P. 2013. Inadequacies of Current Risk Controls for the Cloud. Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010. P. 659-666

[15] 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.

[16] 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

[17] FedRAMP. Marketplace. Web page. Accessed November 21, 2016. https://marketplace.fedramp.gov/index.html#/products?sort=productName

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

[22] 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/

[23] Gartner. 2016. Gartner Says Worldwide Public Cloud Services Market to Grow 17 Percent in 2016. Press Release. Accessed November 20, 2016. http://www.gartner.com/newsroom/id/3443517

[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] ISO Survey. 2015. Accessed November 24, 2016. http://www.iso.org/iso/iso-survey

[29] Jiang, X., Wang, X., Xu, D. 2007. Stealthy malware detection through VMM-based "out-of-the-box" semantic view reconstruction. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)

[30] Jones, S. T., Arpaci-Dusseau, A. C., Arpaci-Dusseau, R. H. 2006. Antfarm: Tracking processes in a virtual machine environment. In Proceedings of the Annual Conference on USENIX '06 Annual Technical Conference (ATEC '06)

[31] Jones, S. T., Arpaci-Dusseau, A. C., Arpaci-Dusseau, R. H. 2008. VMM-based hidden process detection and identification using Lycosid. In Proceedings of the Fourth ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE '08)

[32] Huh, J. H., Montanari, M., Dagit, D., Bobba, R. B., Kim, D. W., Choi, Y., Campbell, R. 2013. An empirical study on the software integrity of virtual appliances: Are you really getting what you paid for? In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS '13). ACM, New York, NY, USA, 231-242. http://dx.doi.org/10.1145/2484313.2484343

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

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

[35] Metheny, M. 2013. Federal cloud computing: The definitive guide for cloud service providers. Waltham, MA: Syngress

[36] 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

[37] Murugesan, S., Bojanova, I. (Eds.). 2016. Encyclopedia of Cloud Computing. John Wiley & Sons, Ltd.

[38] Nickell, C. G., Denyer, C. 2007. An Introduction to SAS 70 Audits. Benefits Law Journal, 20(1), 58-68.

[39] Ormandy, T. 2007. An Empirical Study into the Security Exposure to Host of Hostile Virtualized Environments. Accessed January 25, 2017. http://taviso.decsystem.org/virtsec.pdf

[40] Payne, B. D., Carbone, M., Sharif, M. I., Lee, W. 2008. Lares: An Architecture for Secure Active Monitoring Using Virtualization. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (S&P 2008)

[41] 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/

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

[43] Taylor, L. P. 2013. FISMA compliance handbook. Waltham, MA: Syngress

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

[45] – – –. (2014). Cross-Tenant Side-Channel Attacks in PaaS Clouds. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). ACM, New York, NY. 990-1003