PRIVACY AND SECURITY IN THE CLOUDS:
IT SECURITY AND PRIVACY STANDARDS IN THE EU AND US

BY

CARLO DI GIULIO

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Arts in European Union Studies
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2017

Urbana, Illinois

Master's Committee:

Dr. Masooda N. Bashir, Chair
Dr. Maxime H. A. Larivé

ABSTRACT

Cloud computing represents a revolutionary service model for accessing information technology (IT) services, and an opportunity for governments to reduce maintainance costs of IT infrastructure. However, relying on commercial cloud services may prove challenging for privacy and security if cloud service providers cannot guarantee adequate standards for their services.

In this thesis, I analyze four IT security standards comparing them alongside each other. ISO/IEC 27001 and SOC 2 are two international IT frameworks issued by non-government organizations and available since 2005. FedRAMP and C5 are two more recent cloud-specific standards, respectively issued by the US and German governments.

Examining the four standards in comparison, and evaluating their completeness and adequacy in guaranteeing information assurance in cloud environments, I question whether they really represent an improvement in cloud security, what are their shortcomings, and ultimately the necessity of new cloud security standards in the already crowded IT security landscape.

I combine a broad contextual analysis with empirical results to help understand the reasons for creating C5, and shed lights on its role in the EU political agenda.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

CHAPTER 1: INTRODUCTION

The impact of information technology (IT) on today's business and everyday life is greater than ever before. Remote access to information and computational resources are necessary to efficiently perform job activities, financial transactions, or access personal communications. With the diffusion of cloud computing – known as the "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (NIST, 2011) – an evolution in our approach to IT usage is occuring. Not only are software resources more easily accessible over the internet, but enhanced hardware capabilities and computational resources have also become available remotely, based on commercial service providers' IT infrastructure. An increased number of opportunities, however, corresponds to higher risks for security and privacy of remote systems-based applications. Cyber-treats, such as malicious insiders, account hijacking, or denial of service (DoS) attacks, have driven attention and concern of governments and the IT industry, engaged in finding new solutions to maximize benefits of cloud computing without suffering of its risks. When privacy and security of information are affected by cyber-threats, confidentiality, integrity, and availability (C-I-O) might be compromised, and information trust be at stake. Governments, industry, as well as private citizens can experience data leaks and financial losses. To find shelter against potential threats, attention to improving existing IT security standards – or if necessary creating new ones – has captured considerable effort and resources. The European Union (EU) and the United States (US) represent a bulwark in standardization of security measures and risk management. Yet, differences among the adopted standards and lack of mutual recognition create substantial confusion in the access to IT-based services, and leads to an increased burden on service providers. This is even more striking in consideration of the

enormous amount of information exchanged across the Atlantic. With a combined total of more than 44% and 32% respectively in exports and imports shares in 2014, the two blocks are at the leaders of world trade value in commercial services (WTO, 2015), with the consequent volume of data that needs to be transferred between the US and the EU. However, lack of interoperability of security standards leads to a decrease in efficiency. Where certification or authorization mechanisms are required to operate in a certain country or area (as for providing IT services to the US government, or specific services in the EU, such as electronic document preservation), a *de facto* compliance could not be enough. At the same time, the existence of different standards concurring to the same goal might be detrimental for competition. Only those organizations able to afford multiple certifications could meet the higher security requirements, thus penalizing smaller organization and affecting variety and quality of IT offer.

Referring to harmonization of IT security measures in the Single Market,[1] the European Commission, the executive arm of the EU, has metaphorically defined the whole set of existing standards and certifications as a "jungle" (Gleeson and Walden, 2014). Cloud security certifications grow from common roots, facing same issues and using similar security measures. However, they have extended their branches in slightly different direction in the last few years, in a stratification that aims at protecting security and trust, but often rises confusion and burdens for service providers and users of the services. Among the most relevant IT security standards, ISO/IEC 27001 is available since 2005, year of its first publication. It was updated in 2013 to keep pace with IT innovation and respond to newer threats, and counts more than 27,000 valid certificates worldwide as for 2015 (ISO, 2015). The standard specifies guidelines and requirements

[1] The European Single Market "refers to the EU as one territory without any internal borders or other regulatory obstacles to the free movement of goods and services" (European Commission, 2017a).

to establish, implement, and maintain information security management systems. Another international standard, first issued in 2011 by the American Institute of Certified Public Accountants (AICPA), is SOC 2. The standard is based on an extensive list of trust services principles and criteria (TSPC), also issued by AICPA, and derives its structure from the SAS 70 report, a reporting standard created to assure the integrity of financial statements. SOC 2 evolved from SAS 70 focusing on privacy and security measures implemented in IT systems. In 2011, instead of embracing or building on existing standards, the US government issued its own list of security requirements. The Federal Risk Authorization Management Program (FedRAMP) limits its perimeter to cloud service providers (CSPs) to the Federal Government. CSPs are required to receive an authorization from the FedRAMP Joint Authorization Board (JAB)[2] and comply with FedRAMP control requirements to offer cloud services to Federal Agencies. As for March 2017, only 79 service providers are FedRAMP authorized (FedRAMP, 2017a), and more than one third of them are already ISO/IEC 27001 certified. After its first release, FedRAMP was reviewed in 2015 with additional controls, and completed in 2016 with the introduction of a high security baseline for more sensitive information.

In the EU, at the same time, the *Bundesamt für Sicherheit in der Informationstechnik* (BSI - the German Federal Office for Information Security) issued its own set of controls, aimed to assess information security of cloud services. The Cloud Computing Compliance Controls Catalogue (C5) published early 2016 integrates controls from the major certification schemes, including ISO/IEC 27001 and SOC 2, but not FedRAMP. It supplies to missing controls from existing frameworks, or integrates the ones deemed to be incomplete. Although C5 is not meant to

[2] The JAB members are the Chief Information Officer from the Department of Homeland Security (DHS), General Services Administration (GSA), and Department of Defense (DOD). The JAB is supported by Office of Management and Budget Policy (OMB), CIO Council, and NIST (FedRAMP, 2017b).

be a certification, but rather a checklist and a set of guidelines for cloud security auditors to break on through the jungle of standards described by the European Commission, what it does is adding another standard to the list of existing IT security frameworks.

The narrative emerging from the past few years brings several questions. Is a new framework ultimately necessary? What increased protection can a standard such as C5 guarantee that others cannot? What is the purpose of adding another security standard to a crowded group of international and national certifications? Why does C5 recognize the ISO/IEC 27001 and SOC 2, while it overlooks FedRAMP?

This thesis aims to respond to these questions, compare the effectiveness of C5 to other existing standards, and identify possible areas of improvement. Additionally, it clarifies its relation with FedRAMP, SOC 2, and ISO/IEC 27001 in control area and controls addressed by the four standards, while looking to the role and goals of the European Commission and the US government in the adoption of these standards[3].

1.1. Research Contribution to the Field

Previous work on standards have explained the reasons behind standardization, and the effects of standards on society. The idea of standards as legislative acts justifies their role and potential in driving change in the society by creating a set of ruled drafted by experts. Narrowing down the attention to the literature on IT standards, previous work appears limited to the analysis

[3] Notably the European Commission, through the support of DG Connect, promotes cloud computing initiatives under the European Cloud Strategy 2012, formally initiated with the publication of the communication No. 529 (2012) "Unleashing the Potential of Cloud Computing in Europe" (European Commission, 2012). In the US, the promotion of cloud security falls under the broader "cloud First Strategy (Kundra, 2011), first issued by the CIO council supported by the OMB. The strategy gives a strong signal to federal agencies about the necessity of moving to cloud technology promoting efficiency and security of information.

and comparison of security standards attempting to guarantee information assurance in IT systems, without trying to clarify the role of existing standards in a "bigger picture" incorporating an evolving political, normative, and societal context. Similarly, previous studies on cloud threats, although receptive to the risks associated with the use of cloud technologies and proposing technical remedies, have not offered sufficient elements to integrate their conclusions in the existing security standards adopted by the IT industry. This thesis aims at filling those gaps by combining a review of FedRAMP 2015, SOC 2, C5, ISO/IEC 27001:2013, and a broader contextualization of the standards in the political, legislative, and societal landscape.

Building on the results from previous studies (Di Giulio *et al.*, 2017, 2017a), I propose an analysis of how missing controls result in potential threats to cloud services, and I explore the evolution of these standards by looking at their completeness and effectiveness overtime. Besides clearly stated goals (i.e. information assurance in IT environments), the function of standards such as C5, ISO/IEC 27001, SOC 2, or FedRAMP can be adequately assessed only by measuring the improvement they are able to bring to cloud assurance. The technical analysis helps gauging the effectiveness of existing cloud security standards comparing them alongside each other, while also exploring how resilient the standards are in the face of a dynamic threat landscape. At the same time, a thorough analysis of the international context and the different approaches to privacy and cybersecurity in the US and the EU helps to address and understand the relevance and function of the existing standards. Regulatory measures, policies, and soft law are all instruments contributing to build the identity of each institutional block. Standards as legislative acts are one of those instruments, and must be looked in context to be correctly understood.

CHAPTER 2: IT SECURITY STANDARDS[4]

Standards are pervasive in our life, and standardization – the effect of complying with a standard – has a double function on the market of goods and services. On one hand, standards make users' life easier, creating the conditions for commercial products or services to meet users' expectations. That is because, when products or services are compliant with a standard, their characteristics are generally well-known to the public, and users are aware of their features, capabilities, and limits as well. On the other hand, standards can be adopted to guarantee baseline protection in subjects including, but not limited to consumer's rights, personal data protection, and business competition. For example, food safety standards aim to ensure higher quality of food products, establish safety for human consumption, and at the same time reassure consumers on the production processes adopted by the food industry. The existing literature offers a variety of definitions on what a standard is and what are its functions. In this chapter, I give an overview of definitions, functions, and characteristics of standards with a focus on FedRAMP, ISO/IEC 27001, SOC 2, and C5.

2.1. Standards as Legislative Acts

The National Institute of Standards and Technology (NIST) offers an extensive definition of what a standard is, and operates a distinction depending on the source of the standard and its function. First "technical standards" detail the specifics of products or materials, including the

[4] This Chapter includes material from previously published work. See Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K. Campbell, R., Bashir, M. (forthcoming 2017). "Cloud Security Certifications: A Comparison to Improve Cloud Service Provider Security". In the proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing (ICC 2017), Churchill College, Cambridge, UK. March 22-23, 2017. ACM Proceedings Series

procedures for their management. The second group are "voluntary standards," those not imposed by existing laws or regulations. Third are "non-government" standards, which are those applied in spite of missing enforcement measures by the authorities. Last are "performance standards," which do not specify details on products and materials, such as in the case of technical standards, but rather specify the result that must be achieved (NIST, 1998). The International Organization for Standardization (ISO) provides a more general definition, referring to a standard as "a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose" (ISO, 2017). In brief, a standard can be defined as a prescription of procedures and methods to achieve a given goal. Although the distinction made by NIST of voluntary or non-government standards (which implies the existence of required standards and those created by governments) suggests different strength of a standard depending on its formal value, normative power of a standard is often unrelated to it.

Although standards and guidelines cannot be properly defined as norms, their relevance as regulatory tools and effective drivers for change is well recognized in the literature. Brunsson and Jacobsson (2000) list three possible types of rule: norms, directives and standards. Norms are intended as socially recognized and internalized rules. Norms do not require enforcement by external powers, and individuals comply with them by their own will. Directives are written rules, issued by authorities, and generally accompanied by enforcement measures and sanctions. Standards are the third category, inclusive of explicit rules with no reference to authorities in charge of enforcement measures and sanctions (Brunsson and Jacobsson, 2000, p.13). However, despite being often promulgated by non-government bodies, their endorsement by governments and their direct reference in legislative acts – those which Brunsson and Jacobsson refer to as

"directives"— make them as effective as legislative acts. The ISO/IEC 27000 series, for instance, is issued by a non-government organization. The EU Implementing Regulation 2015/1502, setting out technical specifications and procedures according to the EU Regulation 910/2013 on e-identification and trust services, points out to the ISO 27000 series as guidance for the adoption of information security management systems. At a national level, a more specific example can be found in rules for long-terms storage of electronic documents with preservation of their legal validity. For example, the Italian national agency for digitalization (*Agenzia per l'Italia Digitale* – AgID) has made clear how service providers are required to be certified against ISO/IEC 27001:2013 before being able to offer such a service to the public.[5]

2.2. What Is Behind Standards?

The main reason why governments rely on standards and consider them legitimate to dictate technical requirements is that standards are crafted by experts (Brunsson and Jacobsson, 2000, p. 40). The formalization of experts' opinions through standards represents a means to create a "repository" of knowledge (Brunsson & Jacobsson 2000, p. 42), and serves the purpose of reducing case-by-case consultations with credentialed professional by embedding authority in written rules (Timmermans and Epstein, 2010). However, not always are experts extraneous to the industry, which would make the definition of common practices and guidelines derive exclusively from proactive actions of expert groups or governments, but they can be industry stakeholders, thus making standards a consequence of market self-regulation. Dombalagian notes how "direct standard-setting by regulatory bodies may suffer from poor information about the industry and its

[5] Circular N.65, April 10, 2014. Procedures for accreditation and supervision of public and private subjects providing electronic document storage in compliance with article 44-bis, clause 1 of the legislative decree 82, March 7, 2005 (My translation. Original text: Circolare n.65 del 10 aprile 2014 – Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e private che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n.82).

technical capabilities and cumbersome administrative processes and judicial review" (2015, p. 123). For the sake of market efficiency "[r]egulators generally intervene in standard-setting only when informational intermediaries and industry bodies lack the incentive to develop adequate standards or cannot internalize positive externalities" (Dombalagian, 2015, p. 123). As a consequence, governments may find convenient to allow self-regulation as the benefits deriving, on one hand, from fast competition, and on the other hand from skillful decisions, are greater than dictating their own terms.

In some situations, however, the authorities could be better off leading the standard building process. These cases are particularly those where divergent interests between government and industry might result in detriment for consumers or competition and equal access to markets[6]. Shapiro (2003) argues that governments cannot justify the standards determined in autonomy by the industry because of their transactional costs. Although governments might initially save time and money in delegating the definition of a standard to private parties letting the market free to determine their own best practices, since private actors tend to engage in opportunistic behavior, divergence of interests is more likely to increase the costs in a later moment (Shapiro, 2003, p. 407). A possible consequence is that governments will be forced to intervene with additional burdens on producers and users as well. Shapiro presents his idea of increasing transational costs as generally applicable. However, the unbalance between government and business interests mostly depends on policies, political, and ideological orientation. For example, transactional costs of data protection in the EU may be very likely to increase when governments leaves the industry

[6] An example of conflicting interests between government and industry in the EU is the use of personally identifiable information (PII) for commercial purposes. On the one hand, the best interest for consumers is to keep their data private. On the other hand, businesses prefer less limitations to their use and be able to sell and buy PII for marketing and commercial purposes.

free to determine its best practices. In the EU, the idea of privacy as a human right conflicts with business interests to use personal information for commercial purposes. Protecting privacy once markets have opted for free data flow might be costly, and still insufficient to guarantee full protection.[7] The same issue can be seen from the opposite angle in the US, where the Government tends to be more supportive for business initiative versus private interests. Privacy is considered as a civil right, and personal data are progressively going towards commoditization.[8] In that case, government and business interests coincide, thus making transactional costs less likely to increase in the near future.

In addition to increasing transactional costs, market self-regulation can lead to a variety of problems, including lack of coordination among stakeholders or generate a lock-in effect.

First, lack of coordination, is the result of a failure in achieving full self-regulation, where multiple solutions are adopted to address the same issue, missing to create a standardization across the market. An example is the evolution of mobile chargers. Until 2009, a wide variety of chargers incompatible with other devices was adopted from the major mobile phone producers, accounting for 51,000 tons of redundant charges every year (IEC, 2011). Environmental concern, and inconvenience for users pushed the European Commission to ask for harmonization in the European Single Market. Ten major producers signed the related Memorandum of Understanding issued by the Commission, leading to the market-wide adoption of micro-USB charger as default charger, as recommended in the IEC Standard 62684:2011[9] (European Commission, 2009). As

[7] An exemple is the application of the "Right to be Forgotten" in the EU. See section 3.5.
[8] Privacy protection standards in the US were drastically lowered in March 2017, when the current administration repealed the existing rules requiring higher control of consumers on their data and preventing internet service providers to sell browsing data to third parties (Freking, 2017).
[9] The standard is titled: Interoperability specifications of common external power supply (EPS) for use with data-enabled mobile telephones

shown in the example, the creation of Standards dictated from actors external to the market (in the example the European Commission) can force towards uniformity and solve the *impasse*.

Second, the lock-in effect, may happen when the most powerful actors on the market propose and then adopt a common solution, and hence force the market to uniform. Even in the case of a poor or perfectible solution, it might become impossible for more innovative and efficient ideas to gain relevance, like in an abuse of dominant position. An example of standardization to avoid lock-in effect can be recognized in the adoption of OpenDocument (ODF) file format (e.g. file with extension: .odt, .ods, .odp) as an ISO standard. The format is adopted for a variety of applications, including word processors, spreadsheets, and presentations. Concurrent was the adoption – although with significant doubts on interference of the industry leader in the standardization process[10] – of the Office Open XML file format (e.g. file with extension .docx, .xlsx, pptx). The wide predominance of proprietary formats produced with the Microsoft Office suite (e.g. file with extension .doc, .xls, .ppt) came to a halt in 2006 with the publication of the ISO/IEC 26300:2006 standard "Open Document Format for Office Applications." Only two years later, ISO/IEC published the 29500:2008 standard, based on Microsoft's proprietary format Office Open XML. After their recognition, the ISO/IEC Joint Technical Committee (JTC) 1 Information Technologies is in in charge of maintenance of the standards' specifications. The result of the standardization process was to reach interoperability between documents produced on multiple platforms, including Open Source applications (such as OpenOffice) and Microsoft Office.

As shown in the last example, the risk of a lock-in effect can justify the creation and formalization of new standards removing the conditions for self-regulation (i.e. existing standards)

[10] The European Commission casted doubts on Microsoft violating Anti-Trust Law to obtain recognition of the proprietary format Office Open XML as an international standard from the ISO/IEC (Forelle, 2008).

to allow equal access conditions to the market (Brunsson and Jacobsson, 2010). An identical reason can justify constant update of standards. The update can be promoted to reflect changes in requirements, as well as changes in market conditions. Echoing Brunsson and Jacobsson, Dombalagian argues that, in absence of updates following changes to market conditions, a lock-in effect in favor of well-established actors at the expense of new competitors is likely to happen, and updating old standards creates the potential of further changes and positive contributions (2015, p. 124).

In the EU and the US, some government agencies have a direct involvement in the creation of standards. This is the case of FedRAMP and C5, and in the example of FedRAMP, compliance with the standard has a direct effect on the CSP's ability to offer services to federal agencies. If in some instances the provisions in the standards can assume a direct normative value (e.g. for a CSP offering services to the Federal Government), they represent mere guidelines or recommendations in others (e.g. a CSP offering services to private tenants only). Still, lack of direct normative value for a certain group does not imply a lesser relevance of the standard. By defining a set of requirements, the authorities make a statement about the existence of multiple baselines. In the specific example of FedRAMP and cloud security, the creation of a detailed set of security measures implies a higher security baseline required for federal contractors. CSPs not contracting with federal agencies are free whether complying with the standard or not. However, being FedRAMP authorized may give them a commercial advantage over the competitors, as it means that the certified CSPs respect higher security standards, thus making them more appealing for private tenants as well.

Regardless of their source and statutory value, standards are meant to prescribe rules of behavior, procedures or general requirements. The prescription can assume various forms, and a standard can be organized in general clauses or guidelines, or in more stringent requirements, for instance included in a checklist of controls as in the case of ISO/IEC 27001, SOC 2, FedRAMP, or C5.

2.3. The IT Security Standards

The four standards subject of this study present a similar structure and share similar goals. ISO/IEC 27001 relates to risk management and security requirements in IT environments.[11] SOC 2 is aimed at promoting confidentiality, integrity, availability, and security in service organizations.[12] FedRAMP and C5 serve similar functions, by setting security requirements in the specific context of cloud environments. FedRAMP limits its scope to the Federal Government, whereas C5 is broader and serves as a generic guideline to promote cloud security. All the four standards are organized in control families – homogeneous groups of controls overseeing the same area – each one of which covers a relevant topic in information assurance (Table 2.1). Compliance with the controls in those sections is meant to be verified by specialized auditors, as the result of a thorough assessment of IT infrastructure, internal policies and procedures of the CSP. However, the standard can be used as a guideline for best practices in IT security. With the controls serving as a model, audits can be performed for a formal assessment allowing the CSP to obtain a certification or authorization, or by CSP's employees with the purpose of merely verify compliance with the guidelines and the implementation of baseline security.

[11] The full rubric of the most recent version of the standard is: ISO/IEC 27001:2013 The Information technology—Security techniques— Information security management systems—Requirements

[12] The rubric of SOC 2 is "Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy"

Table 2.1: List of Control Families in FedRAMP, ISO/IEC 27001, C5, and SOC 2

FedRAMP rev4 (2015)	ISO/IEC 27001:2013	BSI C5	SOC 2 (TSPC 2016)
AC - Access Control (43 controls)	A.5: Information security policies (2 controls)	UP - Framework Conditions of the cloud Service (4 controls)	CC1.0 Common Criteria Related to Organization and Management
AT - Awareness and Training (5 controls)	A.6: Organization of information security (7 controls)	OIS - Organization of Information Security (7 controls)	CC2.0 Common Criteria Related to Communication
AU - Audit and Accountability (20 controls)	A.7: Human resource security (6 controls)	SA – Security policies and Work Instructions (3 controls)	CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls
CA - Security Assessment and Authorization (15 controls)	A.8: Asset management (10 controls)	HR – Personnel (5 controls)	CC4.0 Common Criteria Related to Monitoring of Controls
CM - Configuration Management (26 controls)	A.9: Access control (14 controls)	AM – Asset Management (8 controls)	CC5.0 Common Criteria Related to logical and Physical Access Controls
CP - Contingency Planning (24 controls)	A.10: Cryptography (2 controls)	PS - Physical Security (5 controls)	CC6.0 Common Criteria Related to System Operations
IA - Identification and Authentication (27 controls)	A.11: Physical and environmental security (15 controls)	RB – Safeguards for regular Operations (23 controls)	CC7.0 Common Criteria Related to Change Management
IR - Incident Response (18 controls)	A.12: Operations security (14 controls)	IDM – Identity and Access Management (13 controls)	A1.0 Additional Criteria for Availability
MA - Maintenance (11 controls)	A.13: Communications security (7 controls)	KRY – Cryptography and Key Management (4 controls)	PI1.0 Additional Criteria for Processing Integrity
MP - Media Protection (10 controls)	A.14: System acquisition, development and maintenance (13 controls)	KOS – Communication Security (8 controls)	C1.0 Additional Criteria for Confidentiality
PE - Physical and Environmental Protection (20 controls)	A.15: Supplier relationships (5 controls)	PI – Portability and Interoperability (5 controls)	P1.0 Privacy Criteria Related to Notice and Communication of Commitments and System Requirements
PL - Planning (6 controls)	A.16: Information security incident management (7 controls)	BEI – Procurement, Development and Maintenance of Information systems (12 controls)	P2.0 Privacy Criteria Related to Choice and Consent
PS - Personnel Security (9 controls)	A.17: Information security aspects of business continuity management (4 controls)	DLL – Control and Monitoring of Service Providers and suppliers (2 controls)	P3.0 Privacy Criteria Related to Collection
RA - Risk Assessment (10)	A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)	SIM – security Incident Management (7 controls)	P4.0 Privacy Criteria Related to Use, Retention, and Disposal
SA - System and Services Acquisition (22 controls)		BCM – Business Continuity Management (5 controls)	P5.0 Privacy Criteria Related to Access
SC - System and Communications Protection (32 controls)		SPN – Security Check and Verification (3 controls)	P6.0 Privacy Criteria Related to Disclosure and Notification
SI - System and Information Integrity (28 controls)		COM – Compliance and Data Protection (3 controls)	P7.0 Privacy Criteria Related to Quality
		MDM – Mobile Device Management (1 control)	P8.0 Privacy Criteria Related to Monitoring and Enforcement

Sources: NIST, 2013; ISO/IEC, 2013; BSI, 2016; AICPA, 2016.

Controls in the three standards are provided as a textual description of security measures, procedural requirements, and best practices that the CSP must implement (Table 2.2). Coverage of all the controls should guarantee full security of the system certified against the standard, and protect against the most common threats to cloud environments.

Table 2.2: Example of controls in the four standards

Name of the Standard	Content of the control (Section and reference)
FedRAMP rev. 4 (2015)	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures (…) (**CM-9**)
ISO/IEC 27001:2013	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities (**A.6.1.1**)
SOC 2 (TSPC 2016)	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements (…). (**CC1.1**)
BSI C5	(…) On the part of the cloud provider, at least the following roles (…) are described in the security policy or associated policies and corresponding responsibilities assigned: (…). Changes to the responsibilities and interfaces are communicated internally and externally in (…) a timely manner (…). (**OIS-03**)

Sources: NIST, 2013; ISO/IEC, 2013; BSI, 2016; AICPA, 2016.

In spite of their similarities, however, the four standards are not equivalent. Each one has its own distinctive characteristics and operates in a specific context, and being compliant with one standard does not guarantee compliance with the others as well. In the following sections, I give an overview of the four standards, their development, and main differences among them.

2.3.1. ISO/IEC 27001

The ISO/IEC 27001 is a technical standard for "establishing, implementing, maintaining and continually improving an information security management system" (ISO/IEC, 2013) of any organization in the private or public sector (ISO, 2017b). The ISO/IEC 27001 is a joint effort of two different bodies, the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC). ISO is a non-governmental organization that

works through 162 national standards bodies around the world (ISO, 2017a). IEC is a non-profit, quasi-governmental organization structured in National Committees, which members are experts from national organizations, industry, academia, and government bodies (IEC, 2017).

ISO/IEC 27001 is part of a larger family of standards – the ISO/IEC 27000 series – issued by the Joint Technical Committee 1 (JTC1), specialized in Information Technology standards. The first version of ISO/IEC 27001 was issued in 2005 and derives from the British Standard 7799 of 1995 (renamed in 1998 as ISO 17799) (Gantz, 2013). ISO/IEC 27001 is structured in a general section providing comprehensive guidance to organizations on the path to assessment and certification, and a normative section build on detailed clauses specifying the security measures to be implemented. The first version of the standard consists in eleven families and 133 controls in the normative section.

To obtain a certification against the ISO/IEC 27001, an organization must undergo a third-party assessment. A continuous monitoring mechanism is required to maintain the certifications overtime, through receiving periodical controls and audits. The auditor verifies that the organization complies with the controls in the standard through an assessment following a P-D-C-A (Plan, Do, Check, Act) cycle. The planning consists in a broader evaluation of goals and objectives for the assessment: the controls are defined in details and the auditor plans how to perform them; in the second step (Do), the auditors perform the controls selected in the first step to evaluate issues in the organization's ISMS; the third step refers to the evaluation of any discrepancy between the best practices defined in the standard and the current status of the ISMS revealed during the check; the last step (Act) is the implementation of the necessary adjustments to the ISMS to make it compliant with the standard. The cycle repeats until the ISMS results fully

compliant. Although formally removed from the requirements in the newest release of the ISO standard, the P-D-C-A cycle is still considered as the best approach to an ISO/IEC 27001 assessment (Watkins, 2013).

The newest review of ISO in 2013 lowered the number of controls to 114 reorganizing them in eighteen categories. With the new version, the JTC1 wanted to increase interoperability with other standards, and make the ISO/IEC 27001 more flexible to cope with new technologies and newer threats, especially those stemming from the use of mobile technologies (ISO, 2013).

There are more than 27,000 organizations worldwide currently ISO/IEC 27001 certified, of which more than 10,000 in Europe and less than 1,500 in North America. Interestingly, the number of certifications increased by more than 20% between 2014 and 2015 with the higher regional increase in North America with 78% (ISO, 2015). That increase is aligned with a consistent trend since the first publication of the standard in 2005, suggesting progressively higher attention to IT security certification.

2.3.2. Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a federal government-wide risk authorization management program initiated in the US in December 2011 with the publication of the Office Management and Budget's (OMB) "Security Authorization of Information Systems in Cloud Computing Environments" memorandum for Chief Information Officers" (VanRoekel, 2011). FedRAMP is the result of a joint effort of federal agencies, local governments, academia, and non-government organization working together to define minimum security requirements for cloud providers to the Federal Government (VanRoekel, 2011). The program seeks to standardize the assessment and

authorization procedures for the CSPs, thereby establishing a security framework for cloud services in compliance with FISMA (FedRAMP, 2014). FedRAMP allows Federal Agencies to leverage existing authorizations according to a "do once, use many times" perspective, promoting savings in IT expenditure of Federal Agencies, in alignment with the provisions of the 25 Point Implementation Plan (FedRAMP, 2017a).

Much like FISMA, the security assessment required for Federal IT services, FedRAMP assessment derives a selection of controls from the Special Publication (SP) 800-53 developed by the National Institute of Standards and Technology (NIST). The title of this Special Publication is "Security and Privacy Controls for Federal Information Systems and Organizations" and includes a total of 810 controls and control enhancements. The controls provide baseline security measures, while the enhancements provide additional details and strength to the control measures. The controls are organized in 18 families. NIST SP 800-53 considers three possible tiers, following the same distinction and selection described in the Federal Information Processing Standard (FIPS) 199 and FIPS 200. The low baseline includes controls and enhancements designed for systems processing limited security impact information; the moderate baseline is required for systems processing information with medium security impact; the high baseline includes stricter controls aimed at protecting information which loss could cause severe or catastrophic consequences to the organization to which it belongs (NIST, 2004). FedRAMP adopts the same distinction as NIST SP 800-53, specifying controls and enhancements in three tiers.

In its first release in 2011, FedRAMP considered only low and moderate security control baselines for a total of 116 and 297 controls and enhancements, respectively, distributed in 17 families. In 2014, after the last review of the NIST 800-53 special publication, FedRAMP was

updated to a new version, reaching 325 total controls and enhancements for the moderate tier and 125 for the low tier. In July 2016, FedRAMP officially released a high baseline, including additional 96 controls and enhancements. The FedRAMP assessment follows the NIST Risk Management Framework (RMF) from Special Publication 800-37. It is structured in four steps, the first of which embeds steps 1-3 of the original NIST Risk Management Framework (FedRAMP, 2014a). It consists in (1) an initial step collecting information on the system, followed by (2) an assessment of security requirements, (3) an authorization phase to allow the provider to supply services to Federal Agencies, and last (4) a continuous monitoring phase, designed to guarantee the continuance of the same level of security after the initial authorization.

To obtain FedRAMP authorization to operate (ATO) and allow multiple agencies to leverage on the existing authorization, three distinct paths are possible. All of them require the involvement of a third-party assessment organization (3PAO) to act as an independent auditor, performing the required controls and attesting to the compliance of the Cloud Service Provider (CSP). The first path directly involves the Joint Authorization Board (JAB), the second involves a Federal Agency, and the third involves the CSP only. In each case, after the assessment of the 3PAO is complete, the request for an ATO must be submitted to the FedRAMP Program Management Office that will add the authorized system to the list of compliant systems (FedRAMP, 2014). The first FedRAMP ATO dates back in 2013. As of March 2017, 77 systems have been authorized – 4 at a high level – following the three different ATO procedures, and another 52 are in-process. The total number of 3PAOs is 45, but only 16 have been involved in at least one assessment since the program started in 2011 (FedRAMP, 2017c). On the one hand, jurisdictional constraints certainly plays a role in limiting the numbers with FedRAMP. On the

other hand, the authorization process has been havily criticized for being too slow, costly for CSPs, and uneffective in increasing IT security (MeriTalk, 2016).

2.3.3. Cloud Computing Compliance Control Catalogue (C5)

The Cloud Computing Compliance Control Catalogue (C5) was presented in 2016 as a set of cloud-specific measures aimed at simplifying the cloud security certification landscape (Grete, 2016). The C5 builds on the structure of ISO/IEC 27001 and SOC 2 reporting standard to assure complete and comprehensive protection in cloud environments (BSI, 2016). The standard is the result of an effort of the Bundesamt für Sicherheit in der Informationstechnik (BSI–German Information Security Office). BSI presented the C5 as a guideline that could be used by CSPs independently from other standards, or as an integration to existing certifications and assessments. For this purpose, BSI provides a table of comparison with some of the major existing standards used today, such as ISO/IEC 27001, or SOC 2.

C5 is structured in one general and eighteen normative sections, and 118 controls. The control requirements are built at two levels. The first is the basic level: fulfillment of the basic requirements is sufficient for the CSP to be compliant with the standard, assuring them a strong security baseline. The second level is made of additional requirements: these requirements are specified for part of the controls to provide higher security and privacy measures protecting sensitive information

C5 constitutes one of the referencing standards for the creation of the European Secure Cloud (ESCloud), a cloud label which core mission is “to facilitate market players and public bodies gaining trust in cloud services compliant to the requirements of [ESCloud].” ESCloud is

built in cooperation between BSI and the Agence nationale de la sécurité des systèmes d'information (ANSSI), the French national cybersecurity agency (BSI, 2016a).

2.3.4. SOC 2

The American Institute of Certified Public Accountants (AICPA) is a non-government organization founded in 1887 and working on a wide range of activities including certification and standardization policies. AICPA counts more than 418,000 members in 143 countries, mostly from the accounting profession (AICPA, 2016).

In 1992, AICPA released the Statement on Auditing Standards (SAS) No. 70, a reporting standard finalized at providing support to certified public accountants in the analysis of financial statements of service organizations (Nickell and Denyer, 2007). The statement was designed to help service organizations and their clients in the exchange of information about compliance obligations, such as those deriving from the Sarbanes-Oxley Act in the US, and hence facilitating the auditing process. However, soon after SAS 70's release, service organizations consistently started to use the reports resulting from SAS 70 assessments to demonstrate to their clients the adoption of strong privacy and security measures, and their high attention to information assurance (Gartner, 2010). SAS No. 70 reports thus started to play a marketing function not planned by AICPA upon its release (Nickell and Denyer, 2007).

The misinterpretation of the standard forced AICPA to review it to better fit the expectations of client organizations. In 2011, AICPA released the Service Organizations Controls reports (AICPA, 2011), a group including three kind of reports with a broader scope than SAS

70's, including a marketing-oriented component and an explicit focus on security and privacy, other than compliance to financial regulations.

The first reporting standard in the group, named SOC 1, is the direct successor of SAS 70, as it engages in controls aimed at guaranteeing the integrity of financial statements. The other two reporting standards in the group are SOC 2 and SOC 3, which focus on privacy and security of information systems and information assurance. The difference between the two is the deliverable of the assessment. SOC 2 contains an extensive description of the assessment and the controls implemented in the information system, while SOC 3 consists in a brief statement, more suitable for marketing purposes, rather than showing the results of an insightful analysis (AICPA, 2014). SOC 2 reports can be formulated in two different types: Type I gives an evaluation of controls and control objectives chosen by the management to promote information assurance; Type II adds the evaluation of the effectiveness of the chosen controls, observing the effect of their implementation in the system. Since a SOC 2 report contains relevant information on security measures implemented in the information system of the service organization, it is generally restricted to clients of the organization. Conversely, since it does not contain sensitive information and in alignment with its marketing purpose, a SOC 3 report is generally public.

SOC 2 and SOC 3 reports are based on controls selected by the organization's management and the auditors from the list of AICPA's Trust Services Principles and Criteria (TSPC), a set of information assurance measures first released in 2009, and reviewed twice, in 2014 and 2016. The section of TSPC used as the foundation for SOC 2 and SOC 3 assessments is named TSP 100 "Trust Services Principles and Criteria for Security, Availability, Processing Integrity,

Confidentiality, and Privacy." TSP 100 has been deeply impacted by the two reviews of the TSPC both on its structure and the number of controls.

There are 117 controls in TSPC 2009, divided by the principle they protect. Those principles are confidentiality, integrity, availability, and security. Each group contains four categories: policies, communications, procedures, and monitoring. The first oversees the production of adequate documentation of the processes implemented in the service organization; the second is about policy-sharing and approval across all the levels of the organization; the third, procedures, defines formal requirements for policies to be approved and validated; the last category makes sure that policies and procedures are enforced and implemented.

TSPC 2014 deeply reviews the 2009 version, reducing the number of controls to 47, organized in four groups. The simplification is obtained grouping most of the controls under an umbrella category of common criteria protecting confidentiality, integrity, and availability, and organizing the remaining controls in principle-specific criteria similarly to the 2009 version. The goal of the revision is to simplify the assessment process for organizations and auditors. TSPC 2016 makes additional changes to the list of controls, clarifies and optimizes them reducing the number of common criteria and controls specific to confidentiality, integrity, and availability to a total of 44.

In addition to those principles, SOC 2 and SOC 3 reports protect privacy of information. However, criteria related to privacy protection are not included in TSPC 2009 and TSPC 2014. Until the introduction of 20 privacy-specific criteria in TSPC 2016, SOC assessments used the list of Generally Accepted Privacy Principles (GAPP), created by AICPA and the Canadian Institute of Chartered Accountants (CICA). The list is superseded by TSPC 2016.

2.3.5. Differences Among the Standards

The four standards in this study show similar structures and common goals. All of them are built on assessments based on controls and control families. The main goal of the standards is to set a benchmark on privacy and security measures adopted in IT systems of service organizations. Still, each standard has its own peculiarities, and observing them helps giving a better sense of range and scope of each standard.

The first difference is in their focus. ISO/IEC 27001 and SOC 2 are applicable to any organization and IT environment, regardless of whether the audited organization uses virtualized systems or on-premises infrastructure. FedRAMP and C5 are designed for cloud environments, and strictly speaking for the assessment of CSPs. Their different focus reflects on the content of the controls that is more general in ISO/IEC 27001 and SOC 2, more specific in FedRAMP and C5.

A second difference is in the number of controls. Although with few fluctuations after each review, ISO/IEC 27001, SOC 2, and C5 have a comparable number of controls (114, 64, and 118, respectively). FedRAMP shows a higher number of controls (325 in the moderate baseline) suggesting more accurate description of the single measures to be implemented by the CSPs.

Geographic distribution and number of certificates or attestations is another notable difference among the standards. FedRAMP is a national government standard. Its implementation is limited to the US and less than 80 CSPs have currently obtained a FedRAMP ATO. ISO/IEC 27001 active certifications are 1,247 in the US, and more than 27,000 worldwide (ISO, 2015).

Perhaps because of their broader applicability, ISO/IEC 27001 and SOC 2 are worldwide adopted standards. SOC 2, however, is based on personalized reports and does not result in a certification. Hence, data on its diffusion and adoption are not available. The same is for C5, more recent than the others, which is the result of a national initiative supported by the European Commission. The standard is conceived as a guideline and does not offer a formal certification. Yet, C5 is gaining increasing attention from the major Cloud providers (AWS, 2017; Microsoft, 2017).

The last notable difference is in the time in which the standards have been released and updated. ISO/IEC 27001 was the first standard to be released in 2005. Its only review was eight years later in 2013. TSPC, on which SOC 2 assessment is based, were released in 2009,[13] followed by two updates in 2014 and 2016. FedRAMP was released in 2011 and updated four years later in 2015. Its high baseline was introduced in 2016. C5 has only one version, its first release was in 2016.

2.4. Previous Work on IT Security Standards

An extensive body of research literature investigates IT security standards and guidelines. However, previous work is limited in scope as it focuses on the technical aspects related to the standards, and only a limited number of studies analyze FedRAMP, SOC 2, C5, and ISO/IEC 27001. Since fast-pacing technology changes can easily make infrastructures, as well as software outdated in the short period, there is a high probability that existing standards may incur in shortcomings, and hence considerable effort in improving standards and assuring their adequacy is devoted to the study of threats and issues in cloud computing. The identification of new threats

[13] The first version of TSPC was released in 2006. However, the first relevant version for this study (the first on which SOC 2 is based on) is the 2009 version. Although SOC 2 was released in 2011, it based its assessment on the controls in TSPC 2009. For this reason, I consider in the SOC 2 timeline the three versions of TSPC: 2009, 2014, and 2016.

allows a timely identification of weaknesses in existing systems and process, and accurate study may suggest effective responses in addressing the new vulnerabilities. Reactivity and proactivity in the study of threats are expected in the creation and update of IT security standards, and study of cloud vulnerabilities is intimately related to evaluation of completeness and adequacy of controls and control families in current standards.

The Cloud Security Alliance (CSA) has been active since 2008 and reviews existing standards and has even created its own certification (CSA, 2017). As the basis for its certification, CSA has produced a detailed list of controls to be adopted to guarantee information assurance in cloud environments. The controls produced by CSA are the result of analysis of industry-accepted standards, and are conceived as a complement to ISO 27001 in cloud environments (CSA, 2017a). CSA is adept at dealing with menaces to cloud security, periodically reviewing a list of threats based on surveys among experts (CSA, 2010; 2013; 2016). CSA, however, has overlooked connecting existing security standards with potential threats, and has left existing gaps in observed standards unaddressed. Adobe (2015) has developed a Common Controls Framework that enables Adobe's employees to avoid replication of controls common to different security frameworks. Adobe has analyzed multiple cloud security standards – including FedRAMP and ISO/IEC 27001 – to identify overlapping controls, saving time and making their implementation more effective. However, the goal of Adobe's framework is to foster business efficiency and, although demonstrating awareness about differences and similarities among standards, does not offer guidance to improve them with respect to attack vectors. The Cloud Standards Customer Council (2013) offers an overview of major cloud standards and recommends a ten-step process for determining the best framework for the evaluation of cloud security. Although at each step of the process a reference to existing standards is provided, the guideline results in general observations

and does not deal with single security controls, thus offering a limited space for analyzing gaps among standards.

Gikas (2010) offers a comparison between legislative acts promoting security standards for US Federal Agencies and private-sector standards. The author reveals overlapping controls and gaps among the Health Insurance Portability and Accountability Act (HIPAA), used in the healthcare industry, the Federal Information Security Management Act (FISMA), covering IT security for Federal Agencies, the ISO 27000 series, and the Payment Card Industry–Digital Security Standard (PCI-DSS), defining security measures for digital payment systems. ISO/IEC 27001 and PCI-DSS are also the focus in Rasheed's (2014) study, which highlights how these standards consider infrastructure security auditing more heavily than data security, but does not specify additional controls to be considered for improving existing flaws. Gleeson and Walden (2014) widely leveraged the ETSI's (2013) earlier survey and gap analysis of existing cloud standards. The authors distinguish between technical, informational, and evaluative standards, and identify in the latter a source for future challenges to information assurance in the cloud. Underpinning legal reforms may generate some confusion, however, and thus adopted standards may require review, which would jeopardize information assurance in the meantime. Their research is limited to an observation of the certification landscape, and neglects to offer specific directions for future work. Furthermore, they leave aside technical aspects to focus on institutional and legislative activities related to the standard itself. Their work is nevertheless reassuring in their ability to incorporate the coexistence of multiple standards.

Of a different opinion about the effectiveness of existing standards, Sunyaev and Schneider (2013) consider existing certifications and standards as inadequate for fast-moving cloud

technologies. Additionally, and somehow echoing the concerns on market lock-in already noted in Dombalagian (2015), they note how it is hard for small and medium enterprises to fully adopt existing cloud security standards because of the associated cost, which gives a great advantage to big firms with larger capital. Their results are general, however, and the authors do not move beyond denouncing the absence of a core set of widely adopted principles. On a similar note, questioning the approach to information assurance through certifications or pre-determined security frameworks, Bayuk (2011; 2011a; 2015) argues on the inadequacy of control checklists in most of current standards for either the impossibility of being exhaustive covering all possible flaws with a single standard or, on the opposite side of the spectrum, incurring in the risk of adopting a standard too focused on controls inapplicable to the system being audited. She rather suggests to use a holistic approach to IT security and consider the characteristics and goals of the system, assessing its ability to satisfy security metrics defined on a case-by-case basis. The author proposes a new approach to security assessments going beyond standardized assessments, thus refusing them altogether. Although the work by Bayuk must be praised for her attempt to contextualize the adoption of security measures and maximize their effectiveness in relation to the goal of each system, she overlooks the normative function of the standards, reducing their goal to mere best practices, rather than regulatory instruments as suggested in Brunsson and Jacobsson (2000).

Hendre and Joshi (2015) look at cloud-specific threats in literature, security requirements in more than 20 standards, and controls implemented by more than 100 CSPs analyzing publicly available sources. They develop an application able to help cloud customers choosing the CSP offering strongest compliance according to their needs. Although valuable in its

comprehensiveness, the study limits its focus to recommendations to cloud customers, being acritical of current security frameworks.

Three studies focus on classifying threats to cloud security, but their classifications are not matched with existing standards. They thus fail to find a real-case example on which to build an effective evaluation. First, Ardagna et al. (2015) conduct a detailed review of academic and non-academic work on cloud security and standardization. They classify existing work according to a common technique for providing cloud assurance during testing, monitoring, certification, audit/compliance, and SLA's. Similarly, the second study by Fernandez et al. (2014) collects and reviews previous studies from academia and industry on security threats to cloud environments so as to offer a comprehensive overview of trends in cloud security. Third, Huang et al. (2015) review the current status of IaaS security through an extensive study of industrial and academic work. The authors isolate potential threats to the confidentiality, integrity, and availability of information, and to Contractual Security, which refers to the breach of contractual obligations by the CSP or the tenant, and then classify those potential threats according to the violated principle. Two more studies try to analyze specific standards and evaluate them in comparison, but are limited in scope and were performed prior to the publication of the current version of ISO/IEC 27001 and FedRAMP. Creese, Goldsmith, and Hopkins (2013) perform a detailed review of risk controls as defined by the 2005 version of ISO/IEC 27001, and the 2009 NIST SP 800-53 rev. 3. They recognize the inadequacy of the two sets of risk controls to address cloud security issues at the time of their study, suggesting how innovation in multiple areas of control is required to address hybrid and public cloud security. Similarly, in their gap-analysis of ISO/IEC 27001:2005, Beckers et al. (2013) propose a pattern-based analysis to satisfy, on the one hand, certification and legal requirements for non-trivial tasks and, on the other hand, cloud security requirements. Lastly,

among the studies investigating IT security standards, Di Giulio et al. (2017, 2017a) offer a detailed comparison of FedRAMP, ISO/IEC 27001, C5, and SOC 2, looking at the standards and their adequacy in relation to the current threat landscape, and at the evolution of the standards overtime. The two studies, however, limit their scope to technical aspects related to completeness and effectiveness of the standards, but do not expand their conclusions to explain the possible reasons why the standards were created and do not consider the context surrounding their creation.

Previous research on IT security and privacy standards has adopted gap-analysis and classification approaches looking at the control frameworks and threats to cloud environments. However, in the research literature analyzed, only a few studies have been systematic and detailed in their observation of current security standards, while the great majority of them have dismissed existing standards without offering a real gap-analysis. Studies on threats, on the other hand, analyze the risks associated with vulnerabilities in IT environments, and many propose technical remedies. What most studies overlook, however, is a contextualization of those threats in the broader landscape of security standards adopted by the IT industry. While they focus on the controls adopted according to existing security standards, their conclusions are usually too generic to produce effective improvements. The absence of a thoughtful insight on the context and the function of the standards have limited the impact of the reviewed studies, thus creating the need for deeper understanding of the causes and consequences of the creation of multiple IT security and privacy frameworks.

CHAPTER 3: INFORMATION ASSURANCE[14]

The use of cloud technology creates new risks and vulnerabilities for information assurance. On the one hand, the benefits coming from using elastic and flexible IT infrastructure allow industry and governments to reduce their expenses. On the other hand, adequate safeguards to privacy and security are required to make cloud services usable without risks for confidentiality, integrity, and availability of information. Yet, higher levels of data privacy can be required to limit the access to the cloud market and build a protectionist strategy in favor of local service provider.

The first step to understand potential benefits and risks of cloud computing is to define what cloud computing is and what it does. Second, a careful observation of current research on security issues and vulnerabilities in IT environments is also necessary to understand potential risks coming from the adoption of cloud technology. Last, a clear definition of different approaches to privacy is required to understand what are the limitations in the use of technology and what measures are adopted to protect information, as well as the possible use of strict privacy protection as a barrier to foreign investments. In the following sections, I will define the context of my research giving a sense of the main cloud security issues and different approaches to information assurance and privacy in the EU and the US.

3.1. What is Cloud Computing and why does it matter?

Before the creation of the remote access to IT systems known today as cloud computing, access to IT resources has been based almost entirely on proprietary infrastructure and on-premises

[14] This Chapter includes material from previously published work. See Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K. Campbell, R., Bashir, M. (forthcoming 2017). "Cloud Security Certifications: A Comparison to Improve Cloud Service Provider Security". In the proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing (ICC 2017), Churchill College, Cambridge, UK. March 22-23, 2017. ACM Proceedings Series

systems. In this scenario, data and applications are centrally managed and processed, and single devices access their organization's data through local networks (Arasaratnam, 2011). Organizations adopting such model needs to invest their resources in making the system work efficiently and securely, provide day-to-day maintenance and be prepared to face critical events, such as data breaches or cyberattacks, as well as natural disasters. Conversely, cloud computing is a service model allowing remote access to computational, storage, and processing capabilities leveraging on infrastructure created and managed by third parties, the cloud service providers (CSP).

Cloud deployment models can be private clouds, when a single organization uses a dedicated infrastructure to access additional computational resources through the internet. The main difference between private cloud (owned by the CSP) and the traditional private infrastructure (owned by the organization) is in the distribution of responsibilities among actors interacting with the system. The organization is entirely responsible for managing private infrastructures, whereas the CSP is held accountable for most private cloud's malfunctioning or flaws. A second model is the use of community clouds, differing from private clouds in that their resources are available to multiple organizations known to the users. The infrastructure is still maintained and managed by a CSP, but only pre-determined organizations – such as companies in the same holding – can use its resources. The last model is that of public cloud. It allows access to multiple organizations and users (tenants) unaware of co-tenants' activity and identity (Arasaratnam, 2011). The reasons for choosing a public versus a private cloud depend on what the organization moving its services to cloud systems needs. On the one hand, privacy and security risks may be a motivation against the adoption of a public cloud model. The use of shared infrastructure could allow malicious co-tenants to access restricted information (an example is the

“side-channel” attack, which will be discussed in chapter five). On the other hand, the possibility of large economy of scale sharing the same infrastructure with multiple users makes possible for the CSP to offer affordable services to its tenants. Hence, access to convenient additional resources is a motivation to use cloud services.

In its most common configuration, public clouds can be divided into three paradigms: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS allows a tenant to utilize physical infrastructure at a standard fee, without direct costs associated to maintenance and physical security. The main benefit associated with IaaS is the opportunity for tenants to run their own software on the CSP’s system, including specific Operating Systems. PaaS creates a space where tenants can install their applications on predetermined Operating Systems. They rent a virtual machine that can be used for developing applications, or run compatible software. SaaS consists in the use of software applications dynamically allocated in the CSP’s infrastructure, with limited functionalities (Arasaratnam, 2011). A popular example of SaaS is the use of webmail, online document editors, document storage.

However, along with benefits deriving from flexibility, remote accessibility, and the absence of costs associated with maintenance, cloud computing does not allow the same control on tenant’s information as on-premises datacenters. Since information physically resides on infrastructure belonging to a third party (the CSP), risks for privacy and security are a common deterrent to the adoption of cloud models in an organization, and moving data and applications to cloud systems often requires trusting the CSPs and the security measures they adopt to protect their systems. The US government is an example of slow adoption due to privacy and security

concerns. In 2010, after careful evaluation of the benefits deriving from the adoption of cloud technology, and urging to reduce spending in IT infrastructure, the White House published the "Cloud First" strategy (Kundra, 2010), crafted to encourage federal agencies to move to cloud systems, and defining higher security requirements for CSPs supplying services to the Federal Government. The Cloud First strategy has led to a considerable reduction in federal expenditure in IT, moving the Compound Annual Growth Rate (CAGR) from 7.1% until 2009 to 1.8% in the 2009-2017 period (OMB, 2017, p. 288). However, the adoption of cloud services is still slow in the US federal government, with only 8.2% of the $ 89.9 billions for IT expenditure reserved to cloud services (p. 289). In addition, the US government has actively adopted only a minor percentage of the cloud services available on the market (FedRAMP, 2017a).

The adoption of cloud services, however, is not anticipated to decrease in the future. Following a consistent increase over the years, investment in public cloud services have grown of the 17.2% between 2015 and 2016, and investments in IaaS have increased by 43% in the same period (Gartner, 2016), suggesting a trend that will hardly reverse in the future. There are two elements relevant to promote the adoption of cloud services. First, the possibility of saving on IT expenditure is certainly relevant, but also increased attention of CSPs in the adoption of privacy and security measures represent a second possible reason. If cloud users are reassured on confidentiality, integrity, and availability of their data, the cloud becomes more appealing as compare to on-premises solutions. Two elements play a role in building up security and trust in cloud services: one is the understanding of threats and vulnerabilities to cloud systems, which represents a primary need to make these technologies secure against cyberattacks; the second is privacy protection, and the adoption of sufficient guarantees for users that their data are safe against unwanted access.

3.2. The Treacherous Twelve

Standards for cloud computing environments aim to provide a minimum security baseline for CSPs. The goal is to improve the tenants' level of trust in security and privacy of their processed or stored data. To maintain high level of confidentiality, integrity, and availability in the hosting systems, standards must include measures protecting against threats and security issues. Hence studying these threats and weaknesses is necessary to maintain a standard up-to-date.

Among various classifications of security issues, few have been constantly updated and industry-sensitive as those published by CSA. Since 2010, CSA's Top Threats Working Group has proposed multiple lists of threats affecting cloud environments (CSA 2010, 2013, 2016a). Last in the timeline is "The Treacherous Twelve: CSA's Cloud Computing Top Threats in 2016," a detailed study, based on a survey among 271 IT experts worldwide, on the top twelve issues in cloud security ranked in order of importance.

CSA's list of treacherous twelve does not distinguish the issues based on the actor originating them, and does not consider their technical or procedural nature. For example, some of the issues might stem from human error (e.g. data loss or insufficient due diligence), some others could generate as the result of malicious human action (e.g. data breaches, account hijacking, malicious insiders). At the same time, some of the issues are the result of exploitation of weaknesses embedded in the system (e.g. denial of service), other could descend from insufficient security policies and procedures (e.g. weak identity, credential and access management, abuse and nefarious use of cloud services).

Data breaches are first on the list as the most common and feared issue among the interviewee. A breach consists in an incident involving unauthorized access to information residing

in the system. It can involve sensitive or confidential information, including personal identifiable information (PII), and could generate financial losses, or serious privacy violation. A data breach can result from human error or a targeted attack conducted by external actors. Looking to data from 2015, more than sixty-four thousand confirmed breaches took place all over the world, with the public sector first in the ranking with 47,237 events (Verizon, 2016). Agents causing the breach may vary, and could consist in malicious software, hacking, or social engineering techniques, such as phishing (Verizon, 2016). The result of a breach is a disclosure of information to unauthorized third parties, with consequent damage for financial assets, or confidentiality of personal information. Second in order of importance are issues derived from weak identity, credential and access management. Weak passwords, certificates mismanagement, lack of two-factors authentication, are all exploitable deficiencies. As such, they could lead to other issues and nefarious actions. For instance, access to confidential information could pass undetected when an unauthorized person uses approved credentials.

Insecure interfaces or application programming interfaces (APIs) is third in CSA's ranking. The APIs are a common system to interact with cloud technologies, making possible for cloud customers (tenants) to connect their applications to cloud services. To this extent, APIs and user interfaces are a vulnerable access point to cloud services and their exploitation by malicious attackers can easily expose information stored in the clouds. System and Application Vulnerabilities is the fourth issue, which consists in the exploit of a system's or application's weaknesses to perform illegitimate activities. The existence of bugs in software applications can be discovered by malicious attackers and used to access confidential information. Phishing or fraud are an example of account hijacking, the fifth issue on the list. The presence of malicious insiders, the sixth issue in CSA's ranking, is a risk for sensitive information that can be accessed by

members inside of an organization. Malicious insiders refer to malicious or disgruntled employee using access privileges to perform unauthorized activities, an enormous risk especially when they may leverage on familiarity with the system to go undetected. Malicious insider generally falls into a broader category of threats, which is Insider Threats. It is defined as "an individual and, more broadly, the danger posed by an individual who possesses legitimate access and occupies a position of trust in or with the infrastructure or institution being targeted" (Catrantzos, 2012). Although not mentioned among CSA's treacherous twelve, a different issue still related to insider threat is worth of mention in this section: the exploitation of unaware employees to perform illicit activities on a cloud system. In this case, employees targeted by external actors are used as a vehicle for attacking the organization's system. An external attacker, for instance, could infect a mobile device belonging to an employee of a target organization with malware, and access the system when the employee connects his or her device to the internal network. Seventh on the list are the advanced persistent threats (APTs), a set of continuous attacks running surreptitiously on a platform and frequently introduced by direct hacking, use of USB devices, or penetration through partner or third party networks. An example of APT is Stuxnet, a malware introduced into the Iranian industrial control system using a USB flash drive, which eventually caused relevant damage to the Iranian nuclear program in 2010 (Chen, 2014).

Data loss is another common concern among the interviewee contributing to CSA's work, and refers to all those events imputable to events external to an organization, such as a natural disaster, and not related to malicious attacks. A risk due to factors internal to the organization is insufficient due diligence, which represents the ninth of the treacherous twelve. Conversely, if weaknesses involve access and use of cloud services, organizations can be concerned about the abuse and nefarious use of cloud services. An example are distributed denial of service (DDoS)

attacks, where a malware infects multiple devices connected to a cloud system and try to produce an overload to make it unusable for a certain period of time. DDoS leverages on multiple devices and collective computing capabilities typical of distributed systems. On the other hand, when only one device targets the system with an overload of requests to slow it down or make it unusable to other users, the attack is called denial of service (DoS), which is the eleventh threat in CSA's ranking. Last, shared technology vulnerabilities concern issues with the technology and infrastructure underlying cloud services used to offer multiple PaaS and SaaS products.

As clarified in this paragraph, a considerable number of issues could defect security of information stored and processed in the cloud. Some of the examples have shown how exploitation of weaknesses or poor management of security practices have caused financial losses or jeopardized the right to privacy of cloud users. Identification of the issues and determination of their possible causes is necessary to prevent them to happen. The inclusion of effective countermeasures in the standards is necessary to make them effective and relevant in assuring confidentiality, integrity, and availability of information in the cloud.

3.3. Approaches to Privacy of Information

The second element in creating a friendly environment to the adoption of cloud services are privacy safeguards. Higher attention to privacy controls sometimes works in disadvantage of industry stakeholders as it creates additional burdens requiring expensive audits and certification procedures. On the other hand, strong privacy measures work as a reassurance for end users on management and processing of their personal information. Data privacy plays a role in the willingness of private and public organizations to outsource their services, and on the possible risks involved in IT strategies involving outsourcing. In the general framework of an IT strategy,

an organization chooses to outsource its services for efficiency reasons, to enhance its agility, or reduce its operational costs. However, outsourcing also has risks; one of these is loss of control over data (Turban *et al.*, 2015, p. 405). Hence, to protect personal identifiable information or data, organizations are less willing to outsource their services and rather organize their IT strategies with the use of internal resources.

The EU and the US have two radically different approaches to privacy rights. Although a convergence in standards and best practices exist, regulations and policies adopted in the two blocks are far from being interchangeable. One example are rules on protection of personal data. The US, more favorable to business initiative and free market, have paid less attention to privacy of individuals – only recognized as civil rights – with large benefits obtained by organizations adopting aggressive and invasive marketing practices. The EU, on the other hand, recognizes privacy as a human right, and pays high attention to personal data collection and processing, sometimes with burdensome rules on industry.

General, cross-industry guidelines applicable regardless of industrial sector or country – the so-called Fair Information Practices (FIPs) – also exist in form of principles issued by various institutions, starting in the 1970s. Examples are the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued by the OECD in 1980. The US Federal Trade Commission (FTC) also issued a set of recommendation in 1998 enlisting five main principles, including integrity and data security (FTC, 1998). In general, FIPs aim to increase consciousness of consumers about why their data are collected, how they are managed, and what are the measures implemented to promote data security and integrity.

FIPs, however, are general, non-binding principles, and their enforcement depends on their transposition in each legal system. The EU Privacy Directive bases its text on the OECD list of FIPs and the eight main principles contained in it. The US has a general attention to FIPs principles, but inconsistent application in federal and statutory laws. Furthermore, while attention to basic principles – such as notice and choice – is the same as in the EU, other principles are not specified and recommended. Wang and Kobsa (2008) summarize the main privacy principles from the most commonly referred guidelines in a comparison table. From Wang's and Kobsa's table I have selected the OECD guidelines from 1980, the EU Privacy Directive, the FTC Safe Harbor principles and FTC FIPs (table 3.1) that are being presented in this section.

Table 3.1: Privacy guidelines/frameworks and privacy principles

Specification → **Principle ↓**	OECD Guidelines (OECD, 1980)	EU Directive on Data Protection (EU, 1995)	FTC Safe Harbor Principles (FTC, 2000)	FTC Fair Info Practice (FTC, 2000)
Notice/Awareness	X	X	X	X
Minimization				
Purpose specification	X	X	X	
Collection limitation		X	X	
Use limitation	X	X	X	
Onward transfer		X	X	
Choice/consent	X	X	X	X
Access/Participation	X	X	X	X
Integrity/Accuracy	X	X	X	X
Security	X	X	X	X
Enforcement/Redress		X	X	X

Source: Wang and Kobsa, 2008.

3.4. The US Scenario

The EU and the US stands at two very different positions on privacy. Although among the first countries to develop guidelines on the protection of personal data in the 1970s, the US has never followed a consistent path in privacy regulation, shared among all the states. The US has a sectoral approach, where industry-oriented norms provide for details on personal data

management. State laws have only a limited range of application not being applicable at a federal level, and the only protection at a federal level could be found in the Fourth amendment to the US Constitution – protecting against search and seizure – and Tort Law protecting against intrusion upon seclusion as derived from William Prosser's (1960) doctrine.

Some sectors such as finance, healthcare, and children's privacy, are the ones perceived as more at risk, and therefore covered by a higher level of protection with binding norms.[15] The reason for a sectorial rather than a comprehensive protection could relate to market efficiency, as proposed by Cockfield (2010) claiming,

> The sectoral protections are often promoted under the market efficiency rationales: one view suggests that the market will do a better job at reaching a balance between commercial needs and privacy interests because it is simply good business to align a business's collection practices compare with customer needs (2010, p. 56).

It is in the interest of businesses to guarantee a lower protection level, receiving consequently benefits from enhanced agility. The boundaries provided by a strict regulation are a limit for thriving free market and free business initiative. At the same time, if the interests of under-represented categories, people subject to higher risks, or particularly delicate interests are involved, other specific considerations need an assessment. As it happens with financial matters or children's privacy, promotion of free market must be reduced in favor of a protectionist approach, since there is not a tradeoff between economic benefits for businesses and defense of human rights or minorities.

[15] For example the Gramm–Leach–Bliley Act in 1999 or the Health Insurance Portability and Accountability Act of 1996

At a more general level, Privacy rights in the US legislative system are defined as civil rights. Their protection and importance is therefore equivalent to trade and business interests.

3.5. The EU Scenario

Conversely, in the EU privacy rights are considered as Human Rights. The detailed regulation followed by the EU gives little agility to business initiative, but is certainly reassuring for users on integrity and safety of their data.

The Directive 95/46/EC of the EU – at a supranational, European level – provides the core legislation while national laws and recommendations provide specific details about the protection of personal data, collected in the EU, both within or outside of the EU. International guidelines exist on the issue, coming from the Organization for Economic Cooperation and Development (OECD), which first published them in 1980. The guidelines are structured in different principles, all adopted in the cited EU Directive (Shimanek, 2001). These consist in eight different pillars, built to guarantee a transparent processing of personal data and easy access of their data subject to them. According to the principles, other than a general respect of openness and transparency of procedures and processes, limitations to collection without consent are imposed, which means that only under a specific purpose personal data can be collected and used. Furthermore, the purpose must be specified to the data subject before their collection takes place. National schemes are also required to assure data quality, which means accurate, complete and up-to-date information. To guarantee quality, the data holder must guarantee the data subjects with full access to their data, and the possibility to request correction – or even cancelation – of inaccurate information. At the same time, unauthorized access must be prevented, as well as data disclosure without consent of

the data subject. To assure the respect of the above principles, a strong control is required on controller and processor of the personal data.

The core features of the EU Directive are not far from the elements considered more than twenty years before in the first European law on the issue, even before the OECD's guidelines. In 1970, the German federal state of Hesse introduced the first data protection act in reaction to the computerization and centralization of information held by the government. Similar regulations were adopted by the other member states until the formalization with the EU Directive (De Hert & Papakonstantinou, 2012).

According to point 7 of the introduction to the EU Directive, it was necessary to create a general and common framework in order minimize the existing differences in national laws, harmonizing the various legal provisions existing at the time. A fragmented scenario would be cause of distortion in competition, and an obstacle to economic activities in the Common Area (Directive 95/46/EC). However, the reform did not completely achieve the expected effects at a transatlantic level, since perplexities from American investors kept being raised due to complexity and lack of orientation in the European legislative landscape. Hence in 2012, the European Commission announced the reform of the privacy Directive with the preparation of a Regulation. The Commission used a Regulation, which is immediately enforceable within the member states without being transposed into national law. The aim of the Regulation is to achieve, once again, harmonization out of a fragmented regulatory regime in 28 countries, providing at the same time a boost for innovation, growth and reliability in e-commerce and online services (European Commission, 2012). The General Data Protection Regulation was published on April 14, 2016, and will be effective starting by May 2018, fully replacing the Directive. One of the prominent

innovations that the Regulation will promote is simplification of the procedures necessary to obtain authorization for data collection and use, such as the notification to national authorities in case of automated processing. This specific provision traces back to the 1970s, when automatic data processes were an exception. With new technologies and widespread computing, the same type of processes has become extremely common, making less meaningful, if not useless, an obligation to notify them (De Hert & Papakonstantinou, 2012). More simplification will be also provided in the access to authorizations for foreign companies in processing data collected in the EU, since the authorization coming from the authority of one country member will be valid and applicable for the same activity on the whole territory of the EU.

Although source of controversies for the possible consequences on foreign companies, another important innovation introduced in the Regulation is a provision on what has become known as the "Right to be Forgotten." It gives to the EU citizens the right to ask for the erasure of data that are irrelevant or no longer necessary – or the erasure of links to them – even to foreign companies acting as service provider for EU citizens. The enforceability of the right shall be evaluated on a case-by-case basis (European Commission, 2014).

In the EU, national laws and recommendations provide specific details about the protection of personal data. There are not industry-specific norms, since the same principles of the Directive and the Regulation are applicable to every sector, from government to healthcare or finance.

3.5.1. Privacy – The EU drivers

Inquiring about the reasons leading to a strict regulation, one explanation emerges looking to the structure of Data Protection and Privacy Rights in the EU. Primarily coming from the broad

interpretation of the Article 8 of the European Convention on Human Rights (ECHR) of 1953 made by the European Court of Human Rights (Kilkelly, 2003), and more recently by explicit provision of the 2009 Treaty of Lisbon, Data Protection is brought to the rank of human rights. The high consideration for Privacy comes from history, from open wounds and violation of human rights in Europe during WWII. The brutality of the Holocaust, perpetrated by the Nazi regime in the 1940s, has seriously captured the public opinion, at the point of requiring the higher level of protection against abuses that favored the escalation of violence that took place. One of the violations was the use of census data and personal information to reconstruct racial identities, or the belonging to minorities, leading eventually to extermination. In the specific case, it was clear immediately after the WWII that processing personal data, even if collected for innocent purposes, could lead to identification of citizens of ethnic, religious, or other minority groups, revealing even concealed information. It was a risk too big for not being protected at the highest possible level (Singleton, 2002). After German re-unification in 1989, the political initiatives to increase transparency in the institutions and guarantee equal conditions to citizens of the former two blocks reignited the debate on privacy. The surveillance apparatus created by the East German secret police (Stasi) was immediately perceived as a violation and marked as illegitimate (Sperling, 2011), contributing even further to shape the perception of privacy rights as a fundamental right.

3.6. Privacy – New perspectives and controversies

On one side of the Atlantic Ocean, the EU is on its way of developing a privacy regime that could harmonize a fragmented framework among the member states. Moreover, the reform is aimed to simplify the regime of authorizations and procedures required for compliance to the EU legal system. Meanwhile, on the other side of the ocean, the strict regime of the EU has caused problems for US investors through the years, when they have been forced in a continue struggle to

comply with fragmented regulation and referring each time to a different authority in the member states.

Besides harmonizing the EU framework on privacy, the Regulation plays a role in a bigger strategy. European lawmakers are pushing the US to endorse an equal level of protection in federal law (European Commission, 2010). The attempt is not new in the trans-continental relations scenario. Already considered a key issue, data flows were the subject of extensive discussion in the late 1990s, when the European Commission and the US government were involved in a debate around the structure and approach to data protection. At that time, the European Commission tried to convince the US for almost one year to enforce a stricter regime for data protection. Cultural differences and free speech divide were an obstacle for the US to be recognized as reliable under the Directive (Dowling, 2009).

Lacking a broader consensus on privacy rules, the EU and the US created a tailored solution able to allow transatlantic commercial relations, where the single business could adopt the necessary actions to comply with the EU Directive on a voluntary basis. The agreement was called "Safe Harbor." Although the Safe Harbor Agreement was not applicable in some areas, such as the financial sector, it represented an important precedent in terms of interaction between the US and the EU systems and enforcement of high protection standards. However, the rules contained in the Safe Harbor Agreement were often unattended by the US companies (European Commission, 2002), and the agreement was recently overturned with the C-362/14 case, brought in front of the European Court of Justice (ECJ) questioning on the safety and reliability of the Safe Harbor (Scott, 2015). In the case, the ECJ recognized the interference of the US government in fundamental rights of individuals when the data holder, a US based Internet Company, allowed

the US authorities to access EU citizens' data to execute intelligence activities (Court of Justice of the European Union, 2015).

To replace Safe Harbor, the US Department of Commerce and the European Commission issued in January 2016 a new program, the "Privacy Shield." The framework of the Shield includes stricter obligations to US based companies. For example, additional limitations apply to data transfer to third parties, especially if based outside of the EU; Privacy Shield approved companies must include additional notice requirements in their privacy policies, and further restrictions apply to data retention (Goldstein et al. 2016). However, in the opinion of scholars and institutions (Goldstein et al. 2016, Voss 2016), the new Privacy Shield does not assure adequate protection to EU data, and does not include sufficient measures to comply with the GDPR.

3.6.1. Privacy in International Trade

Disagreement on privacy rights were also one of the themes during the negotiation of the Transatlantic Trade Investment Partnership (TTIP). The TTIP is a proposed trade agreement on services and goods between the EU and the US. Its negotiations started in 2012 trying to achieve regulatory harmonization between the two parties, especially by reducing non-tariff barriers to trade that are slowing down the exchange of goods and services (Malmström, 2014). The TTIP is not a traditional trade agreement as the trade barriers between the two sides of the Atlantic are already some of the lowest in the world and considering the level of trade between the EU and US. The idea behind the TTIP consists on deepening the liberalization of trade through deep harmonization of regulations and standards. The TTIP is based on a three pillars model: market access; harmonization of regulatory cooperations; rules of trade related to issues such as

intellectual property rights, energy, sustainable development, and so forth (De Ville, and Siles-Brügge, 2016).

Among all the issue areas negotiated in the TTIP, one of the most controversial has been on personal data flows (Renda and Yoo, 2015). By reducing the distance between their regulatory frameworks, the EU and the US hope to make the cross-border access to services considerably easier, and data flows are a significant component on trade in services, which often requires transmission and processing of personal information. Three years into the negotiations, the European Commission denied the possibility that privacy would be negotiated stating that "Data protection standards won't be part of TTIP negotiations. TTIP will make sure that the EU's data protection laws prevail over any commitments" (European Commission, 2015).

Looking to past negotiations on privacy rights, the strict position of the EU suggests the attempt to create an international standard, a benchmark for leading a worldwide reform of privacy rights. The European Commission stresses how the privacy framework provided by the EU is a broadly recognized set of principles, rules and criteria, especially under the full recognition of the OECD. EU privacy standards have been set as the basis for new legislation in Asia and Africa (European Commission, 2010, p. 15). At the same time, the European Commission recognizes how the same roles are not a guideline in the US, which incorporates in its privacy roles only some of the basic principles of the Directive. The European Commission (2010) states that:

> The scope of these laws are very limited, leaving much information collection to be regulated by other rules, such as the rules against unfair or deceptive business practices. However, this has, if anything, served to underline the overall weakness of the USA model (to the extent that one can speak of a single model there). The

> basic European principles should therefore be re-affirmed and, if anything, strengthened; and efforts to obtain their adoption world-wide should continue (p.15).

As the EU-US controversy on privacy rights does not shrink in size and depth, the EU moves forward with initiatives promoting European IT development. On the one hand, the EU strategy is centered on demonization of US companies such as Google or Facebook, and protecting "EU champions against the current domination of US internet companies" (Renda and Yoo 2015). Comparing the thirty largest "blue-chip" German companies enlisted in the DAX index to only the first five largest US tech firms in the field of IT and web-based technologies – namely Apple, Amazon, Facebook, Google, and Microsoft – the astonishing result is a total value of $1.3 trillion for the former to a total value of $1.8 trillion for the latter (Fairless, 2014). Narrowing the observation down to cloud services, of twenty-five public cloud companies providing services in Europe, the first EU based company is only at the eight place, and seventeen US based companies control the 83% of the entire market (Barker 2016). Being European investments in IT far lower than the American, and being the US the first IT exporter to the EU, the boundaries created by strict regulation in data flows are also a possible form of protectionism in favor of developing European IT companies (Singleton, 2002). To enhance European investments on IT, it becomes necessary to reduce US investments and create opportunities for the local IT industry to grow. The attention shifts from a matter of human rights to the control of the Internet, with all its potential value as the engine for the global economy (Fairless, 2014).

On the other hand, the EU strategy is to promote IT development initiatives among member states and at a pan-European level. This is the main purpose of one of the seven pillars in the

Europe 2020 strategy, which is the promotion of a Digital Single Market. The Digital Single Market strategy is built on three policy areas: first, improving access to digital goods and services, creating a marketplace where EU citizens can buy and sell with no additional fees; second, making digital technology a driver for economic growth, taking advantage of the possibilities it offers; third, creating a favorable environment, allowing digital networks and services to thrive with favorable rules and infrastructure (European Commission 2017). The creation of a Franco-German cloud firm is an example of initiative that fits into the third area. The effort of the French and German Governments in the promotion of a European Cloud started in 2015 (BMWI, 2017) in a joint effort of the French national cybersecurity agency (ANSSI) and the German Federal Office for Information Security (BSI) with the goal of "cementing Europe's position as leader in the digital economy" (Gouvernement Français 2017).

In the context of cloud services, vulnerabilities and security flaws are the first element to consider to build a trusted cloud. Cloud security standards must account for newer threats and vulnerabilities, and include among their controls adequate protection measures. A secure cloud can find larger adoption as it becomes more secure, and an increasing number of organizations are encouraged to migrate their IT services and applications from an on-premises model to cloud environments. Privacy of information is another element to consider when adopting cloud services. If confidentiality and integrity are preserved, an organization is more favorable to move its information to infrastructure maintained by third parties. Yet, privacy standards can be used in the EU as a mechanism to protect domestic investments. As a consequence, the conflict between EU and US on the issue is lively than ever, as the EU tries to set a standard that the US is not willing to recognize as such, being not beneficial for trade and business investments.

CHAPTER 4: ANALYZING THE STANDARDS[16]

To understand the impact and effectiveness of C5, FedRAMP, ISO/IEC 27001, and SOC 2 on cloud security, and explain the stratification of security standards in the past ten years, an observation of the context surrounding the standards is necessary but not sufficient. What helps clarify differences, strengths and weaknesses of each standard is a direct comparison of their provisions.

All the four frameworks in my study are based on controls organized in groups or families. Only two of the standards – ISO/IEC 27001 and C5 – are published along with the control measures. The other two rely on external sources: FedRAMP refers to a selection of controls in NIST SP 800-53, SOC 2 is based on TSPC. In my study, I evaluate the adequacy and completeness of security measures in the standards in relation to cloud security and the current threat landscape comparing the provisions in the standards to each other. For this purpose, I choose to use a third-party checklist with a similar structure to the four standards and cloud-specific security measures, and compare each of the standards with it. The third-party framework used in my study is the Cloud Control Matrix (CCM), created by the Cloud Security Alliance.

The first advantage in using the CCM as an external framework is its completeness and detailed descriptions of a comprehensive set of security controls, which allows a more detailed and accurate evaluation of the privacy and security measures in the standards. Second, CSA offers a

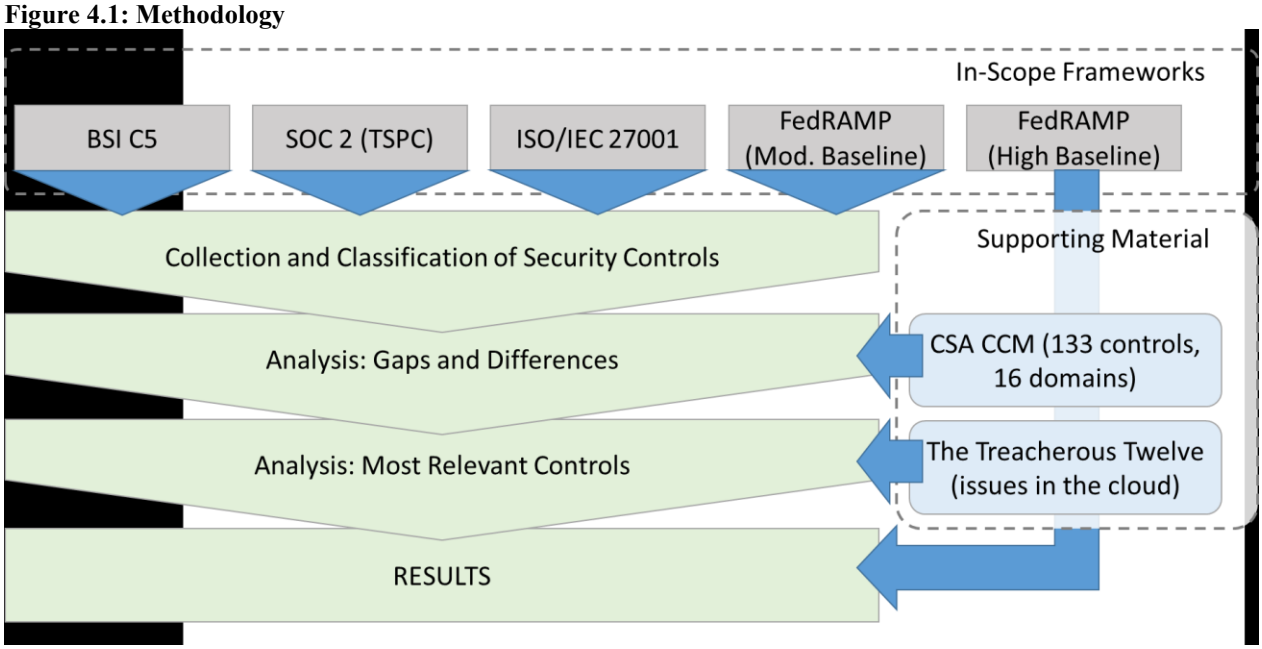
[16] This Chapter includes previously published material. See Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K. Campbell, R., Bashir, M. (forthcoming 2017). "IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers". To be presented at the International Workshop on Assured Cloud Computing and QoS Aware Big Data (WACC '17), Madrid, Spain. May 14, 2017. See also Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K. Campbell, R., Bashir, M. (forthcoming 2017). "Cloud Security Certifications: A Comparison to Improve Cloud Service Provider Security". In the proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing (ICC 2017), Churchill College, Cambridge, UK. March 22-23, 2017. ACM Proceedings Series

third-party viewpoint, with controls that are not NIST, BSI, AICPA, or ISO/IEC specific. The choice of a checklist of controls to be used as an analytical framework is determined by the need of obtaining measurable results, by verifying how many requirements in the CCM are met by the other frameworks.

In my study, I assume that CSPs certified against one or more standards adopt adequate policies and security mechanisms to be compliant with the standards overtime. Compliance with a security standard is not *per se* a guarantee of security, and effectiveness is also related to enforcement of security recommendations and best practices within an organization.

I limit my observation to the controls relevant in each version of FedRAMP (2011 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 2011. Therefore, I 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 is from 2009. I 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, I draw my numerical data from observation of the basic requirements.

Figure 4.1: Methodology



Source: Di Giulio et al., 2017a

To conduct my systematic analysis, I follow a sequence of four steps where I collect and then operate on a selection of data on security controls (figure 4.1). The first step is to collect and classify the requirements in FedRAMP, ISO/IEC 27001, SOC 2, and C5. Then in step two, I analyze the results of my comparison to identify gaps and differences. I use the categorization provided by CSA in the most recent version of their Cloud Control Matrix (CCM), version 3.0.1 released in January 2016 (CSA, 2016) to combine the controls required in the four standards. The CCM provides a classification of security and privacy enhancements organized into 16 control domains, and a total of 133 single controls (Table 4.1).

Table 4.1: CCM Control Families and Controls

Control Family ID	Control Family Name	# of Controls
AIS	Application & Interface Security	4
AAC	Audit Assurance & Compliance	3
BCR	Business Continuity Management & Operational Resilience	11
CCC	Change Control & Configuration Management	5
DSI	Data Security & Information Lifecycle Management	7

DCS	Datacenter Security	9
EKM	Encryption & Key Management	4
GRM	Governance and Risk Management	11
HRS	Human Resources	11
IAM	Identity & Access Management	13
IVS	Infrastructure & Virtualization Security	13
IPY	Interoperability & Portability	5
MOS	Mobile Security	20
SEF	Security Incident Management, E-Discovery & Cloud Forensics	5
STA	Supply Chain Management, Transparency and Accountability	9
TVM	Threat and Vulnerability Management	3

Source: CSA, 2016

CSA's classification offers a direct reference to controls from the 2011 FedRAMP ATO requirements, from ISO/IEC 27001:2005 and 2013, and TSPC 2009 and 2014. In November 2015, CSA released a public consultation to update the CCM, including the new controls in FedRAMP 2015. I include CSA's matching of new controls from that document in consultation within my analysis and combine them with the others. However, since the document has not been officially released as an update to the CCM, I use the content referring to the newest release of FedRAMP as a mere guideline, and reinforce the observation with further considerations.

In the case of C5, BSI has published a reference guide along with the official control list. I use this document as a first guide in matching the controls in C5 with those in the CCM. Then, I verify the correspondence with in-depth content analysis. The analysis builds on a full-text search of C5 provisions based on keywords from the controls in the CCM, and a one-by-one verification of controls in the CCM not matched with controls in C5. Due to high technicality and detail in the controls, and a certain degree of interpretation to verify the correspondence of security measures in different frameworks, the use of analytic tools has been precluded. The same is true for the use of keyword generators, largely based on quantitative principles (i.e. recurrence of a word in a given

sentence). Further supporting material is the NIST SP 800-53, which includes reference and matching to ISO/IEC 27001. Since both CCM and C5 Referencing Table have references to ISO/IEC 27001 and TSPC, NIST SP 800-53 represents a support to connecting FedRAMP (based on NIST controls), and the other frameworks.

Similarly, TSPC are referenced in the CCM only for the 2009 and 2014 version, while TSPC 2016 are excluded. In this case, however, there are only minor differences between TSPC 2014 and 2016 among common criteria and controls impacting confidentiality, integrity, and availability, and the only major revision is the addition of privacy criteria (AICPA, 2015a). Therefore, I focus only on the differences between the two most recent versions, verifying that the changes do not impact the correspondence to the CCM. I verify if the changes and the additional privacy criteria compensate for the controls missing in the matching of TSPC 2014 using the same keyword-based full text search adopted for C5.

In the third step, after matching the controls on the CCM, I operate a further selection on the controls missing from the comparison, skimming on the less relevant to concentrate on the most compelling ones. To evaluate the relevance of each control, I rely on the definition of threats to cloud environments and their severity as defined in the literature, and especially the list of threats identified with CSA's publication "The Treacherous Twelve," which is natively integrated with CSA CCM. Concentrating on the controls lowering the risk coming from one or more of the Treacherous Twelve, I obtain a more accurate evaluation of effectiveness, as well as the completeness of ISO/IEC 27001, C5, SOC 2, and FedRAMP against the requirements suggested in CSA CCM.

In the last step, as I analyze the missing controls in details, I go through the additional 96 controls and enhancements in FedRAMP high baseline – only available after July 2016 – to verify to what extent they can mitigate the deficiencies in FedRAMP 2015 moderate baseline. The final result is a selection of security requirements missing in FedRAMP moderate and high baseline, C5, SOC 2 based on TSPC 2016, and ISO/IEC 27001:2013, with the potential of creating security flaws in cloud environments.

CHAPTER 5: STANDARDS IN COMPARISON[17]

In this chapter, I present the findings of my empirical study of C5, FedRAMP, ISO/IEC 27001, and SOC 2. I detail the mismatches, and their evolution over time, in the mapping between the available versions of the standards and the CCM. I refer to missing controls as the controls in the Cloud Control Matrix used as the analytical framework (See Table 4.1). After presenting the quantitative results, I move to discuss them in the context of cloud security and in relation to the current threat landscape. I discuss the controls omitted in the four standards following a basic threat model, where the possible threats stemming from missing security measures are presented and organized. The threat modeling gives a more concrete dimension to the omissions in the standards, helping a better understanding of possible vulnerabilities resulting from the adoption of the standards and their gaps.

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 satisfied in TSPC 2014 and identical controls in TSPC 2016 (Section CC5 of the TSPC). FedRAMP rev. 3, released in 2011, shows 45 omissions. In contrast, the CSA's matching claims that there are only 44 omissions in total. However, after a careful review, the control Data Security & Information Lifecycle, Data Inventory/Flows (DSI-02)

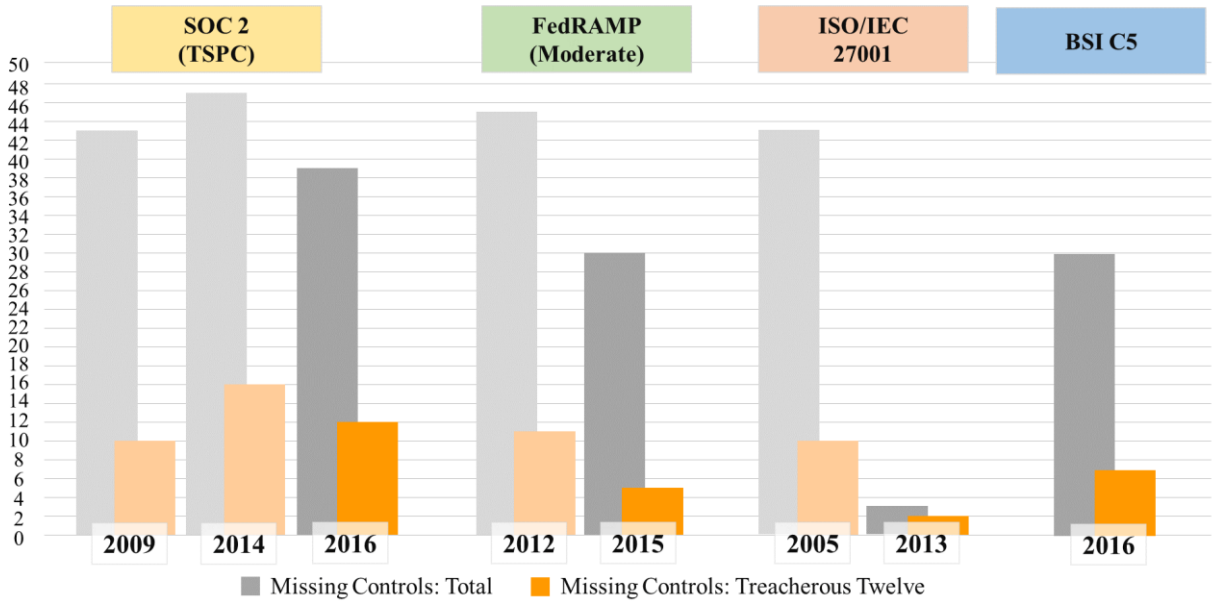
[17] This Chapter includes previously published material. See Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K. Campbell, R., Bashir, M. (forthcoming 2017). "IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers". To be presented at the International Workshop on Assured Cloud Computing and QoS Aware Big Data (WACC '17), Madrid, Spain. May 14, 2017.

appears to be signaled as fulfilled in FedRAMP 2011 by mistake, since the control signaled as adequate in FedRAMP does not relate to DSI-02.[18]

Compared to its older version, the 2015 release of FedRAMP shows a significant improvement. However, it still omits 30 controls from the CCM. ISO/IEC 27001 satisfies all but 43 controls in its 2005 release and 3 controls in the 2013 version (Figure 5.1).

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.

Figure 5.1: Total Missing Controls and Relevant for the Treacherous Twelve



Source: Di Giulio *et al.*, 2017a

Interestingly, two control domains are completely or substantially omitted in most of the analyzed frameworks. The first domain is Mobile Security (MOS). ISO/IEC 27001:2013 is the

[18] The control DSI-02 in the CCM is named "Data Security & Information Lifecycle Management - Data Inventory / Flows" and requires full documentation of data flows of the organization. The control in FedRAMP 2012 signaled as matching is SC-30, which is named "Concealment and Misdirection" and relates to the reduction of the attack surface of the system by using concealment and misdirection techniques such as randomness or virtualization.

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.

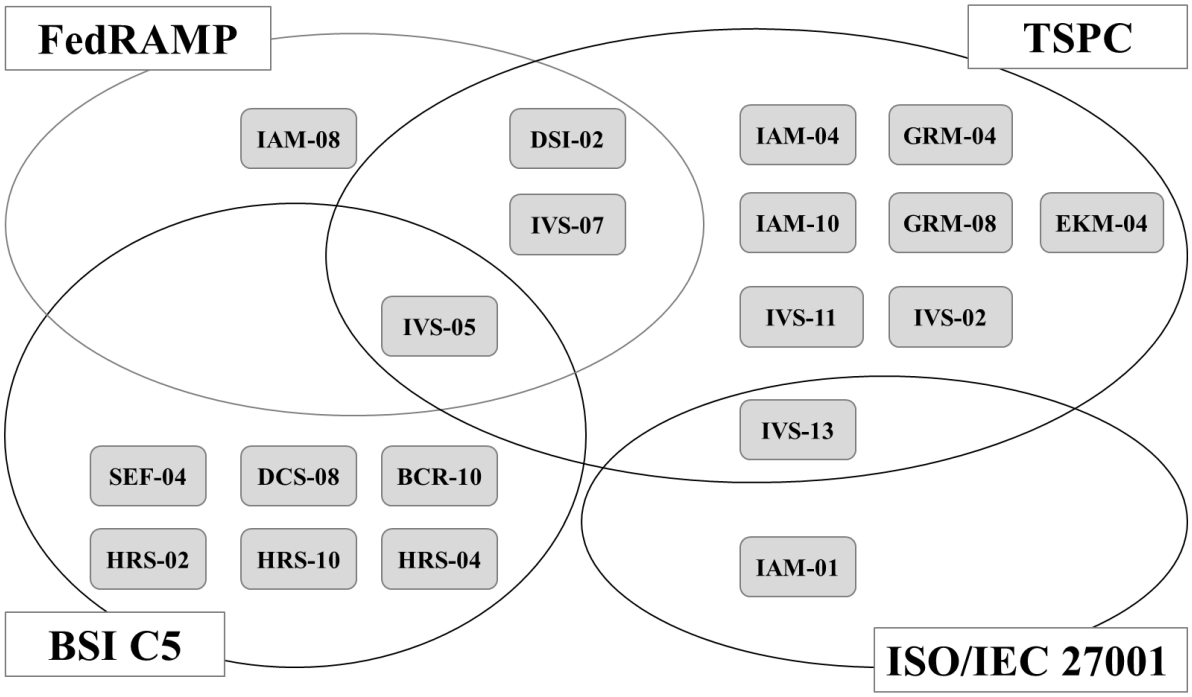
In the control domain Supply Chain Management, Transparency and Accountability (STA), the referred frameworks show significant gaps, except for ISO/IEC 27001:2013 and C5, which cover all security requirements, and TSPC 2016, which omits only 2 of them.

The number of gaps and omissions indicated thus far, however, is substantially reduced when the analysis includes the relevance of the omitted controls according to their impact on at least one of the Treacherous Twelve. Including a consideration on threats and vulnerabilities, it becomes possible to focus on the most significant controls and obtain a more realistic view of the impact of each framework in terms of security and privacy of information hosted in the cloud.

Once the selection applies, the average drop in the number of omitted controls is close to 68%, with a peak of nearly 83% for FedRAMP 2015, 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 2011, 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.

Focusing on the controls relevant for the Treacherous Twelve, 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.

Figure 5.2: Venn's Diagram of omitted controls overlapping in the four standards



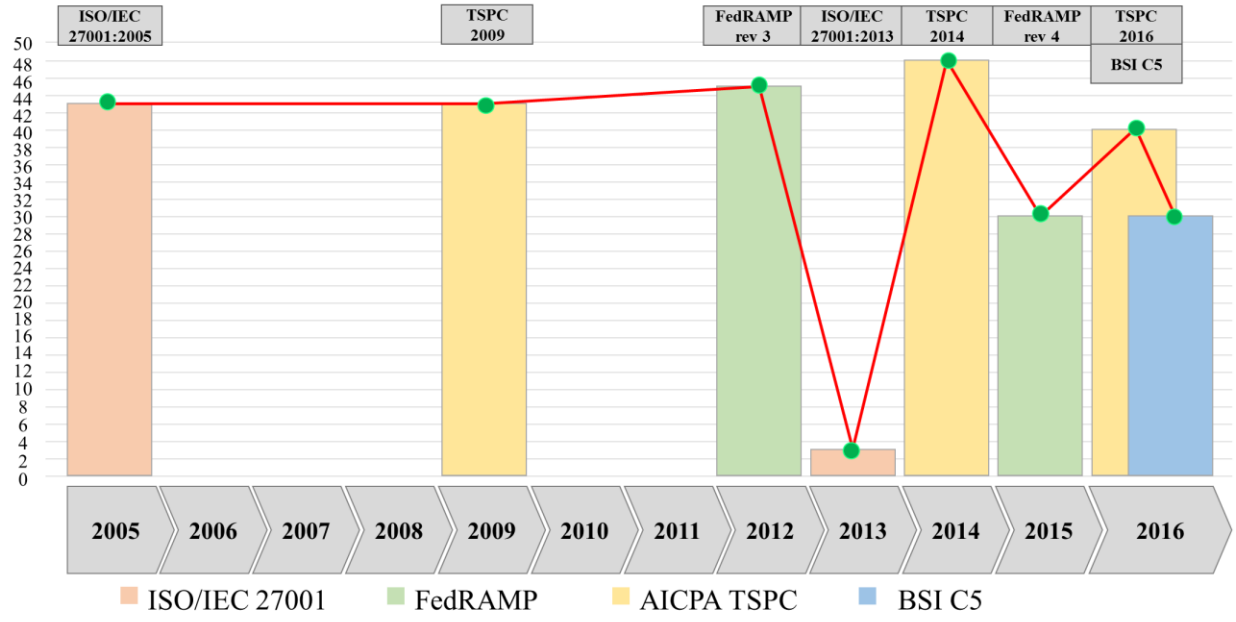
Last, narrowing the observations to the most recent version of each framework, there is an absence of significant overlap among all four standards with respect to the omitted controls that concern the Treacherous Twelve. Certainly, the small number of omissions in ISO (2 controls) reduces the possibility of overlap. Still, limiting the observation to TSPC, FedRAMP, and C5, it looks like only one control is missing in the area of virtualization security (IVS). 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 (Figure 5.2).

5.1. Discussion

Observing the results of the analysis, it stands out 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 5.3). 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 it showed 43 omitted controls, after narrowing the selection based on the Treacherous Twelve, 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 helps fulfill the requirements in the MOS and IPY domains, accounting for 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.

Figure 5.3: Timeline of omitted controls (total) in the four standards



Source: Di Giulio *et al.*, 2017a

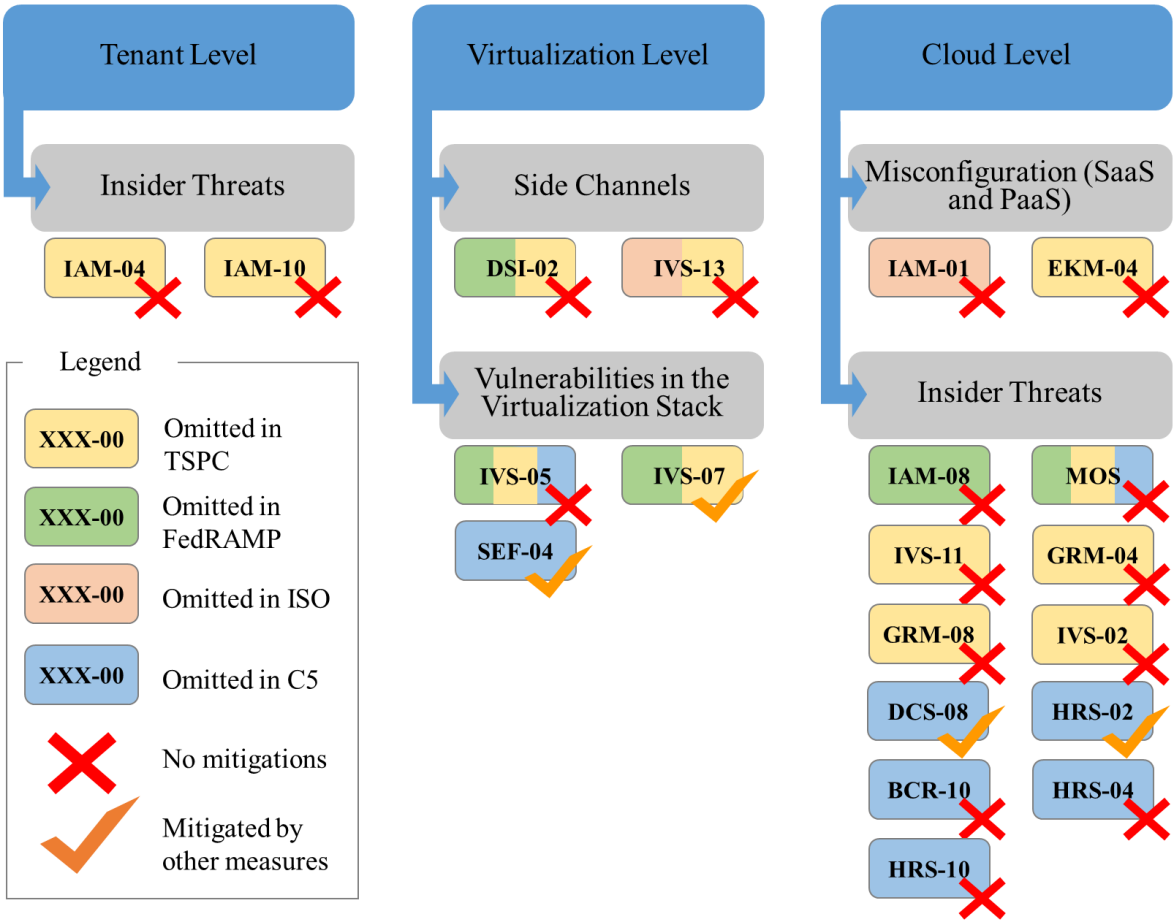
A good improvement in TSPC can be found in the transition between the 2014 and 2016 versions by looking at both the total omitted controls and only the ones relevant to the Treacherous Twelve. AICPA introduced a new set of privacy criteria in the last release, thus providing a more accurate set of criteria 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 Treacherous Twelve-relevant controls (12 missing in 2016, versus 10 in 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.

After narrowing down the observation to the current version of each framework, and focusing the attention to the most relevant security issues with respect to the Treacherous Twelve

selection criteria, it stands out that nineteen controls in the CCM 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 (Figure 5.2). As noted earlier, two control domains, MOS and IPY, although not considered relevant for the Treacherous Twelve, are missing or considerably affected by omissions in C5, TSPC, and FedRAMP. However, controls in MOS are extremely relevant for information assurance. Mobile devices are a common target of cyberattacks, and their vulnerabilities are easily exploitable to obtain unauthorized access to cloud systems (see paragraph 4.1.3). For this reason, in spite of the absence of mobile security measures among the controls involved in the Treacherous Twelve selection, I include consideration of their omission in my detailed analysis.

The threat model used to organize possible attack vectors in this study 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 5.4).

Figure 5.4: Attack model based on omitted controls



Source: Di Giulio *et al.*, 2017a

5.1.1. Tenant-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 and being excluded from considerations on security certifications of cloud vendors. CSPs, on the other hand, may offer additional security measures including, but not limited to, malware detection to improve security of the single VMs (Jiang *et al.*, 2007; Jones *et al.*, 2006; Jones *et al.*, 2008; Lamps *et al.*, 2014; Payne *et al.*, 2008). However, the existing work on those measures is not stable enough to be part of a certification standard addressing full responsibility on CSPs, and must be excluded from this study.

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.

5.1.2. Virtualization-Level Attacks

In the second group, there are attacks perpetrated at the virtualization level. An example are those 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 (Hendre and Joshi, 2015; Liu et al., 2015; Rasheed, 2014; 2014a). 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 (Fernandez et al., 2014), or escalation of access privileges (Ormandy, 2007). 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 (Beckers et al., 2013). 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 (AWS, 2016), or such as in the case of Docker Containers (Docker, 2015). 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). We must keep in mind that FedRAMP is a US requirement, and concerns cloud services for the Federal Government. FISMA requirements, which are generally applicable to federal information systems, also apply to the operating systems used in cloud environments if under the responsibility of the tenant. Conversely, TSPC were not designed specifically for federal

agencies, and their shortcomings are not necessarily mitigated by complementary government 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.

5.1.3. Cloud-Level Attacks

Two classes of vulnerabilities are part of the last group of threats in the threat 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 be missed. 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.

The second class of vulnerabilities consists of insider threats (see section 2.2). 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 (Beckers *et al.*, 2013). In addition, among the provisions of NIST SP 800-53 which constitutes the reference checklist for FedRAMP, the US Federal standard 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), and 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 (Huh *et al.*, 2013).

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 (Drake, 2015; Goodin, 2016). At the same time, specific vulnerabilities in Android can be exploited to access restricted corporate network resources (Perception Point, 2016; Goodin, 2013). Furthermore, mobile devices based on Android, a Linux-based operating system, are vulnerable to recently discovered flaws such as the “DirtyCOW” (Goodin, 2016). 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.

CHAPTER 6: CONCLUSION

The assessment of FedRAMP, C5, SOC 2, and ISO/EC 27001 on the analytical framework provided by the 133 controls in the CCM shows considerable gaps. Although patches and improvements have been introduced with the revisions occurring to the standards over the years, multiple threats could be created and vulnerabilities exploited at a tenant, virtualization, and cloud level. Narrowing down the analysis to the most relevant controls in the CCM, selected according to their connection to the Treacherous Twelve issues in cloud computing presented by CSA, the number of mismatches drops considerably. Yet, the standards still show gaps and shortcomings. Of 133 controls in the CCM, 82 are considered relevant for the Treacherous Twelve: only 63 controls are currently addressed in all the four standards, while 19 controls are missing in one or more of them. The first important consideration is on the type of protection that the four standards guarantee. As long as roughly 77% of the core security measures (63 of 83 controls) are the same, there is not a substantial difference in their purpose or security goal. FedRAMP, ISO/IEC 27001, SOC 2, and C5 all aim at creating a baseline security in IT environments. Nonetheless, there is significant complementarity among the four standards. Of nineteen controls missing in the matching, only four are missing in more than one standard (see figure 5.2), highlighting interesting differences in the approach to cloud assurance. FedRAMP is a US Federal authorization, and must be looked in context. Controls missing in FedRAMP could be compensated by other regulations, such as FISMA, which requires further security measures to Federal Agencies using IT systems. Still, FedRAMP's provisions show high priority to technical protection measures, but less attention to policies and procedures that the CSP must approve and enforce. The requirements in TSPC, used for SOC 2 assessments, result sometimes too general and do not guarantee adequate security and privacy to data residing in cloud environments. There are multiple vulnerabilities not covered

with SOC 2 audits in different areas. Trying to be comprehensive and versatile, SOC 2 fails to protect against specific vulnerabilities. In line with it, SOC 2 did not benefit of the update of TSPC in 2014 with their reorganization into general categories and substantially reducing the number of controls, and still obtaining only minor improvements with the 2016 review. ISO/IEC 27001 is similarly general in its scope, and demands high attention to policies and procedures of the service organization. Yet, ISO/IEC 27001 includes detailed technical controls, and its provisions are adequate and up-to-date in relation to the current threat landscape. Its attention to threats and vulnerabilities is clearly shown in its 2013 update, when mobile security and new technologies, such as cloud computing, were strongly considered, and that helped the standard to improve dramatically. Last, C5 is designed to work for cloud security either as a complement to existing standards, compensating for missing security measures, or as a stand-alone checklist. It performs well as a complement: unlike SOC 2, but similar to FedRAMP, C5 compensates for the two controls missing in ISO/IEC 27001, protecting against misconfigurations and Side Channel attacks. Still, as a stand-alone certification C5's shortcomings cannot go unnoticed. Human resources and identity management are two areas of improvement where insider threat represents a possible security risk.

The overall assessment of the four standards reveals that they guarantee high protection when used in combination. A CSP compliant with multiple standards at the same time is more likely to have full coverage against threats and vulnerabilities. On the one hand, it justifies the co-existence of the four standards. Assurance framework can compensate one another for omitted controls when each has a specific area of strength. On the other hand, the four standards are perfectible with the addition of only a few integrations. Other than more attention to mobile security, only eleven controls are missing in SOC 2, six controls are omitted in C5, four in

FedRAMP, and two in ISO/IEC 27001. Perhaps, covering that "extra-mile," and introducing the missing security measures could be not hard to do. At the same time, it would make the standards more robust.

Still, if complementarity of the standards justifies their coexistence, it does not provide a justification for the creation of new ones when a combination of existing frameworks offer adequate protection. Looking to SOC 2, ISO/IEC 27001, and FedRAMP, they offer already full coverage of the CCM criteria (see figure 5.2), and they were issued long before the publication of C5. Although cloud security criteria are not based on jurisdiction, some may argue that FedRAMP is a US Government standard, thus not applicable outside of the US. Still, FedRAMP is based on NIST SP 800-53 and its security measures, which are universally applicable. Not only does C5 fail in recognizing the existence of FedRAMP, but also ignores NIST SP 800-53.

Once again, the results of the analysis of standards must be looked in context. Perhaps, similarly to what happens with privacy policies and the European protectionist approach, the reason why the EU promoted the creation of a new cloud security and privacy standard with C5 is to contain the US predominance of European IT markets, rather than improve security and cloud assurance. The additional burden of a certification on US-based companies plays a role in the broader context of market regulation. A comparable example is the case of document formats presented in chapter three, where the risk of an abuse of dominant position required a regulatory intervention to open up the market and avoid a lock-in effect. In a similar vein, in the context of cloud services, US-based companies could be stopped only with an intervention of the institutions, creating regulatory constraints able to allow market access to other players initially excluded or forced to comply with rules dictated by bigger companies. In this context, initiatives in support of

less established tech companies is key. The creation of cloud labels such as European Secure Cloud is intimately connected with the publication of C5, and denial of external standards, such as FedRAMP, offering the necessary improvement to the protection of existing international standards, plays a role as well.

The results of the empirical analysis on the effectiveness of the newer standard promoted by the EU for cloud assurance, however, is not reassuring for the quality and comprehensiveness of protection that the standard guarantees. Although the EU has relied on the expertize of specialized agencies such as BSI, the result is not completely satisfactory for privacy and security. Standards issued prior to C5 are already a sufficient guarantee, and the creation of an additional standard does not appear fully justified, if not for campaigning in a "turf war" against US companies for the dominance of the EU digital market.

6.1. Future perspectives

The adoption of C5 as a stand-alone certification is not sufficient to guarantee information assurance in cloud environments. BSI and EU institutions must be aware of its shortcomings and be proactive in reducing its gaps to guarantee full protection against current vulnerabilities. On the other hand, the adoption of the standard as a complement to ISO/IEC 27001 produces important improvements to the certification process, compensating for the missing controls. As the number of ISO/IEC 27001 certifications in Europe is almost seven times bigger than the number of certifications in North America, if C5 was exclusively used in combination with the ISO/IEC standard, still cloud service offering in the EU would largely remain a prerogative for EU companies. It does not necessarily mean complete exclusion of US tech firms from competition in the market for cloud services, since their EU datacenters and headquarters are most likely ISO/IEC

27001 certified, thus accounting for the 10.000 and more European certifications. Exclusion of transatlantic data flow in the access to cloud resources, however, represents a contradiction in terms with the cloud paradigm, and at the same time restrains smaller firms from accessing the EU Digital Single Market. A first step for US tech-companies to fill the gap that the EU initiatives are creating could be a more widely adoption of ISO/IEC 27001 certification and then move towards C5 compliance. In this perspective, US-based CSPs could increase their appeal to EU tenants regardless of the location of their data centers. Still, compliance with security standards is not enough. To allow US companies to provide their services across the Atlantic, the US Government and the European Commission should negotiate a convincing privacy framework. The existing Privacy Shield does not offer adequate guarantees, and the echo of the Schrems case C-362/14 (see section 3.6) is still strong in the EU, jeopardizing credibility of and trust in US firms.

However, the US Government is not taking any visible steps towards the adoption of a more conservative privacy stance, and is rather repealing existing protection measures (see section 2.2). This scenario could represent a unique opportunity for the EU to move forward in creating its own secure cloud. Still, it is important that the European Single Market remains open to US investments, since it is still largely based on US services. A sudden attempt to influence the market of cloud services, for example imposing compliance with C5 to process specific type of data, like FedRAMP in the US, could represent a damage for EU businesses and governments because of inefficiency and migration costs.

PRIMARY SOURCES

American Institute of certified Public Accountants (AICPA). (2009). Trust Services Principles, Criteria, and Illustrations.

– – –. (2014). Trust Services Principles and Criteria

– – –. (2016). Trust Services Principles and Criteria

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2016). Anforderungskataalog Cloud Computing (C5). Accessed November 29, 2016. https://www.bsi.bund.de/C5

Cloud Security Alliance (CSA). (2016). Cloud Control Matrix. Version 3.0.1.

ISO/IEC (2005). ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. International Standard, first edition.

– – –. (2013). ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. International Standard, second edition.

National Institute for Standards and Technology (NIST). (2009). NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. Revision 3.

– – –. (2013). NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. Revision 4.

REFERENCES

Adobe. 2015. Adobe Security and Privacy Certifications. White Paper. Adobe Systems Incorporated. Accessed March 10, 2017. http://www.adobe.com/security.html

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

– – –. (2017). C5 Standard. Webpage. Accessed April 1, 2017. https://aws.amazon.com/compliance/bsi-c5/

American Institute of Certified Public Accountants (AICPA) (2017). Service Organization Controls (SOC) Reports for Service Organizations. Web Page. Accessed March 11, 2017. http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx

– – –. 2011. New SOC Reports for Service Organizations Replace SAS 70 Reports. AICPA Communications, February 7, 2011. Accessed November 24, 2016. https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2011/CPA/Feb/SOCReplaceSAS70Reports.jsp

– – –. 2014. Service Organization Control Reports. Accessed November 21, 2016. http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SOCToolkit_ServiceOrgs.aspx

– – –. 2015. Information for Management of a Service Organization. Accessed August 11, 2016. http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/downloadabledocuments/infoformanagementofsvcorg.pdf

– – –. (2015a). Proposed Revision of Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Exposure Draft. Retrieved from http://www.aicpa.org/InterestAreas/FRC/Pages/default.aspx

– – –. 2016. About the AICPA. Webpage. Accessed November 26,2016. http://www.aicpa.org/About/Pages/About.aspx

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.

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

– – –. (2011a). System Security Engineering. IEEE Security & Privacy. (9) 72-74

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

Barker, T. E. (2016). *Into the Clouds. European SMEs ant the Digital Age*. Report. Atlantic Council. Retrieved from http://www.atlanticcouncil.org/publications/reports/into-the-clouds.

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

BMWI (*Bundesministerium für Wirtschaft und Energie* - Federal Ministry for Economic Affairs and Energy) (2017). Gabriel and Sapin strengthen digital partnership between Germany and France. Press Release. Accessed March 23, 2017. http://www.de.digital/DIGITAL/Redaktion/EN/Meldungen/2016/2016-12-13-gabriel-and-sapin-strengthen-digital-partnership.html

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2016a). European Secure Cloud (ESCloud). Memorandum of Understanding. Retrieved from https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel_node.html;jsessionid=6D058480C461CCCEE6173DFF9B5027A6.2_cid351

Catrantzos, Nick. (2012) Managing the Insider Threat: No Dark Corners. Boca Raton, FL: CRC Press.

Chen, Thomas N. (2014). Cyberterrorism after Stuxnet. Carlisle Barracks, Pennsylvania: Strategic Studies Institute and U.S. Army War College Press

Cloud Security Alliance (CSA). 2010. Top Threats to Cloud Computing V1.0. Accessed March 10, 2017. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

– – –. 2013. The Notorious Nine Cloud Computing Top Threats in 2013. Accessed March 10, 2017. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

– – –. 2016a. 'The Treacherous Twelve' Cloud Computing Top Threats in 2016. Accessed March 10, 2017. https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/

– – –. (2017). CSA STAR: The Future of Cloud Trust and Assurance. Web page. Accessed March 9, 2017. https://cloudsecurityalliance.org/star/

– – –. (2017a). Introduction to the Cloud Control Matrix Working Group. Web page. Accessed March 10, 2017. https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Cloud Standards Customer Council. 2013. Cloud Security Standards: What to Expect & What to Negotiate. Accessed March 10, 2017. http://www.cloud-council.org/resource-hub.htm

Cockfield, A. J. (2010). Legal Constraints on Transferring Personal Information Across Borders: A Comparative Analysis of PIPEDA and Foreign Privacy Laws. Surveillance, Privacy, and Globalization of Personal Information. McGill-Queen's Press. (pp. 50 – 69).

Court of Justice of the European Union (2015). The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. Press Release No 117/15. Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner.

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

De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review* (28). (pp. 130 - 142).

De Ville, F., Siles-Brügge, G. (2016). TTIP. The Truth about the Transatlantic Trade and Investment Partnership. Cambridge: Polity Press

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K. Campbell, R., Bashir, M. (forthcoming 2017). "Cloud Security Certifications: A Comparison to Improve Cloud Service Provider Security". In the proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing (ICC 2017), Churchill College, Cambridge, UK. March 22-23, 2017. ACM Proceedings Series

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K. Campbell, R., Bashir, M. (forthcoming 2017a). "IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers". To be presented at the International Workshop on Assured Cloud Computing and QoS Aware Big Data (WACC '17), Madrid, Spain. May 14, 2017.

Docker (2015). Introduction to Container Security. Whitepaper. Accessed April 4, 2017. https://confluence.cornell.edu/display/CLOUD/Docker+%3A+Whitepaper+-+Introduction+To+Container+Security

Dombalagian, H. (2015) Chasing the Tape: Information Law and Policy in Capital Markets. MIT Press.

Dowling, D.C.J. (2009). *International Data Protection and Privacy Law*. Retrieved from: http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf

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

European Commission (2002). The application of Commission Decision 520/2000/EC of 26 July 2000. Commission Staff Working Paper. Retrieved from http://web.archive.org/web/20060724174359/http://www.ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf

– – –. (2010). *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*. Final Report. Retrieved from: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

– – –. (2012). *Commission proposes a comprehensive reform of the data protection rules.* [Data Protection – Newsroom]. Retrieved from: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

– – –. (2012a). COM(2012) 529 final. Unleashing the Potential of Cloud Computing in Europe. Retrieved from https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy

– – –. (2015). Factsheet on Services. Retrieved from http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152999.2%20Services.pdf

– – –. (2017). Digital Single Market. Policy Areas. Website. Accessed March 23, 2017. https://ec.europa.eu/commission/priorities/digital-single-market_en

– – –. (2017a). The European Single Market. Webpage. Accessed April 8, 2017. https://ec.europa.eu/growth/single-market_en

European Telecommunications Standard Institute (ETSI). 2013. Cloud Standards Coordination Final Report. Accessed March 10, 2017. http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf

Fairless, T. (2014). U.S. Tech Giants Battle Europe's Sovereign States. *The Wall Street Journal.* Retrieved from http://www.wsj.com/articles/europe-vs-u-s-tech-giants-1418085890

FTC (1998). Privacy Online: A Report to Congress. White Paper. Retrieved from http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf.

FedRAMP (2014). Guide to Understanding FedRAMP, Version 2.0. FedRAMP PMO. Accessed May 26. https://www.fedramp.gov/resources/documents/

– – –. (2014a). FedRAMP Security Assessment Framework Version 2.0. 2014. Accessed May 29, 2016. https://www.fedramp.gov/resources/documents/

– – –. (2017a). FedRAMP Compliant Systems. Web page. Accessed March 9, 2017. https://marketplace.fedramp.gov/index.html#/products?sort=productName

– – –. (2017b). Program Overview. Web page. Accessed March 9, 2017. https://www.fedramp.gov/about-us/about/

– – –. (2017c). FedRAMP. Marketplace. Web page. Accessed November 21, 2016. https://marketplace.fedramp.gov/index.html#/products?sort=productName

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

Forelle, C. (2008). Microsoft's Office Push Scrutinized by EU. Wall Street Journal - Eastern Edition. February 8. p. B4.

Freking, K. (2017). Republicans Just Voted to Allow Internet Companies to Sell Your Browsing History. Time Magazine, online edition. Accessed April 9, 2017. http://time.com/4716033/house-internet-browsing-history-fcc-comcast-verizon/?iid=sr-link4

Gantz, S.D. 2013. The Basics of IT Audit: Purposes, Processes, and Practical Information. Syngress. ISBN 9780124171596

Gartner. 2010. Gartner Says SAS 70 is not Proof of Security, Continuity of Privacy Compliance. Press Release. July 14, 2010. Accessed November 25, 2016. http://www.gartner.com/newsroom/id/1400813

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

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

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.

Goldstein, D. S., Hardiman, M., Baker, M. R., & Druckerman, J. A. (2016). Understanding the EU–US "Privacy Shield" Data Transfer Framework. Journal of Internet Law, 20(5), 1-22

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

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/

Gouvernment Français (2017). Franco-German cooperation for a Europe at the forefront of the digital economy. Press Release. Accessed March 23, 2017. http://www.gouvernement.fr/en/franco-german-cooperation-for-a-europe-at-the-forefront-of-the-digital-economy

Grete, P. (2016). The BSI "C5" (Presentation at the Secure Cloud 2016 event, 24/05/2016, Dublin). Retrieved from https://csacongress.org/wp-content/uploads/2016/06/Patrick-Grete-The-BSI-C5.pdf

Grobauer, B., Walloschek, T., Stöcker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security and Privacy*, 9(2), 50-57

Gruber, L. (2000). Ruling the World: Power Politics and the Rise of Supranational Institutions. Princeton University Press.

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

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.

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

Kilkelly, U. (2003). The right to respect for private and family life. Human Rights Handbooks (1). Directorate General of Human Rights Council of Europe. Retrieved from: http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01(2003).pdf

International Electrotechnical Commission (IEC). (2011). *One size-fits-all mobile phone charger: IEC publishes first globally relevant standard.* Web page. Accessed October 11, 2016. http://www.iec.ch/newslog/2011/nr0311.htm

– – – (2015). ISO Survey. Accessed November 24, 2016. http://www.iso.org/iso/iso-survey

– – – (2017). Who We Are. Web page. Accessed March 29, 2017. http://www.iec.ch/about/profile/?ref=menu

International Organization for Standardization (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

– – –. (2015). ISO Survey. 2015. Accessed March 9, 2017. http://www.iso.org/iso/iso-survey

– – –. (2017). Standards. Webpage. Last accessed March 26, 2017. http://www.iso.org/iso/home/standards.htm

– – – (2017a). About ISO. Web page. Accessed March 29, 2017. http://www.iso.org/iso/home/about.htm

– – – (2017b). ISO/IEC 27001 - Information security management. Web page. Accessed March 29, 2017. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm+

ISO

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)

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)

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)

Kundra, V. 2010. 25 Point Implementation Plan to Reform Federal Information Technology Management. Accessed May 23, 2016. https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf

– – –. 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

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.

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.

MeriTalk (2016). Fix FedRAMP. A Six-point Plan. Position Paper. Retrieved from https://www.meritalk.com/study/fix-fedramp/

Microsoft (2017). Compliance. Website (in German). Accessed April 1, 2017. https://www.microsoft.com/de-de/cloud/compliance

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

NIST. (1998). Circular No. A-119. Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities. Last accessed October 10, 2016. https://www.nist.gov/standardsgov/omba119

– – –. (2004). Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. Accessed May 31, 2016.

– – –. (2011). The NIST Definition of Cloud Computing. Special Publication 800-145. Last accessed October 6, 2016. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Office of Management and Budget (2017). Analytical Perspectives. Budget of the U.S. Government. Retrieved from https://www.whitehouse.gov/omb/budget/Analytical_Perspectives

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

Parks, G. T. (2014). *Data Breach Provisions in Outsourcing Contracts*. In the National Law Review. Retrieved from http://www.natlawreview.com/article/data-breach-provisions-outsourcing-contracts

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)

Perception Point. (2016) 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/

Prosser, W. L. (1960). Privacy. California Law Review, 48(3), 383.

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

– – –. (2014a). 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

Samuelson, P. (2000). Privacy as intellectual property? *Stanford Law Review, 52* (5, Symposium: Cyberspace and Privacy: A New Legal Paradigm?), 1125-1173.

Scott, M. (2015). *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*. The New York Times, online edition. Last accessed on October 30, 2015 from http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0

Shimanek, A. E. (2001). Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles. *Journal of Corporation Law* (26). Part 2. (pp. 455 – 477).

Singleton, S. (2002). *Privacy as a Trade Issue: Guidelines for U.S. Trade Negotiators.* EFP02 – The Heritage Foundation.

Smedinghoff, T. J. (2012). Solving the legal challenges of trustworthy online identity. *Computer Law & Security Review* (28). (pp. 532 – 541).

Sperling, S. (2011). The Politics of Transparency and Surveillance in Post-Reunification Germany. In Surveillance and Society. 8(4): 396-412.

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.

Timmermans, S. and Epstein, S. (2010). A World of Standards but not a Standard World: Toward a Sociology of Standards and Standardization. In *Annual Review of Sociology*, 36, pp. 69-89.

Turban, E., Volonino, L., Wood, G. R. (2015). Information Technology for Management. Digital Strategies for Insight, Action, and Sustainable Performance. 10th edition. Wiley.

VanRoekel, S. (2011). Security Authorization of Information Systems in Cloud Computing Environments. Memorandum. Accessed May 28, 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf

Verizon (2016). 2016 Data Breach Investigations Report. Accessed March 14, 2017. http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Wang, Y. and Kobsa, A. (2008). *Privacy-Enhancing Technologies*. In Gupta, M. and Sharman, R. Handbook of Research on Social and Organizational Liabilities in Information Security. IGI Global. Hershey, PA.

Watkins, S. 2013. An Introduction to Information Security and ISO27001:2013, A Pocket Guide, Second Edition. IT Governance Ltd. ISBN-13: 978-1-84928-526-1

World Trade Organization (WTO). 2015. *International Trade Statistics 2015*. Accessed July 30, 2016. https://www.wto.org/english/res_e/statis_e/its2015_e/its2015_e.pdf