Yimam and Fernandez *Journal of Internet Services and Applications* (2016) 7:5
DOI 10.1186/s13174-016-0046-8

Journal of Internet Services and Applications

RESEARCH Open Access

A survey of compliance issues in cloud computing

Dereje Yimam* and Eduardo B. Fernandez

Abstract

Features such as elasticity, scalability, universal access, low entry cost, and flexible billing motivate consumers to migrate their core businesses to the cloud. However, in doing so there are challenges about security, privacy, and compliance. Businesses are pressured to comply with regulations depending on their service types; for example, in the US government agencies are required to comply with FISMA, healthcare organizations are required to comply with HIPAA; public retail companies must to comply with SOX and PCI. We survey work on compliance issues and we conclude that the lack of reference architectures and relevant patterns makes compliance harder than it should be. We also explore current industrial trends of compliance approaches. We end by summarizing compliance issues and give some guidelines about what this architecture and its corresponding patterns should contain.

Keywords: Compliance, Regulations, Cloud compliance, Compliance reference architectures, Patterns

1 Introduction

In the last few years, the use of cloud services has become widespread. According to International Data Corporation (IDC) [37], public spending on cloud services is estimated to reach $107 billion by the year 2017. A large number of cloud service providers (CSP), service brokers, and customers are increasingly taking advantage of cloud features such as elasticity, scalability, universal access, low entry cost, flexible billing, easy metering, and convenient monitoring. Despite the increase in demand and popularity, there are major challenges in moving a business to the cloud, such as compliance, security, and privacy. There are many works considering security and privacy in clouds but we are concerned here only with compliance aspects, which have strong relation to those attributes; in fact, there are relatively few works dealing mostly with compliance aspects.

Regulations are sets of policies that govern the use of sensitive business data. The main intent of these regulations are to protect consumers' privacy and provide security by enforcing attributes such as confidentiality, integrity, availability, and accountability (CIAA). Compliance implies enforcing the rules that implement the policies defined in the regulations. In the opinion of [41], legal compliance may become the most important Non-Functional Requirement (NFR) for a large number of software systems. Government and state regulations are mandatory while industry regulations are suggestions. Regulations vary from country to country but in many cases they use almost identical policies customized to their local needs. We consider here only US regulations but most of our conclusions apply to non-US regulations. Because of the very nature of cloud technology, compliance is a shared responsibility among organizations and service providers; it involves service providers, service brokers, customers, and auditors. According to the National Institute of Standards and Technology (NIST) [48], organizations are fully responsible for all compliance-related issues. The cost of not being compliant may result in penalty fees, lawsuits, and bad business reputation.

Regulations are often verbose, lengthy, hard to read, redundant, ambiguous, and in some cases even inconsistent. They are indeed documents intended for lawyers not for software developers. We examined in detail only a relatively small number of regulations but the opinion of several authors and people we talked to is similar, e.g. [7, 28, 41]. On the other hand, service providers and consumers are expected to be 100 % compliant and they are often required to comply with more than one regulation. There is a need then for tools to assist enterprises

* Correspondence: dyimam@fau.edu
Department of Computer and Electrical Engineering and Computer Science, Florida Atlantic University, Boca Raton, FL, USA

or software houses when implementing software systems that must be compliant, but we have found that the lack of a vendor-neutral standard compliance Reference Architecture (RA) is a basic challenge for service providers, service brokers, consumers, and auditors. An RA is a standardized, generic software architecture, with no platform dependencies, valid for a particular domain [4]. An RA can be used to guide system design and development; it can also be a reference to indicate where the specific compliance policies should be applied in the system architecture. An RA can serve as a common language among stakeholders including business owners, managers, architects, developers, testers, and auditors. References [9, 34, 35, 49, 51, 61] describe RAs intended to guide compliance. There is no accepted definition about what an RA should contain; the available compliance RAs are either vendor specific, lack standard modeling, or are incomplete. In addition, the style and the depth of the architectures are different among vendors. As a result, consumers are challenged to evaluate service providers with no standard compliance RAs that could be used as a common reference and checklist. In particular, when negotiating service contracts it is hard for both consumers and providers to define precisely what it means to be compliant with some regulation. One of the objectives of this paper is to indicate what aspects should be included in such an RA. Some of the regulations have been described by patterns and we indicate also how a catalog of compliance patterns can help to build a compliance RA. We do not provide here an ideal architecture or discuss how to build one, but we have done that in [64].

Often, compliance and security are only addressed either at the testing phase or at the last stage of development, which could potentially result in applications that do not identify potential threats. In order to build good quality and compliant systems, it is critical to consider the enforcement of regulations at all development phases including requirements, design, implementation, and testing phases. An RA emphasizes the need to start from a conceptual view of the semantics of the regulations without getting prematurely involved into implementation details. In [22] we showed the value of an RA as a way to enumerate threats and indicate where countermeasures should be placed. Since compliance is strongly based on security measures and related policies, it is clear that an accepted RA describing specific regulations would provide a way to facilitate building systems that comply with the corresponding regulations. We will consider the use or lack of RAs as a criteria to judge the publications we analyze in our survey. RAs can be built using patterns and use of patterns is another way to make explicit compliance with policies. A *pattern* is a solution to a recurring problem in a specific context, typically expressed using UML (Unified Modeling Language) models [8].

An RA would be a great help to build new regulations by identifying commonalities. Identifying overlaps and patterns among regulations can avoid duplicate implementations and inconsistencies as well as allow considering known security threats [23]. Reference [28] identified 31 technical security features that are common for FISMA [24], HIPAA [33], PCI [52] and ISO [39]. They concluded that implementing compliance guidelines for FISMA could cover compliance for HIPAA, PCI and ISO with the exception of privacy. Reference [30] built a citation graph to analyze interrelated regulations, overlaps, and possible conflicts. Reference [45] identified overlaps among GLBA, HIPAA, PCI DSS, and SOX regulations. These commonalities are important in complying with multiple regulations and for understanding regulations in general.

Most businesses use independent third party certifying agencies [15] and internal IT auditors to assure compliance, security, and privacy. In addition, government agencies in the US that support cloud computing must fulfill the Federal Risk and Authorization Management Program (FedRAMP) [16]. The US government published the list of FedRAMP certified cloud service providers [15] and Third Party Assessment Organizations (3PAOs) [17] that can be used as a reference for any cloud service providers and consumers. Service providers such as Amazon, IBM, Microsoft, Oracle, HP and others claim compliance by certifying their cloud services with 3PAOs. We survey here some industrial compliance efforts. Based on the survey of publications and industrial practice we discuss their significant issues and provide guidance about how this architecture should be.

Section 2 describes some background about regulations, patterns, and RAs. We survey compliance publications in Section 3 and compliance approaches in industry in Section 4. Section 5 summarizes compliance issues and recommendations. We end with some conclusions and future research directions in section 6.

2 Background

In this section we describe some background about regulations, standards, patterns, and RAs.

2.1 Regulations and standards

We summarize below some of the common regulations in the U.S.

HIPAA (Federal regulation): Healthcare organizations are required to comply with the Healthcare Insurance Portability and Accountability Act (HIPAA) [33]. The main objective of HIPAA is to ensure the security and privacy of Protected Health Information (PHI). PHI includes patient medical records, personal information,

credit information, insurance, employment information, and any related information that helps to identify an individual. HIPAA categorizes participating entities as covered entities and business associates. Covered entities include health care providers, health insurers, and health care clearinghouses (i.e. entities that manage billing services and process medical records that come from other systems). Business associates are entities that transfer, store, and service protected health information on behalf of covered entities. HIPAA has five major rules [33]:

- *Privacy rule*: health providers must notify individuals of the use of their health information. In addition, health providers must regulate the use and disclosure of PHI.
- *Security rule*: regulates the security of PHI from breaches, unauthorized access, deletion, and modification held by covered entities and business associates. This rule complements the Privacy rule by defining ways to protect its information.
- *Transaction and Code Sets rule:* Regulates medical transactions, medical coding standards, and reporting.
- *Enforcement rule*: it sets money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations. It regulates the use and disclosure of Protected Health Information for law enforcement officials.
- *Unique identifier rule:* prescribes that employers and participating parties are required to have unique Employer Identification Numbers (EIN) to use for their transactions. Each medical transaction is required to have a unique ID and code set.

PCI-DSS (Credit Card industry regulation): Companies that handle cardholder information are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) [52]. Cardholder information includes debit, credit, prepaid, ATM, and Point of Sale (POS) cards. PCI recommends that only authorized users have access to manage cardholder data. PCI has twelve major rules to protect cardholder data including installation of firewalls, resetting default password and security parameters, authentication, authorization, encryption, and others. Its rules are as follows [52]:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use default passwords or security parameters
- Protect stored cardholder data
- Encrypt transmission of sensitive information across public networks
- Use and regularly update anti-virus and malware protection
- Develop and maintain secure systems and applications
- Restrict access to data by using a need-to-know policy
- Identify and authenticate access to system components
- Restrict physical access to cardholder data
- Track and monitor access to network and cardholder data
- Regularly test security systems and processes
- Maintain an information security policy

Sarbanes-Oxley Act (SOX) (Federal regulation): SOX establishes standards for all US publicly-traded companies to protect shareholders and the general public from accounting errors and fraudulent practices [57]. SOX enforces control on user management, auditing, reporting, security and privacy analysis, authorization, authentication, system development, program and infrastructure management, monitoring, backup, and disaster recovery. Its rules are as follows [57]:

- Establish safeguards against fraudulent financial report, including data accuracy and correction timeline.
- Disclose compliance and security safeguards to independent auditors, including security policies, changes, application and system logs, and operations.
- Establish safeguards to prevent unauthorized data tampering
- Establish safeguards to track data access and changes
- Regularly test security systems, policies, and processes
- Maintain an information security policy
- Detect and notify security breaches

Gramm-Leach-Bliley Act (GLBA) (Federal regulation): It requires institutions that offer financial products or services to consumers to develop, implement, and maintain a comprehensive information security program that protects the confidentiality and integrity of customer records [29]. Its rules include:

- Privacy rule - disclosure policies and procedures on how consumer's data is protected and used.
- Safeguard rule – maintain comprehensive security policies. Security policies need to be applied to all with no exception and need to be reviewed, tested, and maintained frequently.

Control Objectives for Information and Related Technology (COBIT), (IT industry regulation): It is a

standard to provide IT governance and control. It attempts to ensure the integrity of information and information systems by providing technical guidelines on information security, compliance, governance, audit, and risk management [11].

The Federal Information Security and Management Act (FISMA), (Federal government regulation): FISMA applies to government agencies and affiliated companies that collect and process data on behalf of government agencies [24]. It provides guidelines on security controls, user access, identity management, risk assessment, auditing, and monitoring.

ISO/IEC 27000 (IT industry regulation): It is a general security guideline for all types of organization including commercial enterprises of all sizes [39]. It is a family of standards that helps organizations to secure information assets. Some of its standards are:

ISO/IEC 27001 –Information security management systems requirements
ISO/IEC 27002 – Code of practice for information security controls
ISO/IEC 27003 – Information security management system implementation guidance
ISO/IEC 27004 - Security techniques – Information security management

ISO/IEC 27002 defines six access control objectives that cover end user, privileged user, network, application, and information. The objectives include control access to information, manage user access rights, apply good access practices, control access to network services, control access to operating systems, and control access to applications and systems [42].

These regulations and standards are used in service sectors such as healthcare, finance, retail, communication, energy, education, and government agencies. Table 1 shows a summary of a few service sectors with their corresponding regulations. In most cases, service sectors support multiple regulations to comply with government and industry regulations. As mentioned earlier, many countries have similar regulations and standards customized to their local needs. For example, the European Union Data Protection Directive law (EU DPD) has a set of policies to protect the confidentiality, integrity, availability, and accountability of personal data [44]. EU countries are required to comply with these policies.

Table 1 Summary of service sectors with their corresponding regulations

	Service sector	Regulation
1	Healthcare	HIPAA, PCI
2	Retail	PCI, SOX
3	Financial	PCI, SOX, and GLBA
4	Government agencies	FISMA

2.2 Patterns

A pattern encapsulates a solution to a recurring problem in a specific context. Patterns can be used to analyze complex systems, to capture design decisions, assumptions, and experiences. They can improve software quality by promoting reusability, scalability, and consistency. Patterns can be categorized as analysis patterns [19, 25], design and architecture patterns [8, 26], and security patterns [18, 20]. Pattern solutions are usually represented using modeling languages such as the Unified Modeling Language (UML), maybe combined with formal languages such as the Object Constraint Language (OCL) [63]. Patterns may include class diagrams, sequence diagrams corresponding to use cases, and state diagrams, and they are described using templates. A few patterns exist to describe the architectural implications of regulation policies [14, 21].

2.3 Reference Architectures (RAs)

As defined earlier, a Reference Architecture (RA) is a generic abstract architecture, valid for a particular domain (or set of domains), with no implementation aspects or vendor specific details [4, 60]. RAs are special types of architectures intended to understand, analyze, design and standardize complex systems at a high level of abstraction. RAs are reusable, extendable, and configurable; that is, they are kinds of patterns for whole architectures and can be instantiated into specific software architectures by adding platform aspects. Software architectures derived from RAs could mitigate risks, facilitate compliance, and protect confidentiality and integrity of consumers' data [10, 62]). RAs can become a common language among stakeholders including business owners, managers, architects, developers, testers and auditors. RAs can also be used to standardize application design, implementation, and verification. RAs can be built of patterns and there is also a possibility of identifying new patterns while building them. In addition, block diagrams, reference models, viewpoints, use cases, and formal languages can be used to build RAs.

3 Survey of compliance in cloud computing

There are only a few papers that have direct relationship to our survey. We review papers that discuss general aspects of regulations or which consider compliance with specific regulations.

Reference [48] identified a number privacy and security related issues that could have an impact on cloud computing. The paper covers issues and recommendations on governance, compliance, trust, architecture, identity, access management, software isolation, data

protection, availability, and incident report. The paper pointed out that compliance in cloud computing is one of the complex issues to deal with as policies vary from country to country. As per [48], understanding and enforcing regulations are also a major challenge in cloud computing. They analyzed the impact of data location, loss of control, and transparency in public cloud compliance. The issue of electronic discovery that involves identification, collection, processing, analysis, and production of stored information is also covered. The authors didn't cover techniques to map complex policies into best practices, patterns, or RAs. They also mentioned that most cloud service providers use third party certification to confirm their compliance. As per our survey, third party auditors are using proprietary solutions that lack vendor neutral models or architectures that can be used as a checklist by all stakeholders.

Reference [45] compared GLBA, HIPAA, PCI and SOX standards on the basis of generating reports for auditors. Their findings showed that some reports and services share common features including user logon report, user logoff report, user failure report and logs access report as shown in Table 2. They concluded that SOX compliance with respect to reports also covers the required reports for GLBA, HIPAA and PCI-DSS. The authors didn't cover other features of compliance such as privacy, security, user management, and notification. The comparison table would have been more precise if it was backed by more precise artifacts.

Reference [55] analyzed the top seven threats and their possible impact on cloud compliance by mapping threats to applicable regulations. The mapping could be used as a reference to evaluate compliance. However, the paper lacks explicit mappings between compliance and security threats. For example, in Table 3 threats # 2 and #3 are not mapped to any compliance standard. The paper also lacks a precise definition of threats and their corresponding correlation with compliance. For example, they consider threats #2 and #3 as threats but they are vulnerabilities. The authors left out other regulations such as SOX and GLBA and did not try to define an RA. Note also that this list of threats is rather incomplete; for a more comprehensive list see [31, 55].

Reference [54] reviewed privacy regulations in the cloud. They pointed out that there are still many uncertainties with respect to compliance and privacy in cloud computing. As a result, it is becoming very difficult to analyze security, privacy and compliance among cloud service providers. In addition, they indicated that many regulations share common requirements such as privacy, integrity, security and enforcement. They mentioned that organizations are liable in the case of security breaches and lawsuits. They also reviewed the use of independent third parties to certify compliance.

Reference [46] analyzed HIPAA and COBIT with respect to NIST guidelines. According to [46], healthcare organizations that adopt COBIT as their standard will immediately satisfy 50 % of the NIST standards. They concluded that an increase in security threats, complex regulations, lack of qualified security experts, and high implementation and maintenance costs are the most common challenges in the healthcare industry. In addition, the authors pointed out that company compliance can be improved by analyzing regulation overlaps and best practices. The overlap was presented in block diagrams which do not show clearly the type and the nature of these overlaps.

Reference [30] built a citation graph that could be used by analysts to navigate through the various interrelated regulations to uncover overlaps and possible conflicts or

Table 2 GLBA, HIPAA, PCI DSS and SOX report comparison [45]

Reports	GLBA	HIPAA	PCI-DSS	SOX
User logon / Logoff	✓	✓	✓	✓
Logon failure	✓	✓	✓	✓
Audit logs access	✓	✓	✓	✓
Object access		✓	✓	✓
System events		✓		✓
Host session status		✓		✓
Security log archiving	✓	✓		✓
Track account management and use group changes				✓
Track audit policy changes			✓	✓
Successful user account validation		✓		✓
Unsuccessful use account validation		✓		✓
Track individual user actions report			✓	✓
Track application access				✓

Table 3 Threats to compliance mapping

	Threats	Remarks
1	Abuse and Nefarious Use of Cloud Computing - threats related to abusing cloud network and services by using Denial of Service (DoS), malicious file upload, and malware	- The authors mapped this threat to ISO 27001 compliance. We believe that this threat can also be mapped to other regulations
2	Insecure Interfaces and APIs	- This is not a threat, it is a vulnerability.
3	Malicious Insiders	- Not a threat, a vulnerability. It is not mapped to any regulation
4	Shared Technology Issues	- The authors mapped the threat to ISO 27000–27002 and PCI-DSS compliance. We believe that this threat can also be mapped to other regulations
5	Data Loss or Leakage	- The authors mapped this threat to ISO 17826 and HIPAA compliance. We believe that this threat can also be mapped to other regulations
6	Account or Service Hijacking	- There is no clear mapping between this threat and available regulations
7	Unknown Risk Profile – it includes transparency, maintenance responsibility, software version, and fixes	- The mapping between regulations and this threat is not clear.

to understand compliance documents. The authors used a decision support system to identify compliance similarities and differences. They used this citation graph to understand regulations, to uncover overlaps and possible conflicts. They also use the citation graph to detect important provisions by ranking, to assess the impact of change in a particular act, and to validate consistency. The overlaps include security, notification, reporting, and user management. The authors focused only on HIPAA, SOX and GLBA regulations. We can also assert that [45] findings confirm [30] conclusions.

Reference [6] developed a compliant cloud computing (C3) framework to address security, compliance, privacy, and trust issues. According to the authors, C3 can be used to address data privacy by enforcing data storage in specific regions and by applying data fragmentation. They claim that the framework can be used as a broker to integrate multiple service providers. The authors proposed a domain specific language (DSL), a metamodel and an activity diagram to analyze regulations such as HIPAA, PCI and SOX.

Reference [13] developed a framework called MEGHNAD [13] that uses a Multi-Objective Genetic Algorithm (MOGA) to determine an optimal security toolset that could meet security and compliance requirements. The authors claim that the framework can be used to generate compliance checklists and Service Level Agreements (SLAs). They also used the framework to analyze security levels and cloud assurance levels for IaaS, PaaS and SaaS.

According to [12], security and compliance tools could help organizations to certify compliance. They reviewed compliance tools such as WatchGuard and Trust Wave to analyze, and generate compliance coverage reports. The depth and scope of the reports vary from vendor to vendor. The authors categorized service models and defined a compliance mapping matrix based on "who controls what" as shown in Tables 4 and 5. The definitions in these tables are not detailed enough to show precisely the roles of the users of a cloud. For example, access control is a shared responsibility but it is indicated as vendor responsibility in Table 4. In Table 4, requirements 3 and 5 are the same by definition; however, the authors provide different roles for IaaS responsibility. They covered HIPAA and PCI standards but these conclusions may not apply to other standards. The authors suggested that more research needs to be done in order to build consumers' confidence and trust.

Reference [47] discussed PCI compliance challenges and solutions. The authors reviewed challenges such as costs, overlaps, legal uncertainties, security, maintenance, complexity, code quality, and new technologies. Their proposed solutions are based on best practices. The solutions include authentication, authorization, encryption, and monitoring. The authors didn't cover how to address regulation complexities and overlaps.

Reference [28] analyzed security overlaps among FISMA, HIPAA, PCI and ISO. The author identified 31 technical security features that are common to FISMA, HIPAA, PCI and ISO and suggested that implementing the compliance guidelines of FISMA could cover compliance of HIPAA, PCI, and ISO, with the exception of privacy. The paper also confirms regulation overlaps and the need for the systematic approaches proposed by [45, 47, 55].

Reference [44] reviewed the EU DPD law and regulations in the context of cloud computing. They pointed out that parts of the DPD policies are not clear, including the definition of sensitive personal data, the roles of controllers and processors. The authors also mentioned that there are overlaps among regulations. They used an enumeration approach to map the DPD policies to available best practices. They proposed encryption, anonymization, and pseudonymization to secure personal data in

Table 4 Vendor responsibility for HIPAA Requirement Mapping matrix [12]

	HIPAA requirement	Vendor responsibility in		
		SaaS	PaaS	IaaS
1	Security Management Process: Review permission setting and correct access rights	Yes	No	No
2	Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures.	Yes	No	No
3	Workforce Security: Ensure that only authorized workforce members have access to Electronic Protected Health Information	Yes	Yes	No
4	Information Access Management: Implement policies and procedures for accessing Electronic Protected Health Information	Yes	Yes	No
5	Access Control: Allow access only to the authorized workforce	Yes	Yes	Yes
6	Audit Control: Record and examine activities for Electronic Protected Health Information	Yes	Yes	Yes

the cloud. One of the problems with enumerations is that they lack a conceptual model of how the requirements relate to each other.

Reference [14] proposed a Compliance Request Languages that can be used to specify compliance patterns that can be applied to business processes. They built design-time compliance management framework that can be used to automate compliance validation and verification. They made no attempt to define a precise model for their framework.

Stricker et al. [58] built an RA for service-based systems using a pattern-based approach. The architecture contains top-level patterns, abstract patterns, and implementation patterns. They proposed to include a component catalog as part of the architecture. However, [58] did not include a method to map identified components into abstract patterns. Fernandez et al. [22] developed a security reference architecture (SRA) for cloud systems from use cases, threat modeling, and patterns; it maps identified components into abstract patterns using a catalog. We proposed a five-step approach to build RAs using metamodels, patterns, and best practices [64]. First, we analyzed RA input sources from functional requirements, non-functional requirements, stakeholders, regulations and standards. We identified components from use cases, ontologies, threat modeling, policies and best practices. Second, we built a conceptual model (RM) by analyzing domain components, stakeholders and their interactions. We used UML to analyze the static and dynamic nature of the identified components. Third, we mapped the identified components to patterns using abstract patterns. Fourth, we built RAs by combining results from steps 1, 2 and 3. Fifth, we evaluated the architecture by validating its quality attributes such as accuracy, completeness, modularity, reusability, flexibility, and readability. These architectures, [22, 58, 64], can be used to analyze both functional and non-functional aspects such as security and compliance at the architectural level.

In summary, we can conclude that many of the proposed solutions are not approaching compliance challenges at the architectural level using appropriate models. All approaches discussed in this section, except [22] and [64], don't use a comprehensive metamodel that includes both functional and non-functional requirements at the

Table 5 Vendor responsibility for PCI DSS Requirement Mapping matrix [12]

	PCI requirement	Vendor responsibility in		
		SaaS	PaaS	IaaS
1	Install and maintain a firewall configuration to protect cardholder data	Yes	Yes	Yes
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Yes	Yes	No
3	Protect stored cardholder data	Yes	Yes	No
4	Encrypt transmission of cardholder data across open, public networks	Yes	Yes	No
5	Use and regularly update anti-virus software	Yes	Yes	No
6	Develop and maintain secure systems and applications	Yes	No	No
7	Restrict access to cardholder data by business need-to-know	Yes	Yes	Yes
8	Assign a unique ID to each person with computer access	Yes	Yes	No
9	Restrict physical access to cardholder data	Yes	Yes	No
10	Track and monitor all access to network resources and cardholder data	Yes	Yes	Yes
11	Regularly test security systems and processes	Yes	Yes	Yes
12	Maintain a policy that addresses information security	Yes	No	No

architectural level as shown in Table 6. As a result, many RAs are either incomplete or do not follow standard models or architectures. In addition, the proposed solutions and architectures can be more understandable and precise if they used standard models, patterns, and architectures.

4 Compliance approaches in industry

Most businesses use independent third party certifying agencies and internal IT auditors to assure compliance, security, and privacy [15]. The US government published the list of FedRAMP-certified cloud service providers and Third Party Assessment Organizations (3PAOs) that can be used as a reference for cloud service providers and consumers [15, 17]. Reference [15] recommends that consumers review and approve compliance reports and certificates before signing the service contract. Service providers are using 3PAOs and internal auditors to certify compliance. In addition to third party compliance certification, many service providers use enumeration to claim their completeness. The problem with enumerations is that they do not provide a measure of completeness and lack a conceptual model of how the requirements relate to each other and to the system.

Service providers such as Amazon, IBM, Microsoft, Oracle, HP, Cisco, Hitachi, and others claim compliance for HIPAA, PCI, FISMA, SOX, and GLBA. References [2, 35, 49] describe RAs for clouds with conceptual and logical views that include security management and compliance. Their architectures use models and enumeration to describe components and their interactions. Amazon Web Services (AWS) published a list of compliance eligible services such as DynamoDB, Elastic Block Store (EBS), Elastic Cloud Compute (EC2), Glacier, Redshift, Elastic MapReduce (EMR), Simple Storage Service (S3), Identity and Access Management (IAM), CloudTrial, CloudHSM, and Amazon Relational Database (RDS) to protect customers' data at rest and in motion [1, 3]. Reference [51] published an RA for PCI-DSS using specific products such as VMware, Cisco, Trend Micro, and HyTrust; this architecture maps PCI rules to hardware and software products. Reference [61] describes a compliance Reference Architecture Framework (RAF) to address requirements at the infrastructure, application, and end user computing layers. Infrastructure layer compliance includes network security, configuration management, log management, and platform security. Application layer compliance includes permissions and governance, service level agreement, and data security. End user computing layer includes identity management, end point security, authentication, and authorization. Reference [61] maps regulation policies to corresponding layers and VMware products. Reference [10] built regulatory compliant architectures using a risk management framework to address functional capabilities, operational reliability, regulatory compliance, and security. The framework uses a standard enterprise layer architecture (i.e. web layer, application layer, service layer, business, and data layers) to identify components, and map compliance policies to corresponding Cisco products. References [10, 62] proposed a compliance reference architecture by abstracting regulations and corporate policies. References [43, 62] use SOX and Microsoft products to identify components, build the architecture, and map compliance policies to appropriate Microsoft products. Reference [34] proposes a compliance architecture derived from regulation overlaps among corporate governance and regulations. Reference [35] enumerates policies from regulations and maps them to proprietary identity and access management products.

Table 6 Summary of Related Work

Study	RAs	Patterns	Metamodel
[48]	Yes	No	No
[6, 12, 13, 28, 30, 44–47, 54, 55]	No	No	No
[14]	No	Yes	No
[58]	No	Yes	No
[22]	Yes	Yes	Yes
[64]	Yes	Yes	Yes

Compliance in the cloud is a shared responsibility among service providers and consumers [53]. The responsibility of service providers and consumers vary based on the type of their service models. In the case of IaaS, consumers are responsible to secure services, platforms, and data. Service providers are responsible to secure the infrastructure. In the case of PaaS, consumers are responsible to secure services and data; service providers are responsible to secure platforms and infrastructures. In the case of SaaS, consumers are responsible to secure data; service providers are responsible to secure services, platforms and infrastructures. In general, the lack of full control and transparency creates compliance challenges in the cloud.

In summary, most service providers have published compliance architectures, designs, and implementations based on their own proprietary cloud platforms, infrastructures, and products. The available RAs published by service providers are either vendor specific or do not follow standard models, patterns or architectures. As a result, it is very difficult to analyze their level and scope of compliance. Consumers are also challenged to evaluate service providers without having standard RAs and models that could be used as a common reference and checklist.

5 Summary of compliance issues and recommendations

In this section we summarize five major compliance issues.

5.1 Complexity of regulations

As indicated earlier, regulations are written by lawyers and often lengthy and hard to read. In some cases, the rules are redundant, ambiguous, and even inconsistent. Regulations also vary from country to country. There have been attempts to make regulations clearer and more precise by using block diagrams, citation graphs, and reference models. However, there have been only a few attempts to make their software architecture more precise in order to understand and analyze policies at a higher level and eventually guide design and implementation efforts. Reference [21] described the major HIPAA rules as patterns, to make HIPAA clearer and more precise. These HIPAA regulation patterns include: HIPAA security rule, HIPAA privacy rule, HIPAA transactions and code sets rule, HIPAA unique identifiers rule, and HIPAA enforcement rule. Figure 1 shows a UML class diagram for the HIPAA security rule [21]. It shows its major components, entities, and their associations. It includes Role-Based Access Control Authorization, Authenticator, and Security Logger/Auditor patterns [18]. We need to identify more patterns for regulations to make regulations clearer and more precise.

5.2 Regulation overlaps

Our survey reveals that there are overlaps among regulations such as HIPAA, PCI, SOX, GLBA and FISMA [23, 30, 45, 46]. Most cloud service providers are required to support multiple regulations in order to fulfill consumers' needs. The cost of implementing individual regulations can lead to high implementation and maintenance costs, duplication of efforts, and inconsistencies. Hamdaqa and Hamou-Lhadj [30]; Mirković [45]; Netschert [46] attempted to identify overlapping features such as security, user management, notification, and reporting. Reference [30] used a citation graph to identify overlaps. These overlaps could incur unnecessary cost and maybe inconsistencies. There has been only one attempt to identify these overlaps at the architectural level [23].

5.3 Lack of standard Reference Architectures (RAs)

There is no accepted definition about what an RA should contain; [4] provide ways to describe and evaluate RAs by using IEEE recommended architectural description practice [38], Rational Unified Process (RUP) artifacts [40] and UML [5]. Reference [58] built an RA for service-based systems using patterns. Reference [22] built an RA for cloud systems with use cases, activity diagrams, and patterns. We can observe that there are different levels of understanding and approaches to build RAs. In addition, the style and the depth of the architectures are different among service providers. On the other hand, consumers are challenged to evaluate service providers' compliance without having a standard checklist. We can conclude that available approaches don't use a comprehensive metamodel that includes both functional and non-functional requirements. As a result, many RAs are either incomplete or do not follow standard models or architectures. We proposed a five-step approach to build RAs using metamodels, patterns, and best practices [64] (see Section 3). Figure 2 shows a UML class diagram of a compliance and security RA (CSRA) from a SaaS service provider perspective. The

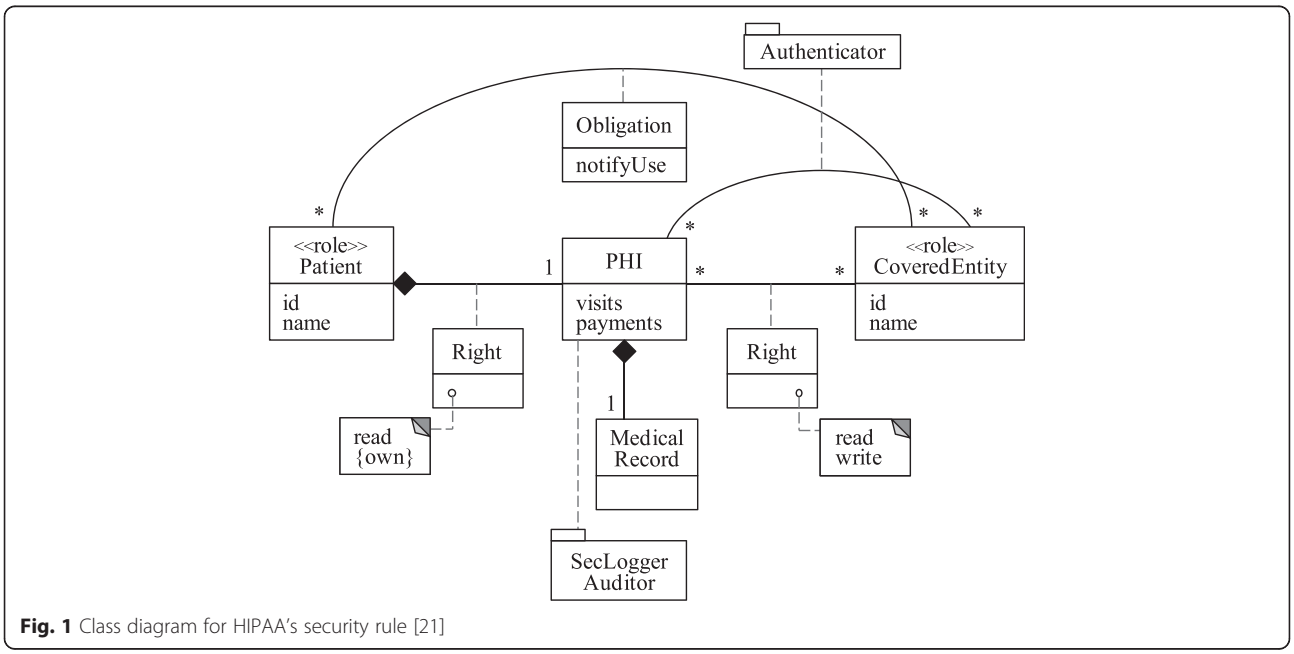

Fig. 1 Class diagram for HIPAA's security rule [21]

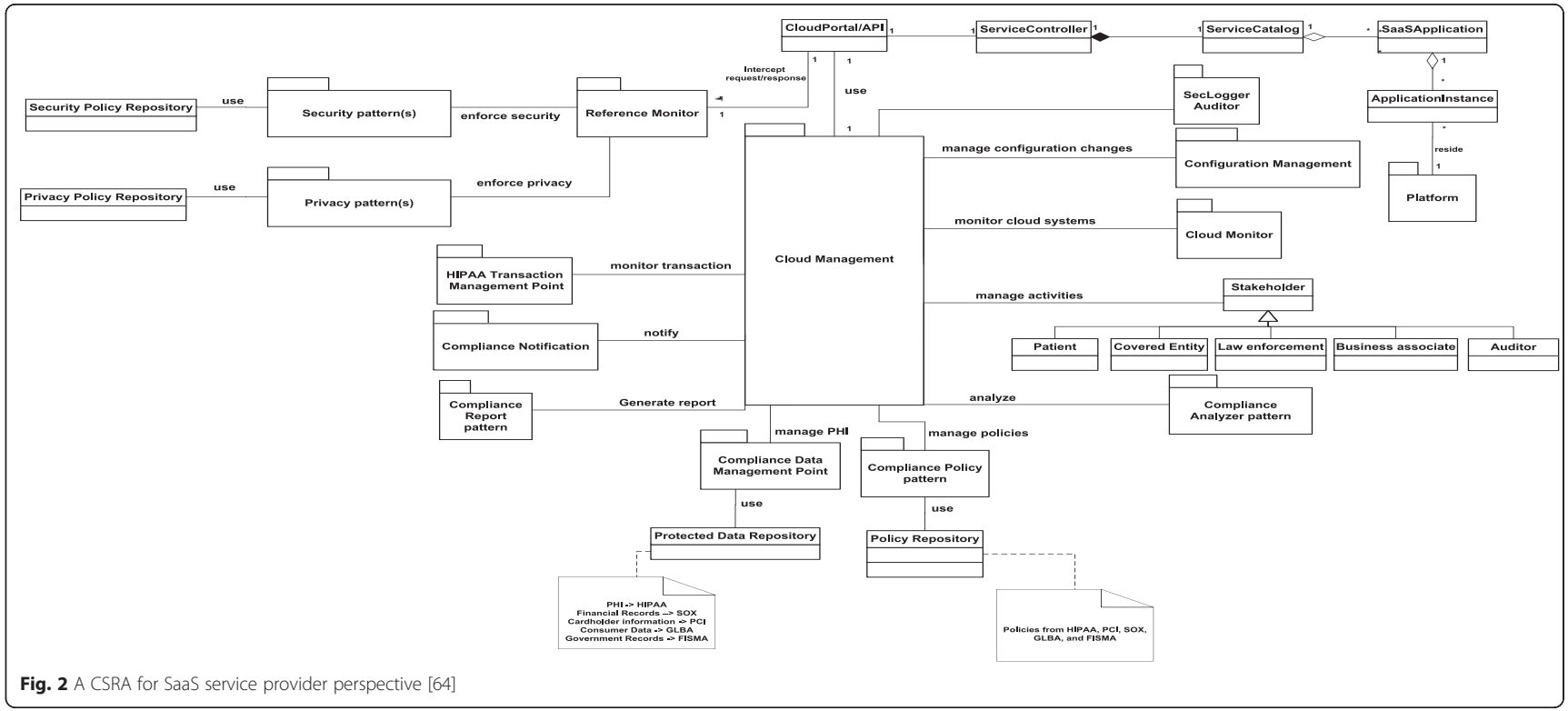

Fig. 2 A CSRA for SaaS service provider perspective [64]

architecture includes major regulation components, stakeholders, cloud components, patterns, and best practices. There are other approaches to build RAs but we think that this is the first one that takes advantage of patterns to properly represent regulations.

5.4 Lack of full control and transparency

The lack of full control and transparency is also one of the compliance challenges in the public cloud [44, 48]. The data stored in the public cloud could be replicated in different regions and / or countries that could violate privacy laws of other countries. In addition, service providers are required to ensure the confidentiality, integrity, availability and accountability (CIAA) of consumers' data as per the government and industry regulations. Reference [6] developed a framework that can control data location while maintaining compliance. Reference [12] suggested more research to build consumers' trust and compliance.

5.5 Security threats

Cloud services like any IT platforms are subjected to a variety of security threats [31, 50]. The complexity and shared responsibilities of cloud computing are also another security threat that could affect the overall compliance. Cloud computing is relatively new and still changing. More research is needed to build consumers' confidence and trust by identifying potential security and compliance threats. Reference [22] developed a security reference architecture to enforce cloud security. The architecture can be extended to support compliance by adding compliance patterns and best practices. The architecture proposed in [64] follows this approach and can handle identified threats by including appropriate security patterns as shown in [22].

5.6 Overlap with security

Most of compliance has to do with security. However, compliance is often handled by different groups who don't have a full expertise on security. Looking at some of the recommendations in the publications we surveyed we find that many of them are rather naïve and not enough to provide a highly secure architecture.

6 Conclusions and future directions

We have analyzed the state of the art in complying with regulations by examining recent publications and surveying industrial approaches. Regulations and standards are complex, possibly redundant and even inconsistent in some cases. A good way to handle compliance complexities, uncertainties, and overlaps is by applying standard models, patterns, architectures, and best practices. There have been attempts to analyze regulation policies and overlaps. However, there has been no attempt to make their software architecture more precise at a higher level to eventually guide design and implementation efforts. These kinds of standard approaches could improve compliance, security, privacy and the overall software quality of cloud systems. We examined how publications and industry have considered this particular aspect as a measure of their ability to cope with an increasing complexity. While there are other aspects that affect compliance we have taken the proper use of architectures as a key point.

Our survey reveals that more research is needed to overcome compliance challenges. Reference [21] described the two major HIPAA rules as patterns to make HIPAA clearer and more precise, but we need to identify more regulation patterns by analyzing available regulations, standards, and policy based systems. A collection of patterns can be used to build pattern-based compliance RAs [64]. We need to develop a complete and precise RA that can be used to analyze complex regulations, avoid overlaps, mitigate security threats, and promote the usage of patterns. We proposed a five-step approach to build RAs using metamodels, patterns, and best practices [64]. We have built an RA for HIPAA and CSRA for cloud systems with the proposed five-step approach. An architecture built out of patterns can be used as a common language among architects, developers, business owners, managers, service providers, and auditors. It can also be used as a reference to design and implement automated systems that can be used for testing, auditing, and compliance verification. We need to build more RAs in the areas of services, platforms, regulations, and policy-based systems to improve software quality. It is very important to convince industry that they need to adopt more abstract compliance architectures that provide greater flexibility and adaptability to new and evolving regulations. We need also to merge the work on compliance with the work on security and provide a unified approach that considers both aspects.

Competing interests

We have no competing interests.

Authors' contributions

D.Yimam found and selected most of the references in the survey sections, evaluated and classifiedthem. E. B.Fernandez wrote most of the Introduction and conclusions. All authors read and approved the final manuscript.

Acknowledgements

We thank the reviewers who provided valuable suggestions that have significantly improved this work.

Received: 7 October 2015 Accepted: 15 April 2016
Published online: 10 May 2016

References

1. Amazon. Amazon web services: risk and compliance. http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf.
2. Amazon. AWS compliance. https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.

3. Amazon Web Services. Risk and compliance. https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.
4. Avgeriou P. Describing, instantiating and evaluating a reference architecture: a case study. Enterp Archit J. 2003. Available online:http://www.rug.nl/research/portal/files/14407113/2003EnterpArchitJAvgeriou.pdf. Accessed 22 Apr 2016.
5. Booch G, Rumbaugh J, Jacobson I. The unified modeling language user guide. 2nd ed: Addison-Wesley; 2005.
6. Brandic I, Dustdar S, Anstett T, Schuman D, Leymann F, Konrad R. Compliant Cloud Computing (C3): architecture and language support for user-driven compliance management in clouds, Proceeding CLOUD '10 Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing. Miami, Florida, USA: 2010; 244–51.
7. Breaux TD, Anton AI. Analyzing regulatory rules for privacy and security requirements. IEEE Trans Soft Eng. 2008;34:5–20.
8. Buschmann F, Meunier R, Rohnert H, Sommerlad P, Stal M. Pattern-Oriented Software Architecture: A System of Patterns, vol. 1.Wiley; 1996
9. Cisco. Cisco compliance solutions. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/pci-compliance/pci-dss-30-wp.pdf. Accessed 22 Apr 2016.
10. Cisco. The risk management framework: building a secure and regulatory compliant trading architecture. http://www.cisco.com/web/strategy/docs/finance/risk_mgmt_C11-521656_wp.pdf.
11. COBIT. IT Governance Framework - Information Assurance Control, ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx.
12. Dasgupta D, Naseem D. Security and compliance testing strategies for cloud computing. https://umdrive.memphis.edu/g-mis/www/memphis/step/STEP2012/STEP2012Proceedings3.pdf.
13. Dasgupta D, Naseem D. A framework for estimating security coverage for cloud service insurance, Proceedings 7th Cyber-Security and Information Intelligence Reserach Workshop, Oak Ridge, TN, October 12-14, 2011.
14. Elgammal A, Turekten O, van der Heuvel W-J, Papazoglou M. Formalizing and applying compliance patterns for business process compliance. J Softw Syst Model. 2016;15:119–46. doi:10.1007/s10270-014-0395-3.
15. FedRAMP. FedRAMP compliant cloud systems. https://www.fedramp.gov/resources/documents/.
16. FedRAMP. Federal Risk and Authorization Management Program (FedRAMP). https://www.fedramp.gov/resources/documents/.
17. FedRAMP. FedRAMP Third Party Assessment Organizations (3PAOs). https://www.fedramp.gov/resources/documents/.
18. Fernandez EB. Security patterns in practice: building secure architectures using software patterns, Wiley Series on Software Design Patterns. 2013.
19. Fernandez EB, Yuan X. Semantic analysis patterns, Proceedings of the 19th Int. Conf. on Conceptual Modeling, ER2000. p. 183–95.
20. Fernandez EB, Larrondo-Petrie MM, Sorgente T, Van Hilst M. A methodology to develop secure systems using patterns. In: Mouratidis H, Giorgini P, editors. Integrating security and software engineering: advances and future vision. IDEA Press; 2006. p. 107–26.
21. Fernandez EB, Mujica S. Two patterns for HIPAA regulations, Procs. of AsianPLoP (Pattern Languages of Programs) 2014. Tokyo: 2014.
22. Fernandez EB, Monge R, Hashizume K. Building a security reference architecture for cloud systems. Requir Eng. 2015; doi:10.1007/s00766-014-0218-7.
23. Fernandez EB, Yimam D. Towards compliant reference architectures by finding analogies and overlaps in compliance regulations, Procs.12th Int. Conf. on Security and Cryptography (SECRYPT 2015), Colmar, France, July 2015.
24. FISMA. Federal Information Security Management Act FISMA. http://www.healthinfolaw.org/federal-law/federal-information-security-management-act-fisma.
25. Fowler M. Analysis patterns – reusable object models. Addison-Wesley; 1997.
26. Gamma E, Helm R, Johnson R, Vlissides J. Design patterns: elements of reusable object-oriented software. Boston: Addison-Wesley; 1994.
27. Gartner. http://www.gartner.com/newsroom/id/2352816.
28. Gikas C. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Inf Secur J. 2010;19(3):132–41.
29. GLBA. Gramm-Leach-Bliley Act. http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.
30. Hamdaqa M, Hamou-Lhadj A. Citation analysis: an approach for facilitating the analysis of regulatory compliance documents, Procs. 2009 6th Int. Conf. on Information technology: New Generations. IEEE; 2009. p. 278–83.
31. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. J Internet Serv Appl. 2013;4:5. 27 February 2013.
32. HIPAA. HIPAA Administrative Simplification. https://www.fedramp.gov/resources/documents/.
33. HIPAA. Understanding Health Information Privacy. http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/understanding-hipaa-notice.pdf.
34. Hitachi. Compliance architecture. http://hitachi-id.com/compliance/compliance-architecture.html.
35. IBM. IBM Cloud computing. http://www.ibm.com/cloud-computing/.
36. IBM. Security compliance services. http://www-935.ibm.com/services/us/en/it-services/security-services/compliance-and-regulatory-services/.
37. IDC. International Data Corporation. http://www.idc.com/prodserv/subservices.jsp.
38. IEEE. IEEE 1471–2000 recommended practice for architectural description of software-intensive systems. 2000. https://standards.ieee.org/findstds/standard/1471-2000.html.
39. ISO. ISO Information Security Standard. Available: http://www.iso27001security.com/.
40. Kruchten P. The rational unified process, an introduction. 3rd ed. Addison-Wesley; 2003.
41. Massey AK, Smith B, Otto PN, Anton AI. Assessing the accuracy of legal implementation readiness decisions, 19th IEEE Int. Reqs. Eng. Conf. 2011. p. 207–16.
42. Mather T, Kumaraswamy S, Latif S. Cloud security and privacy: an enterprise perspective on risks and compliance. O'Relly Media; 2009.
43. Microsoft Azure. Microsoft Azure Trust Center. http://azure.microsoft.com/en-us/support/trust-center/compliance/.
44. Millard C. Cloud computing law. Oxford University Press; 2013
45. Mirković O. Security - How to measure compliance, MIPRO proceedings. 2008.
46. Netschert BM. Information security readiness and compliance in the healthcare industry. Stevens Institute of Technology; 2008
47. Ngugi B, Vega G, Dardick G. PCI compliance: overcoming the challenges. Journal of information security and privacy. Int J Inf Secur Priv. 2009;3:2.
48. NIST. Guidelines on security and privacy in public cloud computing. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Accessed on April 22, 2016.
49. Oracle. Cloud reference architecture. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Accessed April 22, 2016.
50. OWASP. Cloud-10 regulatory compliance. https://www.owasp.org/index.php/Cloud-10_Regulatory_Compliance.
51. PCI-DSS RA. PCI-compliant cloud reference architecture. http://www.hytrust.com/solutions/compliance/.
52. PCI DSS standard. Official source of PCI DSS Data Security Standards. https://www.pcisecuritystandards.org/security_standards/index.php.
53. PCI guidelines. PCI cloud guidelines. https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf.
54. Ruiter J, Warnier M. Computers, privacy and data protection: an element of choice. 2011. p. 361–76.
55. Silva CMR, Silva JLC, Rodrigues RB, Nascimento LM, Garcia VC. Systematic mapping study on security threats in cloud computing. IJCSIS. 2013;11:3.
56. Sony. Sony freezes 93,000 online accounts after security breach. http://www.forbes.com/sites/parmyolson/2011/10/12/sony-freezes-93000-online-accounts-after-security-breach/.
57. SOX law. The Sarbanes-Oxley Act. http://www.soxlaw.com/.
58. Stricker V, Lauenroth K, Corte P, Gittler F, De Panfilis S, Pohl K. Creating a reference architecture for service-based systems a pattern-based approach. 2010; doi:10.3233/978-1-60750-539-6-149. IOS Press.
59. Target. Response & resources related to Target's data breach. https://corporate.target.com/about/payment-card-issue.aspx.
60. Taylor RN, Medvidovic N, Dashofy N. Software architecture: foundation, theory, and practice. Wiley; 2010.
61. VMware. Compliance reference architecture framework. https://solutionexchange.vmware.com/store/products/vmware-compliance-cyber-risk-solutions.
62. Walker M. Architecting regulatory-compliant architectures. https://msdn.microsoft.com/en-us/library/bb233047.aspx.
63. Warmer J, Kleppe A. The object constraint language. 2nd ed. Addison-Wesley; 2003.
64. Yimam D, Fernandez EB. Building Compliance and Security Reference Architectures (CSRA) for cloud systems, IEEE International Conference on Cloud Engineering (IC2E). 2016.