Cloud Security Practices: Literature Review

Chaoran Li
Department of Computer Science
University of Amsterdam
13511440
chaoran.li@student.uva.nl

Chih-Chieh Lin
Department of Computer Science
University of Amsterdam
13501313
chih-chieh.lin@student.uva.nl

Haochen Wang
Department of Computer Science
University of Amsterdam
13500198
haochen.wang@student.uva.nl

Kaixi Ma
Department of Computer Science
University of Amsterdam
12536016
kaixi.ma@student.uva.nl

Abstract

In this article, we discuss three important components of maintaining cloud security; and further, illustrate a practice example from AWS. Plenty of software applications are created using DevOps, while the security aspect shall be taken into consideration as well. This catalyzes the concept of DevSecOps or SecOps. In addition to the process of DevSecOps, cloud security audits are also essential in order to assess cloud services and trace significant events. Moreover, after completion of audits, organizations could be certified by Accredited Registrars. Hence, the international standard created by ISO is necessary for companies to follow. Finally, AWS GovCloud is examined to shed light on whether the security audits and ISO standard are included, and other features in detail in such a practical environment.

Keywords: Security, DevSecOps, Cloud Security, Compliance

1 Introduction

The original idea of cloud computing emerged around the 1950s with mainframe computing. However, the costs for individuals and organizations are unpractical. Then, in the 1970s, the concept of virtual machines was created. With virtualization, different virtual computers can run on the same physical hardware. In the 1990s, telecommunication companies began to provide virtualized private network connections, even though the connections were point-to-point data transmission.[20] With the increase of information system outsourcing services, the development of cloud computing has grown rapidly in recent decades.

There are three models in cloud computing: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). IaaS is at the bottom layer of cloud services and mainly provides some basic resources. Users need to control the bottom layer and implement the logic of using the infrastructure. PaaS offers a software deployment platform that abstracts hardware and software details, which can be scaled well. Developers only need to pay attention to the logic of their own business, not the bottom layer. SaaS means that software development, management, and deployment are all handled by a third party. It is unnecessary for users to care about technical issues and can use the service out of the box.

Cloud computing provides tremendous benefits to business operations. Customer service providers can share software and hardware resources to computer terminals and other devices so that it is unnecessary for business organizations to design and deploy the environment by themselves. Cloud computing service can also allow enterprise organizations to access applications and related data

without the restriction of location and physical environment, which not only saves costs for the deployment but also present a convenient method for business collaboration. If more computing resources are needed, customers can apply and pay on demand without worrying about insufficient cloud computing resources.

Since cloud computing can provide numerous benefits and much convenience, there is no doubt that it is rapidly emerging and widely accepted worldwide. However, users may not know where the data is stored and worry about data privacy issues. As part of computer security, cloud security should also be considered. To manage the cloud security issues, Ramgovind et al. mention that privacy must be designed within the cloud from the beginning, and the service providers need to provide adequate security measures in the daily operations.[24]

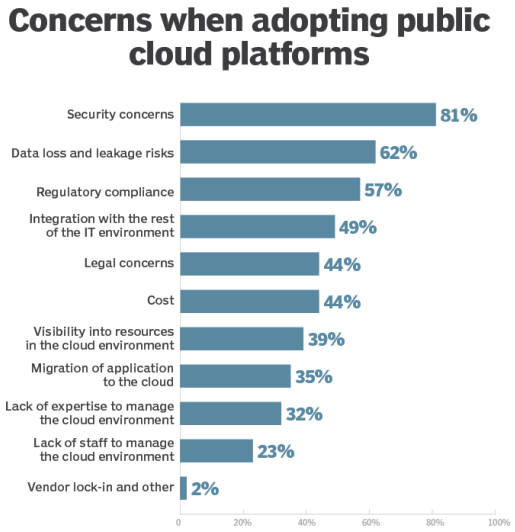

Figure 1: Concerns when adopting public cloud platforms - Security at the top (2019)[13]

In this paper, four practices of cloud security are illustrated and structured as follows: First, we will introduce SecOps. Second, we will describe auditing in cloud computing. Third, ISO compliance, cloud computing-related standards, will be elaborated. Finally, we will discuss in detail the practical design of AWS GovCloud for the United States.

2 SecOps

2.1 Definition

Before illustrating the definition of SecOps, we could first obtain the rules of creating this kind of terminology. For instance, the "DevOps" represents " Developments + Operations". Similarly, the "SecOps" could be seen as " Security + Operations". The corresponded definitions obtained by these simple combination rules are shown in Table 1. Moreover, the exact definition of "DevOps" is illustrated in Table 1 pursuant to the work by Bass, Weber, and Zhu [1].

However, the term SecOps, may not be easily defined in such a way, due to its variety of definitions we found. In this section, we would first list two different definitions of SecOps, followed by a table describing the details of definitions. Afterward, several points of view in related literature would be presented; and finally, the exact definition would be offered.

- 2 different definitions of SecOps
    1. SecOps is short for "security operations", which is the one (SecOps) we described in Table 1.

2. SecOps is interchangeable with DevSecOps and SecDevOps, which could be also seen as the integration of security practices in the DevOps processes. This is correponded to the "DevSecOps" in Table 1.

Table 1: Definitions of SecOps, DevSecOps and DevOps

	Definition	
SecOps	"Security + Operations"	A methodology that IT managers implement to enhance the collaboration between IT security and IT operations teams, helping to achieve the objectives of application and network security without compromising on application performance.
DevSecOps	"Developments + Security + Operations"	DevSecOps is the integration of both DevOps and SecOps, building security into applications during the development processes.
DevOps	"Developments + Operations"	A set of practices intended to reduce the time between committing a change to a system and the change being placed into normal production, while ensuring high quality. [1]

As two different definitions are listed above, there still continue to be a variety of SecOps definitions. Nevertheless, people have discussed "Security DevOps" more, instead of the discussion of "Security Operations". The fact could be demonstrated by the work of Jaatun et al [9]. They presented people's concerns about the security of DevOps, and further provided their metrics for the enhancement of DevOps security in cloud systems.

Furthermore, Gartner, a global research and advisory firm providing information, advice, and tools for leaders in IT, provided their recommendation and analysis of "DevSecOps"[16]. In Figure 2, we could see that they depicted the DevSecOps graphically.

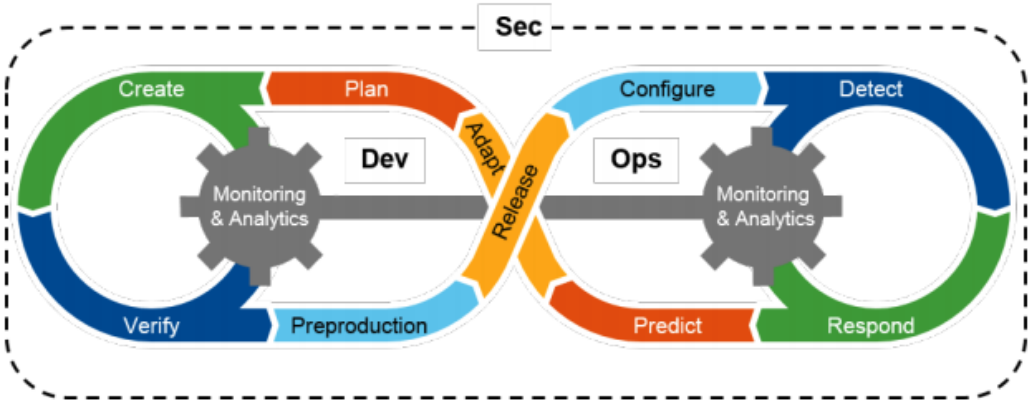

Figure 2: DevSecOps by Gartner (2016)[16]

Moreover, a multivocal literature review of DevSecOps by Myrbakken and Colomo-Palacios[19] interpreted the DevSecOps as *"a concept attempting to create and include modern security practices that can be incorporated in the fast and agile world of DevOps."* Indeed, they regard the DevSecOps as an extension of DevOps. It promotes such extension to the goal of DevOps (enhancing collaboration between developers and operators) by including security experts from the start. Also, Vaishnavi et al.[18] claimed that researchers from industry and academia agree that SecDevOps and DevSecOps imply integration of security practices in the DevOps processes. [2][23]

To conclude this part, the second definition in the list above is the one we are going to delve more into in the following sections since lots of literature and companies had paid their attention to such topics for a period. Therefore, all the SecOps in the following sections shall be seen as DevSecOps defined in the Table 1.

2.2 How SecOps Work

As the DevSecOps graphically depicted by Gartner in Figure 2, it presents the iteration from the developments to the operations with the core of continuous monitoring and analytics. Their objective is to automatically incorporate security controls without reducing DevOps agility, but achieve legal compliance (see section 4) and manage potential risks. However, it was still the superficial concept of DevSecOps. In this section, we would delve into how SecOps (or DevSecOps) works by illustrating its characteristics, workflow, and implementation in Cloud.

2.2.1 DevSecOps Characteristics

Table 2: DevSecOps characteristics [19]

Culture	It is focused on ensuring every member in the organization is aware of and responsible for security. For instance, engineers might report code injection attempts or sales may notice the suspicious emails. Moreover, a set of metrics would be created which each member agrees on and could support and implement.
Automation	The aim of automation is to make sure the security controls are 100% automatic, where the controls could be managed and deployed without manual configuration.
Measurement	In DevSecOps measurements, they not only involve business metrics (such as revenue, performance from DevOps), but also track threats and vulnerabilities throughout the development procedure.
Sharing	The security team shares the methodology, techniques, tools, knowledge to developers and operators. To be more specific, three teams (Developments, Operations, Security) share those to one another so that the security processes would be enhanced.
Shift security to the left	Unlike the traditional software development procedure which place the security at the end of process, DevSecOps move the security to the left which incorporates the security in each part of development process.

Five important characteristics - culture, automation, measurement, sharing, and shift security to the left - are illustrated in Table 2. Those features summarized by Myrbakken and Colomo-Palacios[19] are derived by the principles[1] for DevOps [7] with adding the security from the beginning of the software development process. Apparently, the core feature of DevSecOps is to merge the security controls into the DevOps procedure. Moreover, how such merging works would be illustrated in the next section.

2.2.2 DevSecOps workflow

DevSecOps workflow could be extended to 7 steps cycle from Figure 2, which includes a plan, code, build, test, release, deploy, operate. Dave in [28], emphasized that automating cloud security and management is a key DevSecOps characteristic. Figure 3 presents Dave's point of view. It is

[1]Principles of Culture, Automation, Measurement, and Sharing

important that automatic security controls are embedded in the original DevOps workflow. We further list the main tasks and sub-tasks of automating security mentioned by Dave as follows:

- Embed code analysis, testing in code quality assurance(QA)
- Add operations-centric controls:
  - Logging
  - Event monitoring
  - Configuration, patch, user, privilege management
  - Vulnerability assessment

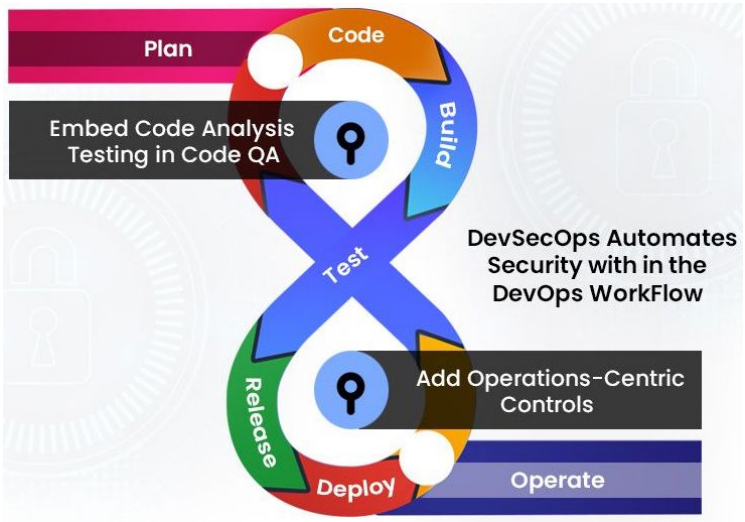

Figure 3: DevSecOps workflow[28][38]

2.2.3 Implement DevSecOps in Cloud

We have realized the characteristics and workflow of DevSecOps from previous sections. However, the implementation of DevSecOps in the cloud which fulfills the characteristics and follows the workflow is also important. We now provide 6 step process of implementation of DevSecOps in cloud[38]:

1. **Code Analysis:** The key to implementing suitable code analysis that matches the DevSecOps objectives is to realize the functionality of each approach and apply them in proper conditions. Nowadays, these functionalities could be delivered by following approaches:
   - **SAST:** Static Application Security Testing is a methodology that incrementally scans source code for vulnerabilities rather than compiles or execute it.
   - **SCA:** Software Composition Analysis detects open source security, license, and operation risks
   - **IAST:** Interactive Application Security Testing secures the runtime applications in real-time(e.g., the app is run by an automated test, interacting with the application functionality).
2. **Automated Testing:** As Dave [28] emphasized, automation is a key to DevSecOps. Automated testing could save time by simplifying the test process with minimum testing scripts and related tools.
3. **Change Management:** Incorporating the developers in the security process makes effective change management. The developers would be aware of associated tools and might find the possible vulnerabilities.
4. **Compliance Monitoring:** Compliance plays an important role in every organization in the IT industries. Here, having the legal compliance and keeping monitoring ease the burden of audit, and also maintain transparency.

5. **Threat Investigation:** Gain knowledge of possible security threats, and then establish methods to detect and respond to those threats.
6. **Personnel Training:** It is also an essential part of every organization. The personnel could gain knowledge of security via courses, training, lectures, or hand-on workshops. Indeed, improving the personnel's skills and background knowledge of security fulfills the "culture" characteristic in section 2.2.1 and would make an organization more successful in managing security issues.

3 Cloud Security Audits

3.1 Definition

There is no doubt that cloud computing is developing rapidly, business can utilize hardware and software at the same time through the Internet without having to deploy software in their physical computers. It can support convenience, reduce cost management, and also significantly improve business efficiency. There are three models in cloud services: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The cloud auditor is a party that can independently assess cloud services [15], trace and log significant events during the system operation. These events can be used for analysis, verification, and validation of security measures.

Both traditional IT audits and cloud audits have the same concerns, such as protecting information assets, maintaining data integrity, and operating effectively. However, compared with traditional IT auditing, cloud auditing has more challenges. For example, auditors need to obtain sufficient knowledge of cloud computing, familiar with cloud computing terminology[26].

3.2 Challenges

Information security in the cloud presents a series of challenges and we need cloud computing audits to protect information security. In this paper, [26], Ryoo et al. illustrate four major challenges in cloud security audits and emerging approaches.

1. **Transparency** The first main challenge of cloud computing is transparency. A good cloud security audit needs to check whether data is transparent to cloud customers because data and security are managed by a third party, and users do not know who processes the data and where data are stored. The lack of transparency can fail to gain the trust of cloud service customers and increase the risk of information security threats. Transparency is not only essential for customers to protect their data, but also for cloud service providers to establish a safer and more reliable cloud computing environment. The higher the customer's trust in the cloud, the more cloud service providers will pay more attention to cloud security issues, thus pointing out a better direction for the cloud environment.
2. **Encryption** When talking about data security, we cannot ignore encryption technology, because customers care about their personal privacy and are unwilling to disclose the data to anyone. When considering encryption in cloud computing, we need to consider whether to encrypt all data or encrypt it before sending it to the cloud. Both methods have their advantages and disadvantages. Encryption on the user side can provide convenience, but it also brings the risk of abuse of authority by the system administrator. If the entire data is encrypted, the security of the data can be effectively improved, but the decryption process will consume a lot of computing resources. In order to address this situation, we can apply a third party, and also use the homomorphic encryption method to alleviate the computational resource consumption [14].
3. **Colocation** The most prominent benefit of cloud computing is flexibility and mobility that numerous organizations can share the infrastructure. With the development and widespread application of cloud computing, there are multiple hypervisors generated, including VMWare, Oracle Virtual Box, Microsoft Virtual Server, etc. Therefore, it is very crucial for cloud service providers to control the access permission of administrators and protect user's data. In the traditional IT environment, there are a series of standards that can provide auditing. However, in the cloud setting, there is still no clear cloud security standard. Therefore, establishing standards and increasing oversight is essential. In section 4, we have more specific research related to cloud computing standards and ISO compliance.

4. **Scale, Scope, and Complexity** In cloud computing, there are a large number of systems that need to be audited. The increase of IT elements brings scale challenges, and the emergence of new technologies also presents scope challenges. In addition, because the data centers where storing organization's data and information are located in different countries, they are subject to different laws and regulations. Cloud auditors need accounting and cloud computing knowledge, as well as local legal background.

3.3 Applications

3.3.1 TrustCloud Framework

Researchers have designed and implemented some cloud audit frameworks or infrastructures to solve real-world cloud audit problems. Ryan et al. mentions in the paper [12] that virtualization is another challenge considering cloud computing. It is essential for virtualized layers to identify events on both virtual servers and physical servers, and accountability is required during the process. Accountability in cloud computing is used to protect sensitive data, gain consumer's trust and handle it responsibly.[22]

Instead of focusing on the preventive controls of the trust components, they pay more attention to the detective controls to increase accountability in this paper. In order to address the cloud accountability from several aspects, they present five abstraction layers in the TrustCloud framework, including system layer, data layer, workflow layer, polities, as well as law and regulations. This model can simplify issues in cloud security and make accountability more achievable. File-centric logging, data-centric logging, and auditing data in the software services can be accomplished in the cloud, which can not only prevent external risks but also internal risks from customer service providers.

3.3.2 An Efficient and Secure Dynamic Auditing Protocol

To provide a more effective cloud audit process, an audit service is required to check the data integrity in the cloud. However, some data checking methods can only verify static data and cannot be applied to cloud auditing services since the data is dynamic and updated in real-time in the cloud.

The paper [41] by Yang et al. introduces the research about auditing framework for data storage and data privacy. Then, they also present the auditing protocol to support the dynamic changes in the cloud, which can effectively solve the security issues, reduce computing costs for auditors and also provide efficiency. The cloud auditing protocol should have the following three characteristics: confidentiality of the owner's data, the dynamic operations of data updates in the cloud, as well as batch auditing to support multiple clouds and owners.

The system model of storage auditing protocol involves three parts: owners, cloud servers, and cloud audits. In order to prevent cloud auditors from decrypting the owner's data directly, which could lead to potential privacy risks, they implement a method that allows cloud auditors to check the correctness of authentication. For security dynamic auditing, there are two types of attack to consider: replay attack and forge attack. In response to these problems, the author introduces an index to record the abstract information of the data and modifies the tag generation algorithm to make the server unable to forge data tags. In addition, cloud auditors can combine numerous auditing requests together and utilize batch auditing techniques for multiple owners to improve the performance and efficiency of the system.

3.3.3 Privacy-Preserving Public Auditing

Another article[39] was written by Cong et al. also looks at the cloud auditing system for data storage and a public audit method for data privacy. They use HLA-based technology to verify the data and support the public audits. Compared with the MAC-based solution, the HLA technique can be aggregated and provide the authentications of linear combinations of a single data block. In order to implement the public audits system, they apply integrated homomorphic linear authentication with random masks, so that the third-party auditors cannot view or obtain customer data and ensure data privacy. The audit system also supports batch auditing and dynamic data updates, which significantly improve efficiency for auditors.

4 ISO Compliance

Compared to get a certification of the ISO, more and more companies decide to be ISO Compliance because of the time-consuming and costly. ISO Compliance means a company adhere to ISO standards but does not get the certification. It will also help the company build a security system.

4.1 Introduction

When we talk about ISO Compliance, we need to introduce two international organizations related to this topic first. The first organization is the International Organization for Standardization (ISO), which focuses on publishing new standards in many fields. The International Electrotechnical Commission (IEC) also works on proposing new standards, but it only focuses on the fields of electrical engineering and electronic engineering. The famous standards of building an information security management system (ISMS) is the family of 27000 standards. These standards are published jointly by the ISO and IEC. Nowadays, they have become the most powerful guidelines of information security.

4.2 ISO Standard

In this section, we will show you an overview of the related standards in Table- 3 and describe them in detail later.

Table 3: Standards of ISO/IEC

Standard	Content
ISO/IEC 27001[31]	The information security management system aims to provide a method for all types of organizations in establishing, implementing, operating, supervision, reviewing, maintaining and improving the information security management system.
ISO/IEC 27002[32]	It is a instructional standard which is used as a reference to help company to select control measures when implementing an information security management system, or as a guidance for companies to select information security control measures.
ISO/IEC 27017[33]	This standard is used to provide enhanced control for cloud service customers and cloud service providers to build a security cloud environment. It also clarifies the roles and responsibilities of both the users and the providers to ensure the data safety.
ISO/IEC 27018[34]	PII (Personally Identifiable Information) is the most important part in this standard. It provides us a guidance of how can we protect the PII based on the ISO/IEC 27002.
ISO/IEC 27032[35]	This standard focus on the Cybersecurity on the Internet. It shows us some issues in this field and proposes some instructions on how to avoid the Cybersecurity problems.

As we can see in the table above, these standards work together to help companies build an information security management system.

4.2.1 ISO Standard 27001 27002

Standard 27001 has the title of "Information technology—Security techniques—Information security management systems—Requirements". This standard can help companies of all sizes (from a small company to a worldwide multinational) and all fields (such as government, university, healthcare)

implement a system that meets the requirements of being an information security management system. The requirements in this standard include all steps a company will experience in its life spans, such as the implementing stage, operating stages, and development stage. Including 27001, the ISO 27 K family of standards refer directly to the "Plan-Do-Check-Act" (PDCA cycle) cycle—well known from Deming's classic quality management[6], which can give us a brief understanding of the steps we need to take to build an information security management system by a model.

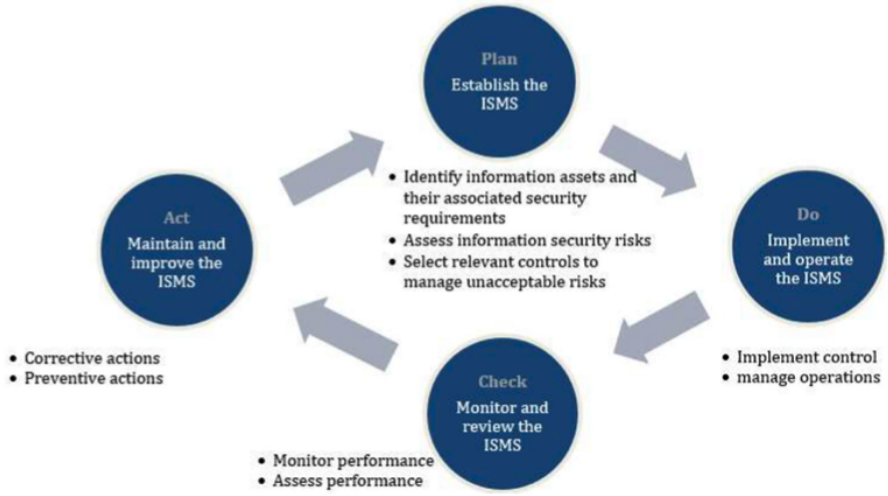

Figure 4: PDCA cycle in ISO 27001[36]

Figure 4 comes from the article written by Najat Tissir[36]. This cycle can work with ISO standards to help company build the system. According to this figure, when we want to build an ISMS, we need to understand the information assets and their security requirements and find out suitable controls to manage risks. Some documents used to guide the developers are necessary for this step. Implementation is the next step in this figure, controls and measures written in documents are implemented, ISMS is managed appropriately. We also need to formulate some plans to encounter risks in this step. After the implementation step, it is important to monitor and review your ISMS system. Take the documents we use before, check if the system is running to conform to the regulation in the first step. It will help you find out potential security risks and know more about the system. With the help of our monitor and review step, we are acknowledged that there are some risks and short-comes in our system. In the final step, we correct some wrong actions and do some precautions to improve our system. The cycle of steps will help a company continuously improve its ISMS.

The requirements in ISO 27001 are described in detail in another standard: ISO 27002. It describes the necessary steps to identify and assess security risks to determine the requirements for protecting information and information systems. The continuous development of ISO 27002 is based on the content of ISO 27001, which explains the 39 control objectives listed in ISO 27001 in more detail. A total of 134 measures have been allocated to these goals, which are reasonable and described in detail in 27002[6].

4.2.2 ISO Standard 27017 27018

These two standards focus on the field of cloud. The ISO standard 27017 is an expansion of the 27001. It not only provides the control sets from ISO 27001 but also proposes 7 new controls about the cloud. It is necessary to clarify the responsibility between both cloud service providers (CSP) and customers. Following are the terms of security responsibilities from 27017 with cloud service providers, some with the customer, and some are shared with both[40].

- Who is responsible for the relationship between the cloud service provider and the cloud customer
  - This relationship need to be clearly laid out, recorded and communicated.
- When the contract is terminated, how to deal with the assets

  - These assets belongs to the customers should be returned or removed.
- How to protect and separate the customers' virtual environment.
- Virtual machine configuration
  - Customers and providers should ensure the virtual machine's configuration and strength to meet the security requirements.
- Cloud environment-related management operations and processes
  - List the responsibilities with the customers on defining, monitoring and documenting the cloud related administrative operations.
- How can customers monitor the cloud activities
- Connection between cloud network environment and virtual environment
  - Addresses building standards and configurations must be consistent. So the virtual network environment is in line with information security policies around the physical network[40].

Another standard pay attention to the PII (Personally Identifiable Information). It gives us some definitions related to PII and guidance on how to protect the PII. It tells us some definitions about the PII Principal, PII Controller, PII Processor which can help companies to clarify the responsibilities in the cloud. What should data processors do to protect the PII is described as follows[40].

- Notice customers if their PII is being used
  - Such as the PII is processing by others or accessed by unauthorized activity.
- Help customers to manage their PII
  - The PII controller should have rights to access, modify and delete their PII.
- Virtual machine configuration
  - Customers and providers should ensure the virtual machine's configuration and strength to meet the security requirements.

Companies can use these standards in conjunction to provide enhanced control for cloud services.

4.2.3 ISO Standard 27032

This standard mainly addresses the problems in the field of cybersecurity. It focuses on attacks caused by malicious and potentially unwanted software, social engineering attacks, information sharing in cybersecurity[36]. What's more, it provides some advice and guidance to deal with the cybersecurity risks and proposes to build a formalized framework to share cybersecurity problems and experiences in dealing with them.

4.3 Application

For those large companies, get the ISO certification is worth doing because you can drive the trust of others in your business, provide a competitive advantage to your company, protect brand reputation, facilitate the development of enterprises, and help your company become a multinational early.

However, for those small companies, it is a time-consuming and unaffordable cost. So there are many types of research focus on using these standards to check security by companies. Article from NA Kamaruddin proposed a pre-assessment model for cloud providers to determine if their system is safe[10]. It can assess the cloud security readiness level to judge if the measures used here are safe enough. And it also can help the organization increase the awareness of cloud security.

These standards can increase the development of cloud services. Here we would like to introduce an example about PII data in cloud services from Kemp. Microsoft uses this standard immediately after the publication of the 27018 to protect the services in its cloud. And this standard can be used across the service delivery models and the layers in the main model [11].

Finally, we can also use these standards to investigate the data quality in cloud services[25] and propose solutions related to cloud security in smart business[8].

4.4 Problems in Cloud

There are some areas that ISO does not include in their standard, it may cause some risks in security. It does not contain the protection of the Audit part, which may help attackers delete logs after access the cloud services. The missing part of high-risk environments in these standards can lead to advanced persistent threats and side-channel attacks[4].

5 AWS GovCloud

With cloud computing developing fast, the market size of cloud computing grows over a 30% compound annual growth rate reaching $383.4 billion in 2020. This figure is expected to be updated to $832.1 billion by 2025.[30] Governments around the world have passed various legislation related to the safeguard of sensitive or private data. In this section, we will look insight at one security practice of the famous cloud service provider, AWS GovCloud, especially for the United State.

5.1 Definition

AWS GovCloud literately contains the connotation of two parts, AWS and GovCloud.

AWS stands for Amazon Web Services. Amazon has a long history using a decentralized IT infrastructure. With the impact and promise of cloud computing, Amazon has spent more than thirty years and over six billion dollars building and managing the large-scale, reliable, and efficient IT infrastructure that powered one of the world's largest online cloud service providers. AWS was launched in 2006 to enable other organizations could benefit from Amazon's experience and investment in running a large-scale distributed, transactional IT infrastructure. Today, it serves hundreds of thousands of customers worldwide.[37]

Users purchase AWS to request compute power, storage, and other services in minutes and have the flexibility to choose the development platform or programming model that makes the most sense for the problems to solve. Some well-known cloud services provided by AWS are EC2 and S3 These services have a different purpose and use different databases such as RDS, DynamoDB, and Elastic Cache.[21]

GovCloud means AWS gives state and federal government customers and their partners the flexibility to architect secure cloud solutions. AWS GovCloud has commercial cloud capability across all classification levels making it possible to execute missions.

- Unclassified: non-sensitive data and workloads
- Sensitive: classified sensitive non-government workloads
- Secret: classified sensitive by non-intelligence government organizations
- Top Secret: separated from the public Internet, hosted on-premise at the CIA

AWS GovCloud (US) provides an environment where those customers can run ITAR-compliant applications and provides special endpoints that utilize only FIPS 140-4 encryption.[21] As mentioned previously, AWS GovCloud follows and complies with the government regulations and compliance regimes, which is discussed detailedly in the next Subsection.

5.2 Regulation and Compliance

For all AWS data centers worldwide, they include the ISO 27001 certification[31]. AWS holds the FISMA moderate certification also it operates over the FIPS 140-2 validated hardware.[29] Adhering to the FISMA guidelines AWS rotates keys. Amazon provides reporting processed for security vulnerabilities and penetration testing.[21]

For United States Government, AWS GovCloud compliance features include data safety and access control, with granular control of individual data at the API level. AWS GovCloud (US) complies with the FedRAMP High baseline, Cloud Computing Security Requirements Guide, and other compliance regimes.

These and other security-related regulations bring it into full compliance with a broad range of United State government security and restricted access regulations.[17]

- Federal Risk and Authorization Management Program (FedRAMP)
- Department of Defense Security Requirements Guide (SRG) through level 5
- Department of Justice Criminal Justice Information Service Security Policy
- Defense Federal Acquisition Regulation Supplement (DFARS)
- U.S. International Traffic in Arms Regulations (ITAR)

The USA Air Force's Next Generation GPS runs in AWS GovCloud, and so does the General Services administration's website, which is the central cloud platform used by the federal government. Plus, the Justice Department uses AWS GovCloud both for internet operations and public-facing services.[17] Therefore, AWS GovCloud (US) must follow the regulations and compliance regimes of the American state and federal government to control access to sensitive data and keep authentication of secret workloads.

5.3 Security Features

The same principles of security apply as for other non-cloud systems, but the main differences are the lack of control of the cloud services and the secrecy of how these systems are managed by AWS GovCloud.[5] It takes some measures to protect the security of data and workloads. We discuss three of the most common practice AWS GovCloud (US) has taken.

Besides government strict requirements of regulations and compliance, users must pass the AWS GovCloud screening process. All customers who use AWS GovCloud (US) must either be Government organizations or other approved private entities in Government-related industries such as we mentioned before.[17] Each customer is vetted to ensure they are a United States entity and cannot be prohibited or restricted by the United States government from exporting or providing services. AWS GovCloud no matter US-East or West Region is only operated by employees who are United States citizens on United States soil. It is only accessible to United States entities and root account holders who pass a screening process.

The second feature is the independence of resources. Network, Data, and Virtual Machines in GovCloud are isolated from all other AWS Cloud Regions. AWS GovCloud features a separate identity and access management stack with unique credentials, which only work with the GovCloud region, and comes with a dedicated management console, as well as endpoints that are specific to the GovCloud region.[3] Separate physical resources make sure of enclosure of a working environment. The probability of being attacked significantly decreases.

The third measure is a specific department, AWS Security Hub. It is the department responsible for cloud security. AWS Security Hub gives a comprehensive view of the security posture of the services. These security controls detect when accounts and deployed resources do not align with security best practices defined by AWS security experts. There is a range of powerful security tools, from firewalls and endpoint protection to vulnerability and compliance scanners. Important and common security measures include DDoS protection, brute-force detection, secure HTTPS access using SSL, built-in firewall, multi-factor authentication, private subnet etc.[21]

5.4 Services

Look back to the cloud service itself, AWS GovCloud not only provides services the same as ordinary region version but also has additional unique services mainly focused on security.[27]

- Safeguard sensitive data — shield sensitive unclassified data with server-side encryption in Amazon S3. Store and handle security keys yourself with AWS Key Management Service (AWS KMS).
- Improve cloud visibility — audit access and use of sensitive data with your keys in AWS CloudTrail, operated by US citizens.
- Strengthen identity management — restrict access to sensitive data by time and location, and specify which API calls users can make. GovCloud offers powerful access control features.
- Shield accounts and workloads — apply continuous security monitoring for AWS accounts and workloads using Amazon GuardDuty. Monitor workloads for malicious or unauthorized behavior that may indicate an account compromise.

We also review two commonly used services, EC2 and S3, which we are familiar with. Compared with a regular type of AWS, we can discover what special limitations are set to raise the security level.

Elastic Compute Cloud (EC2) provides resizable computing capacity that users build and host software systems. In AWS GovCloud, we must launch all EC2 instances in a virtual private cloud. EC2 Serial Console is currently disabled in AWS GovCloud (US). The image copy and snapshot copy do not support the origin of another AWS Region. And we can only use the API-only method to conduct the CPU optimization in AWS GovCloud (US).

Simple Storage Service (S3) is storage for the internet, which provides several interfaces for access. AWS GovCloud is a closed storage environment, as we mentioned in **5.3** independency. We cannot copy the data of an S3 bucket in the AWS GovCloud Regions to or from another AWS Region. It is required to use the Amazon Resource Names identifier. The name of the bucket must be unique in AWS GovCloud and not be shared across other standard AWS Regions. S3 transfer acceleration is also disabled.

There are many restrictions and limitations in usages of AWS GovCloud (US), which can be found in the manual documentation. For more intuitively acknowledged, we just show some of them to learn the advanced security protections applying to AWS GovCloud.

6 Discussion

It could be emphasized that the core of DevSecOps is to shift security to the left. Unlike the traditional DevOps which implements the security testing after the step of releasing, the DevSecOps keep security controls through all the process of software development. That is, the security scanning is implemented from the start of the development procedure. An apparent benefit is that the vulnerabilities could be found earlier. Therefore, the security issue could be solved and be managed as soon as possible; and it would decrease the probabilities of bug found by customers. That is why the "security shift to the left" should be considered to merge into the DevOps procedure.

Cloud auditing plays an important role in cloud computing. Based on the literature review, we have discussed several major challenges in cloud auditing and related strategies. We have also studied some technologies of audit frameworks or infrastructure, and the benefits they bring. As cloud computing is still undergoing continuous development and progress, it is very necessary to design a credible auditing mechanism for cloud computing.

When we look at the standards related to information security management systems and cloud security, plenty of organizations have published multiple standards to verify the security of a cloud. However, there is no single standard that can cover all the potential risks. As the BSI C5, it omits six controls compared to other standards. And according to Di Giulio et al. 's attack model, the most frequent risks caused by omissions in C5 are at the cloud level and are internal threats[4]. So we think it is important to combine them to get a higher safety level.

The practice of cloud security for both public and private cloud providers is still facing challenges in implementing the cloud computing model. That is one of the main reasons that AWS GovCloud has only open its business to the United States. The legislation protecting sensitive data and workloads is another obstacle. Laws, regulations, and compliance vary around the world. Therefore, it is impossible for a cloud service provider to deploy the private cloud services globally, like government-oriented business. One current solution is that government cooperates with local cloud service providers to establish private clouds to maintain the security of cloud services.

7 Conclusion

In this review, we first look at the history of cloud computing and security problems related to the cloud nowadays. Afterward, the definition of SecOps is clarified by comparing the concepts of SecOps, DevSecOps, and DevOps; and also by the information gathered from lots of literature. The workflow and characteristics of DevSecOps in this review are used to introduce the implementation of DevSecOps in the cloud. We find that several features are of great importance in implementation. In the Audits section, we introduce the definition of cloud audits and the challenges. The audits are wildly used in the cloud to check if the system is safe enough. We also introduce some standards

about ISMS and cloud security that come from ISO to use as guidance to build a safe system. These standards can not only be used as certification references but also increase the development of cloud services. After that, we describe an example of AWS and GovCloud. It is a real-world example that pays more attention to the security problems in the cloud because of its usage. The security of the cloud attracts an increasing number of attentions , but there is still some problem in this field.

References

[1] Len Bass, Ingo Weber, and Liming Zhu. *DevOps: A software architect's perspective*. Addison-Wesley Professional, 2015.

[2] S Cash et al. "Managed infrastructure with IBM cloud OpenStack services". In: *IBM Journal of Research and Development* 60.2-3 (2016), pp. 6–1.

[3] CloudBasic. *AWS GOVCLOUD (US)*. [EB/OL]. `https://cloudbasic.net/aws/rds/alwayson/govcloud/` Accessed May 26, 2020.

[4] Carlo Di Giulio et al. "Cloud standards in comparison: Are new security frameworks improving cloud security?" In: *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*. IEEE. 2017, pp. 50–57.

[5] Oscar Diez and Andres SIlva. "Govcloud: Using cloud computing in public organizations". In: *IEEE technology and society magazine* 32.1 (2013), pp. 66–72.

[6] Georg Disterer. "ISO/IEC 27000, 27001 and 27002 for information security management". In: (2013).

[7] Jez Humble and Joanne Molesky. "Why enterprises must adopt devops to enable continuous delivery". In: *Cutter IT Journal* 24.8 (2011), p. 6.

[8] Igor Ivkic et al. "On the cost of cyber security in smart business". In: *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE. 2017, pp. 255–260.

[9] Martin Gilje Jaatun, Daniela S Cruzes, and Jesus Luna. "Devops for better software security in the cloud invited paper". In: *Proceedings of the 12th International Conference on Availability, Reliability and Security*. 2017, pp. 1–6.

[10] Nur Ahada Kamaruddin et al. "CLOUD SECURITY PRE-ASSESSMENT MODEL FOR CLOUD SERVICE PROVIDER BASED ON ISO/IEC 27017: 2015 ADDITIONAL CONTROL". In: *Revolution* 2.5 (), pp. 01–17.

[11] Richard Kemp. "ISO 27018 and personal information in the cloud: First year scorecard". In: *Computer Law & Security Review* 31.4 (2015), pp. 553–555.

[12] Ryan K.L. Ko et al. "TrustCloud: A Framework for Accountability and Trust in Cloud Computing". In: *2011 IEEE World Congress on Services*. 2011, pp. 584–588. DOI: `10.1109/SERVICES.2011.91`.

[13] George Lawton. *Use modern cloud security best practices*. Aug. 2019. URL: `https://searchcloudcomputing.techtarget.com/tip/Use-modern-cloud-security-best-practices`.

[14] Jian Li et al. "A simple fully homomorphic encryption scheme available in cloud computing". In: *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*. Vol. 1. IEEE. 2012, pp. 214–217.

[15] Fang Liu et al. "NIST cloud computing reference architecture". In: *NIST special publication* 500.2011 (2011), pp. 1–28.

[16] N MacDonald and I Head. "Devsecops: How to seamlessly integrate security into devops". In: *Gartner, Tech. Rep.* (2016).

[17] Joseph Mahakian et al. *AWS GovCloud Resource and Cost Analysis*. Tech. rep. The MITRE Corporation, 2020.

[18] Vaishnavi Mohan and L Othmane. "SecDevOps: is it a marketing buzzword". In: *Department of Computer Science, Technische Universität Darmstadt, Darmstadt* (2016).

[19] Håvard Myrbakken and Ricardo Colomo-Palacios. "DevSecOps: a multivocal literature review". In: *International Conference on Software Process Improvement and Capability Determination*. Springer. 2017, pp. 17–29.

[20] Maximilliano Destefani Neto. *A brief history of cloud computing*. Mar. 2014. URL: https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/.

[21] Deepak Panth, Dhananjay Mehta, and Rituparna Shelgaonkar. "A survey on security mechanisms of leading cloud service providers". In: *International Journal of Computer Applications* 98.1 (2014), pp. 34–37.

[22] Nick Papanikolaou, Siani Pearson, and Nick Wainwright1. "Accountability in Cloud computing". In: *BUILDING International Cooperation for Trustworthy ICT* (2011), pp. 1–3. URL: www.bic-trust.eu/files/2013/01/Papanikolaou_AccountabilityInCloudComputing_June2012.pdf.

[23] Akond Ashfaque Ur Rahman and Laurie Williams. "Software security in devops: synthesizing practitioners' perceptions and practices". In: *2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED)*. IEEE. 2016, pp. 70–76.

[24] S Ramgovind, M M Eloff, and E Smith. "The management of security in Cloud computing". In: *2010 Information Security for South Africa*. 2010, pp. 1–7. DOI: 10.1109/ISSA.2010.5588290.

[25] Jonathan Roy, Hebatalla Terfas, and Witold Suryn. "On the use of ISO/IEC standards to address data quality aspects in Big Data Analytics cloud services". In: *International Conference on Business Information Systems*. Springer. 2017, pp. 149–164.

[26] Jungwoo Ryoo et al. "Cloud Security Auditing: Challenges and Emerging Approaches". In: *IEEE Security Privacy* 12.6 (2014), pp. 68–74. DOI: 10.1109/MSP.2013.132.

[27] Amazon Web Services. *AWS GovCloud (US)*. [EB/OL]. https://aws.amazon.com/govcloud-us/ Accessed May 26, 2020.

[28] Dave Shackleford. "The devsecops approach to securing your code and your cloud". In: *SANS Institute InfoSec Reading Room A DevSecOps Playbook* (2017).

[29] Preston Smith, Baijian Yang, and Carolyn Ellis. "Trusted CI webinar: REED+ Purdue's Evolution From a CUI Environment to an Ecosystem to a Community". In: (2021).

[30] Aishwarya Soni and Muzammil Hasan. "Pricing schemes in cloud computing: a review". In: *International Journal of Advanced Computer Research* 7.29 (2017), p. 60.

[31] International Organization for Standardization. *ISO/IEC 27001:2013*. 2013.

[32] International Organization for Standardization. *ISO/IEC 27002*. 2005.

[33] International Organization for Standardization. *ISO/IEC 27017*. 2015.

[34] International Organization for Standardization. *ISO/IEC 27018*. 2019.

[35] International Organization for Standardization. *ISO/IEC 27032*. 2012.

[36] Najat Tissir, Said El Kafhali, and Noureddine Aboutabit. "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal". In: *Journal of Reliable Intelligent Environments* (2020), pp. 1–16.

[37] Jinesh Varia, Sajee Mathew, et al. "Overview of amazon web services". In: *Amazon Web Services* 105 (2014).

[38] Veritis. *DevSecOps Solution to Cloud Security Challenge*. https://www.veritis.com/blog/devsecops-solution-to-cloud-security-challenge/.

[39] Cong Wang et al. "Privacy-Preserving Public Auditing for Secure Cloud Storage". In: *IEEE Transactions on Computers* 62.2 (2013), pp. 362–375. DOI: 10.1109/TC.2011.245.

[40] Tim Weil. "Taking compliance to the cloud—Using ISO standards (tools and techniques)". In: *IT Professional* 20.6 (2018), pp. 20–30.

[41] Kan Yang and Xiaohua Jia. "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing". In: *IEEE Transactions on Parallel and Distributed Systems* 24.9 (2013), pp. 1717–1726. DOI: 10.1109/TPDS.2012.278.