network

Review

An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions

Milan Chauhan [1] **and Stavros Shiaeles** [2,*]

[1] Department of Computing, University of Portsmouth, Portsmouth PO1 2UP, UK; up2093411@myport.ac.uk
[2] Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth PO1 2UP, UK
* Correspondence: stavros.shiaeles@port.ac.uk

Abstract: The rapidly growing use of cloud computing raises security concerns. This study paper seeks to examine cloud security frameworks, addressing cloud-associated issues and suggesting solutions. This research provides greater knowledge of the various frameworks, assisting in making educated decisions about selecting and implementing suitable security measures for cloud-based systems. The study begins with introducing cloud technology, its issues and frameworks to secure infrastructure, and an examination of the various cloud security frameworks available in the industry. A full comparison is performed to assess the framework's focus, scope, approach, strength, limitations, implementation steps and tools required in the implementation process. The frameworks focused on in the paper are COBIT5, NIST (National Institute of Standards and Technology), ISO (International Organization for Standardization), CSA (Cloud Security Alliance) STAR and AWS (Amazon Web Services) well-architected framework. Later, the study digs into identifying and analyzing prevalent cloud security issues. This contains attack vectors that are inherent in cloud settings. Plus, this part includes the risk factor of top cloud security threats and their effect on cloud platforms. Also, it presents ideas and countermeasures to reduce the observed difficulties.

Keywords: cloud security; security frameworks; NIST; COBIT; ISO; AWS; ENISA

check for updates

Citation: Chauhan, M.; Shiaeles, S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network* **2023**, *3*, 422–450. https://doi.org/10.3390/network3030018

Academic Editor: Khaled Elleithy

Received: 26 July 2023
Revised: 16 August 2023
Accepted: 1 September 2023
Published: 12 September 2023

1. Introduction

First and foremost, what exactly is cloud computing? Cloud computing is a technology that allows anybody to remotely access high computing equipment and computing services without having to purchase physical infrastructure. And the fundamental advantage of cloud computing is that it only costs on a pay-as-you-go basis. The cloud is a game-changing technology because it enables flexibility, scalability, and a cost-effective means of managing IT resources. According to recent predictions, the worldwide cloud computing market will exceed $800 billion in the next 2–3 years [1–3].

However, the acceptance and expanded use of cloud computing raises security concerns. Data breaches, unauthorized access, and data loss during transfer or due to system failure are examples of security issues. Five factors determine the major component of security concerns [4–6].

1. Network related
2. Confidentiality and privacy
3. Data-related issues
4. Virtualization-related issues
5. Others

Cloud security frameworks are created to assist organizations in understanding their vulnerabilities when building cloud infrastructure. Cloud security frameworks are a collection of rules, standards, and best that companies may use to safeguard their cloud environments against security risks. Its core overview is the required policies, tools, settings, and procedures for securing and managing cloud infrastructure. It helps organizations to identify, access, and reduce risks by providing a systematic method for managing cloud security threats.

There are several well-known frameworks available. CSA STAR (Cloud Security Alliance Control Matrix), FedRAMP, NIST (National Institute of Standards and Technology), COBIT 5, International Organization for Standardization, and Well-Architected Cloud Frameworks (AWS, Azure, Google) are a few examples. Companies confront considerable issues when it comes to guaranteeing the confidentiality, integrity, and availability of their data and applications in cloud environments. Inadequate cloud security typically leads to vulnerabilities, unauthorized access, data breaches, and significant harm to the organization's brand and consumer confidence.

In carrying out this evaluation project, it is essential to identify the targeted outcomes of the project. The question behind the author's mind is as follows:

1. What is the procedure for implementing a cloud security architecture in an organization? What tools are needed to carry out each step?
2. What are the important issues for organizations when establishing a cloud security strategy in terms of training, awareness, and change management?

Hypothesis on cloud security frameworks.

Hypothesis 1: *The effectiveness of cloud security frameworks significantly influences the overall security posture of cloud-based systems.*

Hypothesis 2: *The implementation process of the Cloud Security Framework is very hard to understand.*

Hypothesis 3: *Implementing comprehensive security measures and adopting robust solutions can effectively mitigate common cloud security problems and enhance the overall security posture of cloud environments.*

At this juncture, it is valuable to provide an overview of the structural organization of this study paper, along with the underlying reasons that guided its composition. This paper endeavors to comprehensively delve into the intricate domain of cloud security frameworks, highlighting prevailing challenges and presenting potential remedies. To achieve this objective, the paper has been meticulously structured into distinct sections, each serving a pivotal role in presenting a cohesive narrative.

The following is a synopsis of each chapter:

Section 1 is the study's rationale and introduction. This contains the purpose, objectives, research questions, and hypothesis.

Section 2 provides an overview of the literature on cloud computing, cloud security frameworks, and cloud security concerns and solutions. The literature review is carried out by searching certain questions.

- A Historical Overview of Cloud Computing
- A critical examination of the history and context of cloud security frameworks
- Description of gaps, prior study's findings, cloud security framework discussion areas and views, cloud security concerns and solutions
- A description of why this study is vital and how it will help the field.

Section 3 covers the concepts, pillars, weaknesses, and strengths of the frameworks, as well as the ways to apply each phase of the frameworks.

Section 4 depicts the top five most prevalent cloud computing security issues, along with the names of the methods that attackers can use and remedies to prevent them.

Section 5 is the paper's conclusion.

2. Literature Review

Cloud computing has its roots in several fundamental concepts and technologies. In the 1960s, J.C.R. Licklider, a prominent computer scientist, envisioned an "Intergalactic Computer Network" that allowed remote access to programs and data, laying the groundwork for distributed computing models. In the 1990s, grid computing emerged as a way to harness geographically dispersed resources for computationally intensive tasks. The Globus Toolkit, developed by Ian Foster and Carl Kesselman, provided a software infrastructure for managing computational grids. Utility computing also emerged during this time, offering computing resources as a pay-per-use utility. Sun Microsystems and Amazon introduced utility computing models, demonstrating the benefits of on-demand resource rental.

The phrase "cloud computing" first appeared in the mid-2000s, revolutionizing how computer resources are distributed and utilized. Amazon Web Services (AWS) established Infrastructure as a Service (IaaS) in 2006, providing virtualized servers, storage, and networking capabilities via the Internet. This revolutionized traditional hosting paradigms by introducing scalable and adaptable cloud-based infrastructure. The National Institute of Standards and Technology (NIST) was instrumental in standardizing cloud computing, describing it in 2011 as a concept that allows on-demand network access to a shared pool of programmable computing resources. NIST emphasized the model's ease of use and universality. Extensive study has been conducted to examine many views on cloud computing, offering insight into its consequences and potential.

2.1. Cloud Security Frameworks

2.1.1. Ability of Framework

Cloud security frameworks are designed to ensure an organization's data's confidentiality, integrity and availability in a cloud environment [3]. Undertook a critical examination of the usefulness of new security frameworks in increasing cloud security. The study aims to analyze and evaluate various cloud security standards and frameworks to assess their strengths, limitations, and overall influence on improving cloud security posture. The authors undertook a thorough examination of many well-known cloud security frameworks, including the Cloud Security Alliance (CSA) Security Guidance, the NIST Cloud Computing Security Reference Architecture, and the ISO/IEC 27017:2015 Cloud Security Controls. These frameworks were assessed based on their ability to meet important cloud security concerns such as data protection, access management, encryption, and incident response. The study revealed the benefits and drawbacks of each framework through a comparison. It provided readers with insights into the precise security controls and recommendations provided by these standards, allowing them to grasp their application and significance in various cloud deployment models. Furthermore, the study looked at how new security frameworks fared compared to earlier standards [5].

Di Giulio's [5] research paper adds to the current body of knowledge by offering a complete comparison of cloud security standards and frameworks. It is a great resource for practitioners and academics who want to understand the strengths and limitations of various security frameworks and make educated decisions when adopting cloud security. Key difficulties in cloud computing, according to Gartner, include governance, cloud environment selection, and security/privacy. Cloud investments should be guided by the board of directors in order to minimize risk, regulate expenses, and produce profit [7]. Table 1 will describe the perpective, different conversional topics and future work or gaps of cloud security frameworks.

Table 1. Perspective, Debates and Gaps of Cloud Security Framework.

Cloud Security Framework		
Perspective	Risk Management	These frameworks seek to give a systematic way to detect possible security threats, vulnerabilities, and risk levels. In the context of cloud settings, they frequently emphasize the significance of risk assessment, risk treatment, and risk monitoring.
	Security for organization	These frameworks provide security policies for a variety of areas, including identity and access management, encryption, network security, and incident response.
	Compliance	These frameworks offer rules and recommendations for achieving certain compliance standards including GDPR, HIPAA, PCI DSS, and FedRAMP.
	Perspective on Architecture and Design	These frameworks offer recommendations for developing safe cloud architectures, such as network segmentation, data isolation, multi-tenancy, and secure deployment methods.
Debates	standardization vs. Customization in Implementation	Standardization encourages uniformity and simplicity of implementation; customization enables organizations to adjust security policies to their individual requirements. To handle organizational requirements and particular hazards, the correct mix of standardization and customization is critical.
	Centralized vs. Decentralized Implementation	Whether the responsibility for executing cloud security frameworks should be centralized or distributed across several departments. While centralization guarantees consistency and centralized expertise, decentralization may improve agility and alignment with individual business units.
Gaps	Lack of knowledge and comprehension	The security policies and recommended may be improper recommendations or misinterpreted.
	Inadequate Training and Skill	Lack of training may not invest properly in growing the skills of their employees, resulting in implementation gaps and issues.
	Inadequate Configuration and Customization	May miss this phase or fail to fully apply the appropriate configurations, exposing possible risks and holes in their security posture.

2.1.2. Use of Framework

It went over how these frameworks addressed new security problems including container security, DevOps security, and threat information sharing. The study's findings offer light on the changing landscape of cloud security frameworks and their influence on cloud security. It emphasized the significance of continuously evaluating and improving these frameworks in order to with the dynamic nature of cloud threats. ISACA recommends adopting the COBIT 5 framework to oversee and manage cloud investments, guaranteeing consistency in order to maximize value and minimize risk. Overall, strategy alignment and goal accomplishment are critical in cloud computing, making cloud governance a crucial feature. This framework integrates several crucial components, including governance, risk management, compliance, incident response, and ongoing monitoring. It stresses the necessity for a comprehensive and proactive approach to ensuring cybersecurity in cloud settings. SLA management is critical in the governance structure and cannot be emphasized. NIST, ISACA, and CSA principles were used to create a scorecard prototype for cloud SLAs (ISACA, 2012), (CSA, 2011), and (NIST, 2011). From conference paper of Naseer's emphasizes the need to address security, data privacy, and availability issues as critical parts of cloud risk management [8]. Table 1 will describe the perpective, different conversional topics and future work or gaps of cloud security frameworks.

2.1.3. Implementation Challenges

Implementing cloud security frameworks presents a range of challenges stemming from the complex nature of cloud ecosystems and evolving threat landscapes. Studies by [9,10] emphasize the following challenges:

Integration Complexity: Organizations often struggle with integrating cloud security frameworks seamlessly into existing IT infrastructures, resulting in interoperability issues and redundant controls.

Resource Allocation: Limited resources, both human and financial, can hinder effective implementation [11] suggest that organizations must carefully allocate resources to address critical security controls.

Shared Responsibility Model: Cloud providers and users share responsibility for security. Defining roles and responsibilities can lead to ambiguity and gaps in implementation.

Compliance and Regulations: Ensuring compliance with industry regulations and data protection laws adds complexity to implementation [11] highlight the need to adapt frameworks to meet specific regulatory requirements.

Dynamic Environment: Cloud environments are dynamic and scalable, making continuous monitoring and control adaptation a challenge. Automation and real-time threat detection are vital to maintaining security.

While the literature on cloud security frameworks is rich, earlier research has highlighted many limitations. These gaps represent areas where further research and development are required to improve the efficacy of cloud security systems.

2.2. Cloud Security Problems and Solutions

Cloud computing has revolutionized the way organizations store, process, and access data and applications. However, this paradigm shift has introduced a range of security challenges (as shown in Figure 1) that need to be addressed to ensure the confidentiality, integrity, and availability of data in the cloud [12–14].

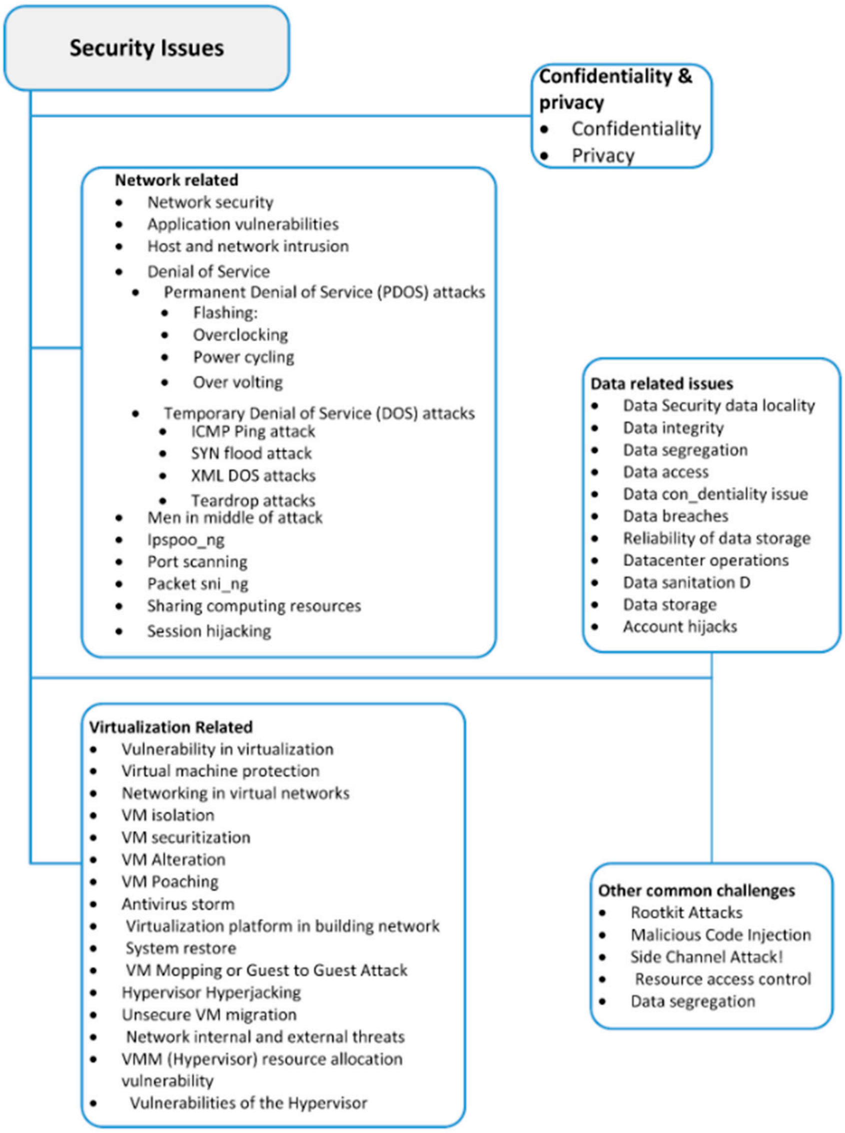

Figure 1. Main Components of Cloud Security Issues. Image Source: [15].

2.2.1. Cloud Security Problems

Data Privacy and Leakage: Data privacy concerns arise due to the shared nature of cloud environments. Unauthorized access or data breaches can lead to sensitive information leakage [16].

Data Location and Jurisdiction: The dynamic nature of cloud infrastructures can lead to uncertainty about the physical location of data, potentially causing conflicts with data protection regulations and legal jurisdictions [17].

Multi-tenancy Risks: Multi-tenancy introduces the risk of resource and data co-residency, where data from different customers may reside on the same physical hardware, potentially leading to data exposure [18].

Inadequate Access Control: Ensuring proper access control mechanisms to prevent unauthorized users from accessing resources and data is challenging in cloud environments with complex access requirements [18].

2.2.2. Cloud Security Solutions

Various methods have been suggested and used to solve the issues and lessen the dangers connected with cloud security. Here are some examples.

Encryption and Key Management: Encrypting data at rest and in transit helps protect against unauthorized access. Proper key management solutions are crucial to maintaining the security of encryption mechanisms [19].

Identity and Access Management (IAM): Robust IAM solutions are essential for managing user identities, roles, and permissions. Implementing the principle of least privilege helps minimize potential risks [20].

Virtualization Security: Properly securing the virtualization layer is essential to prevent attacks that target vulnerabilities in the hypervisor or virtual machine instances [16].

Cloud-specific Security Tools: Utilizing cloud-native security tools can enhance threat detection and response within the cloud environment. Tools like AWS GuardDuty and Azure Security Center offer real-time monitoring.

Security Monitoring and Incident Reaction: The use of comprehensive security monitoring technologies and methodologies enables the identification and timely reaction to security issues. Continuous monitoring, log analysis, and threat intelligence are all critical in detecting and mitigating security breaches [9].

Standards and Certifications for Cloud Security: Industry-recognized security standards and certifications provide a framework for analyzing and assuring the security of cloud services. ISO 27001, CSA STAR, and FedRAMP standards assist organizations in evaluating the security capabilities of CSPs [10]. Regular security assessments and audits assist organizations in identifying vulnerabilities and ensuring compliance with security regulations. A proactive security strategy includes independent audits, penetration testing, and vulnerability scanning [12]. Implementing safe setups for cloud services as well as hardening the underlying infrastructure to mitigate possible vulnerabilities [8,21].

While there are some gaps identified in the previous literature. The requirement for a thorough knowledge of the increasing threats and dangers connected with cloud systems is one of the gaps in cloud security research. New attack vectors and vulnerabilities develop as the cloud ecosystem constantly advances, necessitating continual study to keep ahead of possible dangers [18]. Cloud security suffers from a lack of consistent standards and legal frameworks. This creates difficulties in maintaining compliance and good security across various cloud service providers (CSPs) and organizations. It is necessary to do research in order to establish standardized frameworks that satisfy security and compliance needs [22]. A fundamental shortcoming in cloud systems is the absence of transparency and auditing capabilities. Organizations frequently have limited insight into CSP-implemented security measures, which can impede effective monitoring and incident response activities [9]. The cloud computing shared responsibility paradigm raises concerns regarding accountability and culpability in the event of a security incident or data loss. Establishing legal frameworks for accountability and determining the level of obligation between customers and CSPs is an ongoing difficulty. Effective threat intelligence is crucial for proactive security measures. However, there is a gap in the availability of comprehensive threat intelligence specific to cloud environments. Research is needed to enhance threat intelligence mechanisms tailored to cloud-based threats [23,24].

A research study paper is essential in the field of research since it serves numerous objectives and helps the growth of knowledge and understanding in a certain area. Table 2 is an explanation of the importance of this study paper and how it can contribute to the area.

Table 2. Importance and Contribution to cloud computing.

Importance	Contribution to Field
Practical Guidance	The implementation guide offers practical advice and recommendations for organizations wishing to efficiently adopt cloud security frameworks. It provides step-by-step instructions, best practices, and real-world examples to assist organizations in navigating the intricacies of cloud security.
Bridging the Gap Between Theory and Practice	While research on cloud security frameworks exists, there is frequently a gap between theoretical understanding and actual application. This gap is filled by the implementation guide, which translates theoretical principles into tangible procedures and tactics that organizations can easily use for their cloud security projects.
Cloud security is a critical concern	The research paper will offer advice on how to create cloud security frameworks, covering frequent difficulties and best practices. This will assist organizations in improving their knowledge and use of cloud security measures.
Comprehensive Analysis of Cloud Security Problems	The research paper provides a thorough examination of the numerous security issues that exist in cloud computing. It finds and categorizes typical issues including misconfigurations, poor identity and access management, data security concerns, shared infrastructure hazards, and so on. This report gives a good overview of the unique problems that organizations face when it comes to safeguarding their cloud installations.
Proposal of Effective Solutions	The study reports not only highlight cloud security challenges but also suggest potential remedies to these difficulties. It recommends realistic and effective security solutions, best practices, and technology breakthroughs that may be used to improve cloud security. Secure configuration practices, strong identity and access management, data encryption approaches, increased isolation and virtualization security, and continuous monitoring and incident response procedures are among the solutions offered.

3. Cloud Security Frameworks

The growing use of cloud computing in recent years has altered the way businesses handle and store data. The cloud has various advantages, including scalability, cost-effectiveness, and flexibility. However, with the growing reliance on cloud services, implementing adequate security measures is critical. Cloud security frameworks help organizations define and implement security policies that are particular to their cloud environments [25,26]. They provide advice on risk assessment, selecting and implementing security measures, security monitoring, incident response planning, and continuing security improvement. Table 3 introduce to different type of frameworks available in the market.

Table 3. Introduction to Frameworks.

Frameworks	Description
COBIT 5 for Cloud Computing	The COBIT framework is extended to solve unique cloud computing concerns.
NIST	Provides standards and best practices for cloud computing security and privacy issues.
ISO 27017	Code of practice for information security measures for cloud services based on ISO/IEC 27002.
FedRAMP	A federal program in the United States provides a standardized method for cloud security evaluation and authorization.
AWS Well-Architected Framework	Best practices and guidelines for creating and running safe and efficient cloud infrastructures are provided.
CSA STAR	A registry that details the security practices of cloud service providers using the CSA's Cloud Control Matrix.
ENISA Cloud Security Guide	Addresses several security topics while providing information on analyzing and reducing threats in cloud settings.
CIS Controls for Cloud	Based on the CIS Controls, tailored security controls and practices for safeguarding cloud environments.
Cloud Controls Matrix (CCM)	Provides a set of cloud-specific security measures that are compliant with industry standards and legislation.
CSA Security Guidance	Describes thorough security best practices and controls for various cloud service architectures and deployments.

1. COBIT 5 for Cloud Computing:

COBIT 5 for Cloud Computing offers a governance and management framework that aligns IT activities with strategic business goals. It emphasizes the importance of risk management, performance measurement, and process improvement in the cloud context. This framework provides guidance for defining roles, responsibilities, and controls necessary to ensure secure cloud adoption while ensuring business objectives are met.

2. NIST SP800-144:

NIST SP800-144 is a specialized publication that focuses on cloud security and provides an in-depth understanding of cloud-specific threats, vulnerabilities, and risks. It offers a comprehensive overview of security issues relevant to cloud services and outlines practical guidelines and recommendations for mitigating these risks. This framework is widely respected and referenced across the cybersecurity landscape.

3. ISO 27017:

ISO 27017 is an international standard that specifically addresses cloud security controls. It provides guidance on implementing effective security measures for cloud services, covering areas such as data classification, encryption, access management, and incident response. This standard ensures that cloud service providers and users have a common set of security controls to build upon.

4. FedRAMP:

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government initiative that standardizes the security assessment and authorization process for cloud services. It focuses on ensuring cloud services used by government agencies meet stringent security requirements. FedRAMP compliance demonstrates a high level of security readiness for cloud services targeting government clients.

5. AWS Well-Architected Framework:

The AWS Well-Architected Framework offers a structured approach for designing secure and optimized infrastructure on Amazon Web Services (AWS). It encompasses five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization. By following this framework, organizations can ensure that their cloud architectures are aligned with best practices for security and performance.

6. CSA STAR:

The Cloud Security Alliance Security Trust Assurance and Risk (STAR) program provides a comprehensive framework for evaluating the security posture of cloud service providers. It offers a detailed questionnaire that assesses security controls, compliance, and overall risk management. Organizations can use CSA STAR to assess and compare various cloud providers before making informed decisions.

7. ENISA Cloud Security Guide:

The ENISA Cloud Security Guide offers practical advice for enhancing cloud security. It covers a wide range of cloud security topics, including risk assessment, governance, compliance, and incident response. This guide is valuable for organizations seeking comprehensive insights into cloud security considerations.

8. CIS Controls for Cloud:

The Center for Internet Security (CIS) Controls for Cloud provides a set of best practices for securing cloud environments. It focuses on critical security actions that organizations should implement to protect cloud resources. These controls cover areas such as identity management, data protection, and vulnerability management.

9. Cloud Controls Matrix (CCM):

The Cloud Controls Matrix (CCM) by Cloud Security Alliance offers a comprehensive framework for assessing the security posture of cloud services. It maps security controls to various industry standards and regulations, providing a detailed reference for evaluating cloud provider security.

10. CSA Security Guidance:

The Cloud Security Alliance (CSA) Security Guidance offers a set of best practices and recommendations for securing cloud environments. It covers a wide array of cloud security topics, including governance, risk management, compliance, and encryption. This guidance is valuable for organizations seeking to build a robust security foundation in the cloud.

These frameworks are used to improve security by both cloud service providers and cloud clients. Cloud security frameworks are widely recognized and used across a wide range of sectors. Organizations use these frameworks to analyze cloud providers' security postures, review their own security procedures, and create confidence with customers and stakeholders. Compliance with well-known frameworks contributes to the development of a common language and knowledge of cloud security standards. This chapter gives an overview of the cloud security framework, its implementation process, and the importance of putting one in place.

The frameworks we will focus on are:

1. COBIT 5 (Control and Assurance in Cloud: Using COBIT5)
2. NIST (National Institute of Standards and Technology)
3. ISO 27017 (International Organization of Standardization)
4. CSA STAR (Cloud Security Alliance Security, Trust, and Assurance Registry)
5. AWS Well-Architected Framework

These five frameworks cover a range of perspectives, from offering a structured approach to aligning IT with business goals (COBIT5) then comprehensive cloud security considerations (NIST SP800-144) to specific security controls (ISO 27017)and practical implementations (AWS Well-Architected Framework and CSA STAR). Also a short comparision of these 5 frameworks with their focus, scope, and approach are in the Table 4.

3.1. *COBIT 5 for Cloud Security*

ISACA (Information Systems Audit and Control Association) developed COBIT 5 is a worldwide recognized methodology for enterprise IT governance and management [27]. While COBIT 5 is not created expressly for cloud security, it does present a complete set of principles and practices that can be used to successfully regulate and safeguard cloud computing systems [28]. It provides governance, risk management, and control objectives that allow organizations to successfully manage and secure cloud services.

3.1.1. Principles

Here is the understable definition of each principles of the Figure 2.

Separating Governance from Management: Define and separate the roles of cloud security governance (strategic decision-making and supervision) and management (day-to-day operational tasks).

Meeting stakeholder needs: Align cloud security activities with the needs and expectations of stakeholders such as consumers, regulators, and business partners.

End-to-end Enterprise Coverage: Adopt a comprehensive approach to IT governance and management that includes all parts of the business. This principle emphasizes the need to consider the full IT value chain, from strategy development and execution through value delivery, resource management, and risk management.

Applying a single integrated framework: Use a consistent framework for cloud security management that corresponds with existing governance and management frameworks and standards, such as ISO 27001 or the NIST Cybersecurity Framework.

Enabling a holistic approach: Adopt a comprehensive and integrated approach to cloud security that includes people, procedures, and technology. Take into account all relevant factors, including legal, regulatory, and contractual requirements.

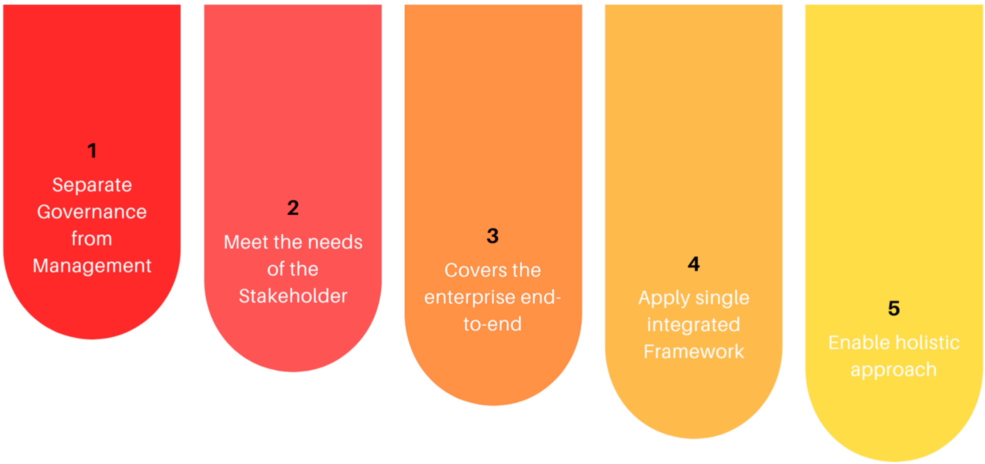
1
Separate Governance from Management
2
Meet the needs of the Stakeholder
3
Covers the enterprise end-to-end
4
Apply single integrated Framework
5
Enable holistic approach

Figure 2. COBIT5 Principles.

Table 4. Comparison of Frameworks.

	Focus	Scope	Approach
COBIT 5	COBIT5 is a comprehensive framework that provides direction for enterprise IT governance and management, including security measures.	It addresses a wide range of IT disciplines, such as security, risk management, and compliance.	COBIT5 focuses on governance, risk management, and compliance (GRC) procedures and emphasizes connecting IT with business objectives.
NIST SP 800-144	NIST SP 800-144 addresses security and privacy problems in public cloud computing systems particularly.	It gives guidance for organizations using cloud computing and focuses on risk management, security measures, and data privacy.	NIST SP 800-144 takes a risk-based approach and addresses particular security and privacy concerns for cloud installations.
ISO 27017	ISO 27017 is a standard that focuses on implementing information security measures for cloud services especially.	It addresses security issues such as data protection, access restrictions, incident management, and regulatory compliance for both cloud service providers and cloud users.	ISO 27017 adopts a risk-management approach to cloud security and provides a set of controls and recommended.
CSA STAR	CSA STAR is a program that allows cloud service companies to show their security practices and consumer openness.	It focuses on evaluating cloud service providers' security, privacy, and risk management skills.	CSA STAR presents a set of control goals and criteria for assessing cloud service providers' security posture, allowing consumers to make educated decisions regarding their cloud services.
AWS well-architected	The Amazon Web Services (AWS) Well-Architected Framework is particular to AWS and provides assistance for developing, implementing, and running safe and efficient cloud systems.	It discusses different areas of cloud architecture, such as security, dependability, performance, cost optimization, and operational excellence.	Security, dependability, performance efficiency, cost optimization, and operational excellence are the framework's five pillars. It outlines best and design guidelines for each of the pillars.

3.1.2. Strengths

1. Holistic Approach: COBIT 5 provides a comprehensive approach to cloud control and assurance, encompassing topics like governance, risk management, control goals, and performance assessment. It provides a complete framework for managing cloud security in a methodical and integrated manner.
2. Risk Focus: COBIT 5 emphasizes a risk-oriented approach to cloud control and assurance. It assists businesses in identifying, assessing, and prioritizing risks connected

with cloud services, data security, and regulatory compliance. This helps organizations to properly allocate resources and prioritize risk reduction activities.

3. Alignment with Industry Standards, Frameworks, and Laws: COBIT 5 is aligned with industry standards, frameworks, and laws, allowing organizations to satisfy compliance needs. It advises on how to apply best practices from standards such as ISO 27001, the NIST Cybersecurity Framework, and GDPR. This alignment makes it easier to implement a uniform and effective control and assurance program.
4. Control Objectives: COBIT 5 provides a set of specified control goals targeted to cloud settings. Access management, data protection, incident response, and vendor management are among the important control objectives addressed. They serve as realistic guidance for building cloud security policies.
5. Continual Improvement: COBIT 5 encourages a culture of continuous development in cloud control and assurance. It promotes businesses to evaluate their control system, measure performance, and identify opportunities for improvement. This iterative strategy assists organizations in adapting to changing cloud security concerns and continuously improving their control environment.

3.1.3. Limitations

1. Complexity: To implement COBIT 5 for cloud control and assurance, a complete grasp of the framework and its components is required. It can be difficult, particularly for organizations with few resources or technical knowledge. Adequate training and assistance may be required to properly capitalize on the benefits of COBIT 5.
2. Customization Issues: COBIT 5 provides a broad framework that must be customized to an organization's individual needs and cloud environment. Customizing the framework to meet specific needs and cloud service providers may necessitate more effort and skill.
3. Tools Dependency: COBIT 5 gives guidelines on control and assurance operations but does not advocate specific tools or technology. Organizations must rely on outside sources or expertise to choose and deploy appropriate cloud control and assurance systems.
4. Dynamic Cloud Environment: Cloud environments are ever-changing and dynamic. COBIT 5 may need to be updated and adjusted on a regular basis to accommodate new technology, emerging risks, and changing regulatory requirements. Organizations must stay current in order to keep their control and assurance practices relevant.

3.1.4. COBIT 5 Process for Securing Cloud Infrastructure

COBIT 5, the most recent version of the COBIT framework, provides management recommendations for cloud environments to guarantee successful IT governance and administration. Below are some significant COBIT 5 management standards relating to cloud computing. And Table 5 illustrates the tools needed to use this framework.

1. Define and Align IT Goals: Clearly identify IT goals and match them with the wider business objectives of the organization. Understanding the potential advantages and dangers of cloud adoption, as well as aligning cloud plans with business goals, are all part of this process.
2. Assess Cloud Readiness: Conduct a complete assessment of the organization's technical, operational, and security skills to determine its preparedness to utilize cloud services. This evaluation should take into account considerations such as data sensitivity, regulatory requirements, and business continuity.
3. Establish Cloud Governance: Put in place a solid governance structure to assist cloud decision-making. This involves developing rules and processes, defining roles and duties, and assuring compliance with relevant laws, regulations, and standards.
4. Vendor Selection and Management: Develop a systematic strategy for selecting cloud service providers (CSPs) based on stated criteria such as security measures, service dependability, and compliance capabilities. Contracts and service level agreements

(SLAs) that explicitly explain expectations, duties, and performance indicators should be established.

5. Risk Management: Risk management includes identifying and assessing the hazards connected with cloud adoption, as well as developing risk mitigation techniques. This involves examining security procedures, determining the dependability and availability of cloud services, and dealing with data privacy and confidentiality problems.
6. Data Management: Establish data management practices to assure the confidentiality, integrity, and availability of cloud-stored data. Data classification, encryption, backup and recovery procedures, and adherence to data protection requirements are all part of this.
7. Incident Response and Forensics: Create cloud-specific incident response strategies, including methods for identifying and reacting to security problems. When creating investigative methods, keep in mind the particular problems of cloud forensics, such as data dispersion, shared resources, and multi-tenancy.
8. Performance Measurement: Define and monitor key performance indicators (KPIs) to assess the efficacy and efficiency of cloud services. Assess and report on the performance and value supplied by cloud services on a regular basis to ensure they fulfill business needs.
9. Continuous Improvement: Implement a continuous improvement process for cloud services, including regular reviews and assessments to identify areas for enhancement. Continuously monitor emerging cloud technologies, industry trends, and regulatory changes to ensure ongoing alignment with best.

Table 5. Tools for COBIT5.

Process	Tools and Technique
Define Objectives and Scope	Document management tools (e.g., Microsoft Word, Google Docs)
Assess the Current State	Risk assessment tools (e.g., Qualys, Nessus)
Define Governance Framework	GRC (Governance, Risk, and Compliance) platforms (e.g., RSA Archer, MetricStream)
Identify Risk	Risk assessment tools and methodologies (e.g., FAIR, OCTAVE)
Define Control Objectives	COBIT 5 framework documentation and guidance materials
Design Security Controls	Cloud security management platforms (e.g., AWS Security Hub, Azure Security Center)
Implement Security Controls	Cloud-native security services (e.g., AWS IAM, Azure AD)
Monitor and Measure	Security information and event management (SIEM) tools (e.g., Splunk, IBM QRadar)
Perform Audits and Reviews	Audit management tools (e.g., ACL, TeamMate)
Continual Improvement	IT service management (ITSM) tools (e.g., ServiceNow, Jira Service Management)

3.2. NIST SP 800-144

The National Institute of Standards and Technology (NIST) has created a framework to help businesses defend their cloud infrastructure. This framework offers a complete collection of concepts, rules, and best for cloud-based environment security. Organizations may improve the security of their cloud infrastructure and efficiently manage risks by adopting the NIST methodology [29,30]. However, it is critical to recognize both the NIST framework's strengths and limits. However, the parent framework of NIST SP 800-144 consists of five core functions [31].

Identify: Understanding the organization's systems, assets, data, and capabilities is part of this role. It entails identifying and recording the resources that must be safeguarded, as well as the hazards connected with them. This role serves as the foundation for creating successful cybersecurity policies and procedures.

Protect: The Protect function is responsible for putting protections in place to assure the delivery of key services and the security of data. Access control, data encryption, training and awareness programs, and adopting security measures to reduce identified risks are all part of it.

Detect: The Detect function is responsible for designing and deploying tools to quickly identify cybersecurity occurrences. It contains methods for continuous monitoring, anomaly detection, and incident response to detect and respond to cybersecurity events in real-time.

Respond: The Respond function is responsible for developing and implementing a response strategy to reduce the effects of cybersecurity events. It includes creating an incident response strategy, doing incident analysis, and taking the necessary steps to contain and recover from cybersecurity problems.

Recover: The Recover function's goal is to restore services and capabilities that have been impacted by cybersecurity events while also preventing future occurrences. It comprises tasks such as system recovery, stakeholder communication, and using lessons gained to enhance future incident response.

3.2.1. NIST's Advantages in Cloud Infrastructure Security

1. Comprehensive and Proven: In the cybersecurity field, the NIST framework is well-recognized and accepted. It provides a complete and organized approach to cloud security, including risk assessment, security controls, incident response, and continuous monitoring. Based on industry input and evolving security concerns, the framework is constantly updated and optimized.
2. Flexibility and adaptability: The NIST framework is intended to be adaptable to various organizations and cloud settings. It allows organizations to adjust security controls and to their individual demands and regulatory requirements. This adaptability enables organizations to build security measures tailored to their own cloud architecture and business activities.
3. Vendor-neutral perspective: NIST SP 800-144 is vendor-neutral, concentrating on the basic security and privacy principles that organizations should consider while adopting public cloud services. This enables organizations to use the recommendations independently of the cloud service provider they select, increasing flexibility and adaptability.
4. Practical advice: The paper provides practical advice and the best for safeguarding public cloud systems. It offers practical advice on setting security controls, analyzing cloud service provider's security capabilities, and meeting compliance requirements. This assists organizations in translating advice into actionable steps to improve cloud security.

3.2.2. NIST's Limitations in Protecting Cloud Infrastructure

1. Rapidly emerging Threat Landscape: Threats and weaknesses to cloud security are continually emerging. Although routinely updated, the NIST framework may not always keep up with developing risks. To successfully manage the shifting threat landscape, organizations should augment the NIST framework with continuous monitoring, threat information, and industry-specific security.
2. NIST SP 800-144 has limited coverage of foreign standards and regulations since it is primarily aimed at US government organizations and may not handle international standards and regulations completely. Organizations having worldwide operations or those operating in many countries may need to consider extra regulatory frameworks and norms particular to their geographical location.

3.2.3. NIST Best Practice

NIST Special Publication 800-144 outlines security and privacy principles for public cloud computing. Here are several NIST 800-144 best for protecting a cloud-based environment each steps given in Figure 3:

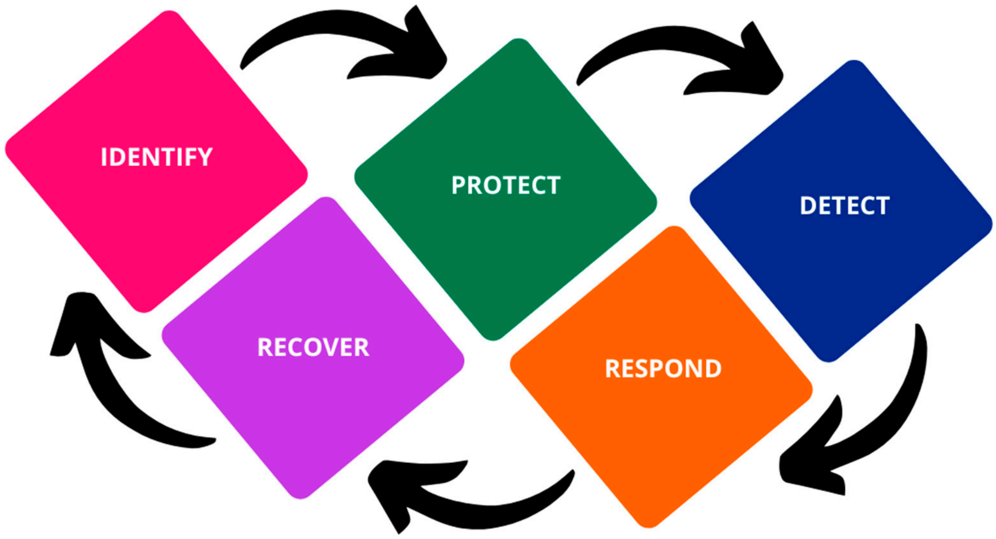

Figure 3. NIST Core Functions.

1. Understand the Cloud Environment: Gain a thorough awareness of the cloud environment, including the types of cloud services utilized (e.g., Software as a Service, Platform as a Service, and Infrastructure as a Service) and the security and privacy issues that come with them.
2. Security and Privacy standards: Determine and record your organization's security and privacy standards. Data sensitivity, compliance needs, legal concerns, and other industry-specific standards are all part of this.
3. Selection and Evaluation of Cloud Service Providers (CSP): Examine possible CSPs' security capabilities and practices. Consider the CSP's security certifications, incident response methods, data encryption systems, and adherence to relevant standards.
4. Data Protection: Put in place suitable safeguards to secure data in the cloud. This involves encrypting sensitive data at rest and in transit, imposing least privilege access rules, and putting in place data backup and recovery methods.
5. Implement robust identity and access management (IAM) controls to guarantee that only authorized personnel have access to cloud resources. To efficiently manage user rights, employ multi-factor authentication, strong password rules, and role-based access controls (RBAC).
6. Secure Configuration Management: Securely configure cloud resources by adhering to industry best practices and CSP standards. Review and update setups on a regular basis to meet emerging threats and vulnerabilities.
7. Continuous Monitoring and Logging: Implement strong monitoring and logging methods in the cloud environment to follow activities and detect security occurrences. To discover possible risks and abnormalities, monitor system logs, network traffic, and user actions.
8. Incident Response and Recovery: Create and implement a cloud-specific incident response plan. Create protocols for identifying, reacting to, and recovering from security events. To ensure the plan's efficacy, test and update it on a regular basis.
9. Compliance and Governance: Ensure that appropriate legislation, standards, and contractual commitments are followed. To manage cloud security, create a governance structure that includes roles and duties, policies, and processes.

10. Security Awareness and Training: Provide ongoing security awareness and training to educate employees about cloud security risks and best. Foster a culture of security awareness and accountability within the organization.

Each phase of the NIST architecture for securing cloud infrastructure necessitates the use of a variety of tools and technologies. Here, are some regularly used tools that might help with each step. Table 6 gives information about tools required to implement NIST framework

Table 6. Tools for NIST.

Process	Tools and Techniques
Understand the cloud deployment models and service models	Cloud Service Provider assessment tools: CAIQ, CCM
Prioritize security and privacy requirements	Risk assessment tools: Nessus, Qualys and for framework: NIST Risk Management Framework, FAIR
Protect data in transit and at rest	Encryption tools: SSL/TLS protocol
Implement strong identity and access management controls	Identity and access management (IAM) solutions (e.g., Okta, Azure Active Directory, AWS IAM)
Security controls implementation	Network Security Tools: IDPS, Wireshark Secure configuration management tools: Chef, Ansible
Continuous Monitoring and Logging	Security information and event management (SIEM) systems (e.g., Splunk, Elastic SIEM) Log management and analysis tools (e.g., LogRhythm, Graylog) Threat intelligence platforms (e.g., ThreatConnect, Recorded Future)
Incident Response and Recovery	Incident Response tools: IBM Resilient, Service Now, EnCase, Volatility
Compliance and Governance	RSA Archer, MetricStream
Personnel training and education:	Security awareness training: KnowBe4, SANS Simulation tools: Cofense, Gophis

3.3. *ISO 27017:2015*

ISO 27017 was created as part of the ISO 27000 series to address the particular security problems associated with cloud computing. It is based on the larger ISO 27001 standard, which specifies the criteria for implementing an information security management system (ISMS). ISO 27017 tailors these criteria explicitly for cloud service providers and clients, giving additional guidelines and controls to improve cloud security. ISO/IEC 27017 provides guidelines for information security controls relevant to the use of cloud services by giving further implementation instructions for the 37 controls listed in ISO/IEC 27002 as well as seven additional cloud-related controls (As shown in Figure 4) that address the following.

3.3.1. Security Controls for Cloud

ISO 27017 specifies a set of security rules that organizations may use to safeguard their information assets in a cloud computing environment. These rules are intended to handle the specific risks and problems that cloud services present. ISO 27017 specifies the following important security controls in Table 7:

Table 7. Controls of ISO/IEC.

Controls	Description
Asset Management Controls:	Asset inventory: Keep track of all cloud-based assets, including data, apps, systems, and infrastructure components. Classification of assets: Classify cloud assets based on their criticality and sensitivity to ensure appropriate security measures are applied.
Access Controls	Identity and access management: Implement controls to manage user identities, authentication, and authorization for accessing cloud resources. Control and monitoring of privileged access to cloud environments to reduce the danger of unauthorised acts.
Cryptographic Controls	Encryption: Use encryption technologies to safeguard data at rest and in transit in the cloud. Key management: Establish proper key management processes to ensure the secure generation, storage, and destruction of encryption keys.
Incident Management Controls	Incident response planning: Create and implement a cloud incident response plan that outlines roles, responsibilities, and processes for dealing with security events. Logging and monitoring: Implement logging and monitoring mechanisms to detect and respond to security events and potential breaches within the cloud environment.
Supplier Management Controls	Supplier evaluation: Evaluate and choose cloud service providers (CSPs) based on their security capabilities and compliance with recognised security standards. Contractual agreements: In contracts with CSPs, define specific security standards and duties, such as data protection, incident reporting, and compliance obligations.
Compliance Controls	Legal and regulatory compliance: Ensure that all applicable laws, regulations, and contractual duties for information security and data protection in the cloud are met. Auditing and evaluation: Conduct frequent audits and evaluations to ensure compliance with security measures and standards.
Data Protection Controls	Implement procedures to ensure the logical and physical separation of client data within the cloud environment. Establish data backup and recovery mechanisms to prevent data loss or destruction within the cloud environment.

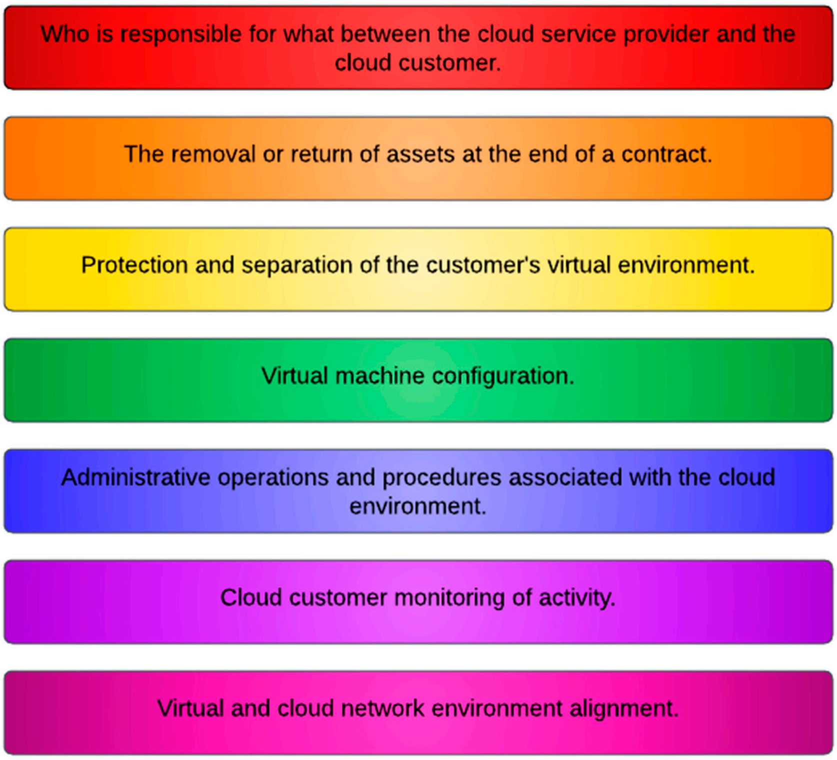
Who is responsible for what between the cloud service provider and the cloud customer.
The removal or return of assets at the end of a contract.
Protection and separation of the customer's virtual environment.
Virtual machine configuration.
Administrative operations and procedures associated with the cloud environment.
Cloud customer monitoring of activity.
Virtual and cloud network environment alignment.

Figure 4. Standards of ISO/IEC 27017.

3.3.2. Benefits

ISO/IEC 27017 can help enterprises in [32]:

1. Within the Cloud computing environment, they must safeguard their information assets.
2. Comply with all applicable laws and regulations.
3. Reduce the likelihood of data security problems.
4. Reduce the need for redundant controls to save money.

3.3.3. Required Steps to Implement

To implement ISO 27017 in your organization, you would normally take the following steps:

1. Acquaint yourself with the Standard: Obtain a copy of ISO 27017 and thoroughly read it. Understand the standard's objectives, requirements, and recommendations.
2. Examine Your Present Cloud Environment: Assess your current cloud infrastructure, platforms, and services. Determine how ISO 27017 might assist in addressing possible risks and gaps in security controls.
3. Form a Project Team: Within your organization, form a team that will be in charge of implementing ISO 27017. Stakeholders from IT, security, legal, compliance, and other relevant areas should be included.
4. Conduct a gap analysis to match your present security practices to ISO 27017's standards and recommendations. Determine which areas require improvement or extra controls.
5. Create an Implementation strategy: Develop a thorough strategy including the actions, milestones, and dates for adopting ISO 27017. Determine the risk and criticality of the actions.
6. Implement Security Controls: Follow ISO 27017's specified security controls and procedures. Access controls, encryption, data segregation, incident response protocols, and supplier management are some examples.
7. Provide training and awareness programs to educate staff on the significance of cloud security and their duties under ISO 27017. This ensures that everyone knows their duties in safeguarding information assets in the cloud.
8. Documentation and Policies: Create and maintain documentation that proves ISO 27017 compliance. Policies, processes, risk assessments, incident response plans, and records of security occurrences and their resolution may be included.
9. Regular evaluation and Improvement: Monitor and evaluate your cloud security on a regular basis to guarantee continuing compliance with ISO 27017. Conduct audits, risk assessments, and evaluations on a regular basis to identify areas for improvement and execute necessary adjustments.
10. Third-Party Evaluation: Consider hiring a third-party auditor or consultant to evaluate your cloud security practices in relation to ISO 27017. They may conduct an impartial assessment of your compliance and make recommendations for improvement.

To efficiently implement and manage ISO 27017 in organizations, a variety of tools and resources are available. The following are some necessary tools for implementing ISO 27017:

ISO 27017 is an addition to ISO 27001, which offers the overarching foundation for developing an Information Security Management System (ISMS). Understand the larger context and standards within which ISO 27017 functions by being acquainted with the ISO 27001 standard.

ISO 27017 Standard Document: Obtain a copy of the ISO 27017 standard. This paper specifies the standards, rules, and principles for safeguarding data in cloud computing systems. It is used as a reference to guarantee that the ISO 27017 requirements are followed.

Tools for Risk Assessment: Risk assessment is a critical component of the ISO 27017 application. Various risk assessment techniques and frameworks can help in detecting and analyzing hazards in cloud computing systems. The NIST Risk Management Framework (RMF) or industry-specific risk assessment methodology are two examples.

Tools for Evaluating Cloud Service Providers (CSPs): It is critical to analyze CSP security capabilities and adherence to ISO 27017 criteria when selecting and assessing CSPs. Cloud security evaluation questionnaires and vendor security assessment frameworks, for example, can help in assessing and comparing CSPs based on their security controls and practices.

Cloud Security Monitoring and Management Tools: Putting in place effective security controls and monitoring in a cloud environment frequently necessitates the use of specialized tools. These technologies aid in the monitoring of cloud infrastructure, the detection of security issues, the management of access restrictions, and the enforcement of security rules. Cloud security platforms, security information and event management (SIEM) systems, and identity and access management (IAM) solutions are some examples.

Documentation and Policy Templates: Using templates and frameworks will help you develop the relevant documentation and policies in accordance with ISO 27017. These materials may be used to develop an information security policy, risk assessment reports, incident response plans, and other necessary documentation. Templates are accessible from a variety of sources, including industry groups, consultancies, and information security organizations.

Training and awareness programs can help educate workers and stakeholders about ISO 27017 and its standards. These can include e-learning courses, workshops, and awareness campaigns targeted to certain organizational roles and responsibilities.

Audit and Compliance Tools: Tools that aid in performing internal audits, monitoring ISO 27017 compliance, and tracking remedial actions can be beneficial in maintaining an effective ISMS. These systems can automate audit operations, create compliance reports, and streamline nonconformity and corrective action management.

3.4. Cloud Security Alliance (STAR)

The Cloud Security Alliance (CSA) created the CSA STAR (Security, Trust, and Assurance Registry) architecture to address the requirement for transparency and assurance in cloud service provider (CSP) security. It offers a collection of best guidelines for identifying and managing the security risks associated with cloud services [33].

Cloud Security: The framework focuses on safeguarding cloud-based systems and data from unauthorized access, data breaches, and other security risks.

Trust: It is critical to establish trust between cloud service providers and cloud clients. The framework's goal is to increase openness, accountability, and trust in the cloud environment.

Assurance: Providing proof and validation of security controls and practices is what assurance is all about. The framework encourages third-party audits and certifications to improve cloud security assurance.

3.4.1. Strengths

1. Standardized Assessment: The CSA STAR framework provides a standardized way to evaluate CSP security posture. It offers a standardized set of control objectives and criteria that organizations may use to evaluate and compare various cloud service providers.
2. Transparency and accountability: The framework encourages CSPs to give thorough information about their security, data handling methods, and regulatory compliance. Customers may thus make educated judgments when purchasing and using cloud services.
3. Third-Party Certification: The CSA STAR program provides a certification mechanism for CSPs to certify compliance with the CSA's security principles and best. This accreditation gives clients peace of mind about the security of their selected cloud services.

4. Collaboration among Industry Experts: The CSA STAR framework is developed through collaboration among industry experts, ensuring that it contains a diverse variety of viewpoints and experiences. This contributes to the development of a comprehensive and strong framework for addressing numerous security risks in cloud computing.

3.4.2. Limitations

1. Reliance on Self-Assessment: The CSA STAR methodology is based on self-assessment by cloud service providers. While CSPs are urged to submit accurate and full information, the framework makes no guarantees regarding the quality or completeness of the information given. Customers must use caution and check the promises provided by CSPs.
2. Developing Technology Coverage Is Limited: The CSA STAR framework may not adequately address the security problems associated with developing technologies or niche cloud services. As technology advances, new security issues that are not expressly addressed in the framework may emerge.
3. Lack of Enforcement: CSPs' compliance with the CSA STAR framework is entirely voluntary. Although the framework promotes openness and best, it lacks legal or regulatory enforcement measures. Organizations must evaluate the credibility of a CSP's promises and adopt extra security measures depending on their unique needs.

3.4.3. How an Organization Can Use the Framework?

To implement the CSA STAR (Security, Trust, and Assurance Registry) framework for cloud security in your organization, follow these steps:

4. Become acquainted with the CSA STAR Program: Understand the CSA STAR structure, its aims, and the certification criteria. To obtain a thorough grasp of the program, go over the CSA STAR materials, including the STAR Certification Control Objectives and Criteria.
5. Determine Who Your Cloud Service Providers (CSPs) Are: Determine which cloud service providers (CSPs) your organization is presently utilizing or contemplating for cloud services. Examine their security practices, certifications, and openness about their security procedures.
6. Perform Due Diligence: Perform due diligence on CSPs by seeking information on their security, certifications, independent audit reports, and any other relevant paperwork. Examine their security disclosures for completeness and correctness.
7. Implement Risk Mitigation Measures: Identify any risks or vulnerabilities connected with the identified CSPs based on the evaluations. Implement risk-mitigation strategies such as extra security controls, data encryption, access controls, or legally binding security promises.
8. Establish Contractual Agreements: Contractual agreements should be negotiated and established with CSPs to explicitly outline security expectations, duties, and compliance requirements. Ensure that the contract addresses issues such as data protection, incident response, service-level agreements (SLAs), and regulatory compliance.
9. Monitor and Review: Continuously monitor and review the performance and security posture of your CSPs. Conduct frequent evaluations and audits to ensure compliance with the CSA STAR framework and the efficacy of the security measures in place.
10. Stay Updated with CSA STAR Program: Keep up to date with the CSA STAR Program: Keep up to speed with CSA STAR program updates and adjustments. Review the most recent CSA STAR documentation, control goals, and criteria on a regular basis to ensure continued alignment and compliance with the framework.

Tools required to implement each step of framework is given in Table 8.

Table 8. Tools for CSA STAR.

Process	Tools and Techniques
Understand CSA STAR	CSA STAR Certification Guidelines document, CSA STAR Self-Assessment Tool.
Choose CSPs	CSA STAR Registry to identify certified CSPs, and vendor assessment tools (e.g., security questionnaires, third-party risk assessment platforms).
Perform Due Diligence	Vendor risk management tools, and document management systems.
Implement Risk Mitigation Measures	Risk assessment tools (e.g., risk assessment frameworks, risk assessment questionnaires), compliance management tools (e.g., GRC platforms).
Establish Contractual Agreements	Cloud security frameworks (e.g., CSA CCM, NIST SP 800-53), contract management tools.
Monitor and Review	Security information and event management (SIEM) tools, log management tools, and compliance management tools.

3.5. AWS Well-Architected Framework

AWS Well-Architected is an Amazon Web Services (AWS) framework that provides architectural best practices and guidelines for creating and maintaining cloud-based applications. It outlines the fundamental ideas and best practices for developing safe, high-performing, robust, and efficient systems on AWS. The Six pillars of the Well-Architected Framework are shown in Figure 5.

Figure 5. Six Pillars of AWS (Source: Tutorials Dojo).

3.5.1. Pillars

Security: Security is concerned with the safeguarding of information, systems, and assets through secure design and execution.

Reliability: Ensures that systems can recover from faults, scale automatically, and mitigate interruptions.

Performance efficiency: Performance efficiency is concerned with optimizing resource utilization in order to improve system performance while lowering expenses.

Operational Excellence: Operational Excellence is concerned with the effective operation and management of systems in order to deliver corporate value.

Cost Optimization: Cost optimization seeks to reduce expenses over the system's lifespan while preserving required performance and functionality.

Sustainability: The sustainability discipline considers your company's long-term environmental, economic, and societal effects.

3.5.2. Advantages

1. The following are some of the advantages of adopting the AWS Well-Architected Framework:
2. Best Practices: The framework includes a collection of tried-and-true best practices for creating, deploying, and running AWS applications. Following these best practices

will help you enhance your system's overall architecture, security, dependability, performance, and cost-efficiency.

3. Mitigation of Risks: The framework assists in identifying possible risks and vulnerabilities in your architecture. By tackling these risks early on, you may improve your systems' security, compliance, and resilience, minimizing the possibility of security breaches, downtime, or performance difficulties.
4. Cost Optimization: By implementing the Cost Optimization pillar, you will be able to analyze and optimize your AWS resource utilization and expenses. This assists in identifying possibilities to cut needless spending, remove inefficient resources, and enhance overall cost efficiency, potentially saving money.
5. The Performance Efficiency pillar is concerned with optimizing the performance of your applications. You may increase the responsiveness, scalability, and performance of your systems by using best practices such as auto-scaling, caching, and efficient data storage.
6. The framework emphasizes operational efficiency, allowing organizations to optimize their procedures and workflows. You may improve system dependability, streamline processes, and save manual work by integrating automation, monitoring, and effective incident response systems.
7. Scalability and Flexibility: By following the guidelines of the framework, you may build your applications to be highly scalable and adaptable, allowing them to handle variable workloads and adapt to changing business requirements. This allows you to adapt to market needs fast and grow your systems as needed.
8. AWS Service Alignment: The Well-Architected Framework is compatible with a variety of AWS services, features, and technologies. You may use the framework to construct powerful, scalable, and cost-effective solutions by using AWS's vast spectrum of services.

3.5.3. Limitations

1. While AWS Well-Architected has many advantages, it also has several restrictions and drawbacks that should be considered:
2. Adoption of the Well-Architected Framework may include a learning curve for teams who are unfamiliar with AWS or cloud architecture. To successfully comprehend and use the best, training and upskilling are required.
3. Overemphasis on AWS Services: The Well-Architected Framework strongly encourages the usage of AWS services, which may result in vendor lock-in. Organizations may grow unduly reliant on AWS-specific services, making migration to alternative cloud providers difficult if necessary.
4. Assessing Complexity: Performing Well-Architected reviews and evaluations can take a long time and a lot of resources. It necessitates data collection and analysis, architectural evaluations, and change implementation, which may be a big endeavor for organizations.

3.5.4. Deployment Guide

Follow these major steps to deploy the AWS Well-Architected Framework:

1. Get to Know Framework: Understand the Well-Architected Framework's five pillars: operational excellence, security, dependability, performance efficiency, and cost optimization. Discover the best practices related to each pillar.
2. Evaluate Your Architecture: Compare your current or planned architecture to the Well-Architected Framework. Determine areas for improvement and associated dangers. For a first assessment, use AWS's Well-Architected Tool.
3. Set clear goals and priorities for your architecture based on the evaluation results and business needs. Choose your priority inside each pillar to concentrate on.

4. Design for Well-Architected: Align your architecture with the Well-Architected Framework. Consider the AWS best practices and recommendations for each pillar. Address any risks or deficiencies that have been discovered.
5. Create an Action Plan: Make a thorough action plan outlining the measures needed to close the identified gaps. Define tasks, assign responsibilities, and establish timetables for achieving improvements.
6. Test and validate: Perform extensive testing to check that the introduced modifications have remedied the highlighted issues and that the workload is functioning as intended. Validate the architecture's performance, security, and dependability.
7. Review and Improve: Review your architecture on a regular basis to ensure that it adheres to the Well-Architected Framework. Formal Well-Architected Reviews should be conducted with AWS Solution Architects or authorized partners to obtain professional perspectives and recommendations for future enhancements.
8. Foster a Culture of Best Practices: Within your organization, foster a culture of best practices and architectural excellence. Educate and train your teams on the Well-Architected Framework's concepts and urge them to use them in their everyday work.

Several tools are available to help you adopt the AWS Well-Architected Framework. Here are some examples of widely used tools:

The official AWS Well-Architected Tool provides a thorough framework for examining and grading workloads against Well-Architected best practices. It employs a questionnaire-based technique, creates reports, and makes suggestions for enhancement.

AWS Trusted Advisor is an AWS service that gives automatic advice for optimizing your AWS infrastructure. It analyses your AWS infrastructure and makes suggestions based on the Well-Architected Framework to help detect possible security, performance, and cost optimization concerns.

AWS CloudFormation is an Infrastructure as Code (IaC) solution that lets you create and provision AWS services using a declarative template. It aids in the consistent and repeatable deployment of infrastructure, allowing you to execute Well-Architected best practices in a controlled and automated way.

AWS Config is a service that gives a full inventory of your AWS resources and records configuration changes over time. By regularly monitoring and reviewing the configuration of your resources, it may assist in verifying that your infrastructure complies with the Well-Architected principles.

AWS CloudWatch: CloudWatch is an observability and monitoring service that gathers and records metrics, logs, and events from your AWS services. It may be used to monitor the performance and availability of your applications and infrastructure, allowing you to spot possible problems and verify that the Well-Architected principles are followed.

AWS Cost Explorer: A cost management tool that allows you to analyze and visualize your AWS spending. It analyses your consumption patterns, discovers cost-saving options, and helps you optimize your infrastructure expenses in accordance with the Well-Architected cost optimization pillar.

Finally, the cloud security framework gives a thorough overview and analysis of several cloud security frameworks, models, and best practices. The purpose of this section was to investigate the present state of cloud security and to emphasize the significance of adopting robust security mechanisms in cloud systems.

4. Cloud Security Challenges and Proposed Solutions

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort and or service provider interaction", According to the National Institute of Standards and Technology (NIST), cloud computing is a fast emerging technology. Many individuals utilize cloud computing unconsciously in their daily lives through services such as Microsoft Office 365, Gmail, and Dropbox. Adopting cloud computing has several benefits, including anytime-anywhere accessibility, increased geographic coverage, lower infrastructure investment, and more [34]. There are, however, security risks involved with cloud computing. These risks can jeopardize the security of cloud-stored data, programs, and infrastructure. With organizations increasingly utilizing cloud services, it is critical to recognize and manage these threats in order to protect the confidentiality, integrity, and availability of cloud resources. The diagram below depicts some frequent cloud security issues. The given Figure 6 describes some common cloud security problems [35–37] and Table 9 describe the effects on cloud & affected cloud services.

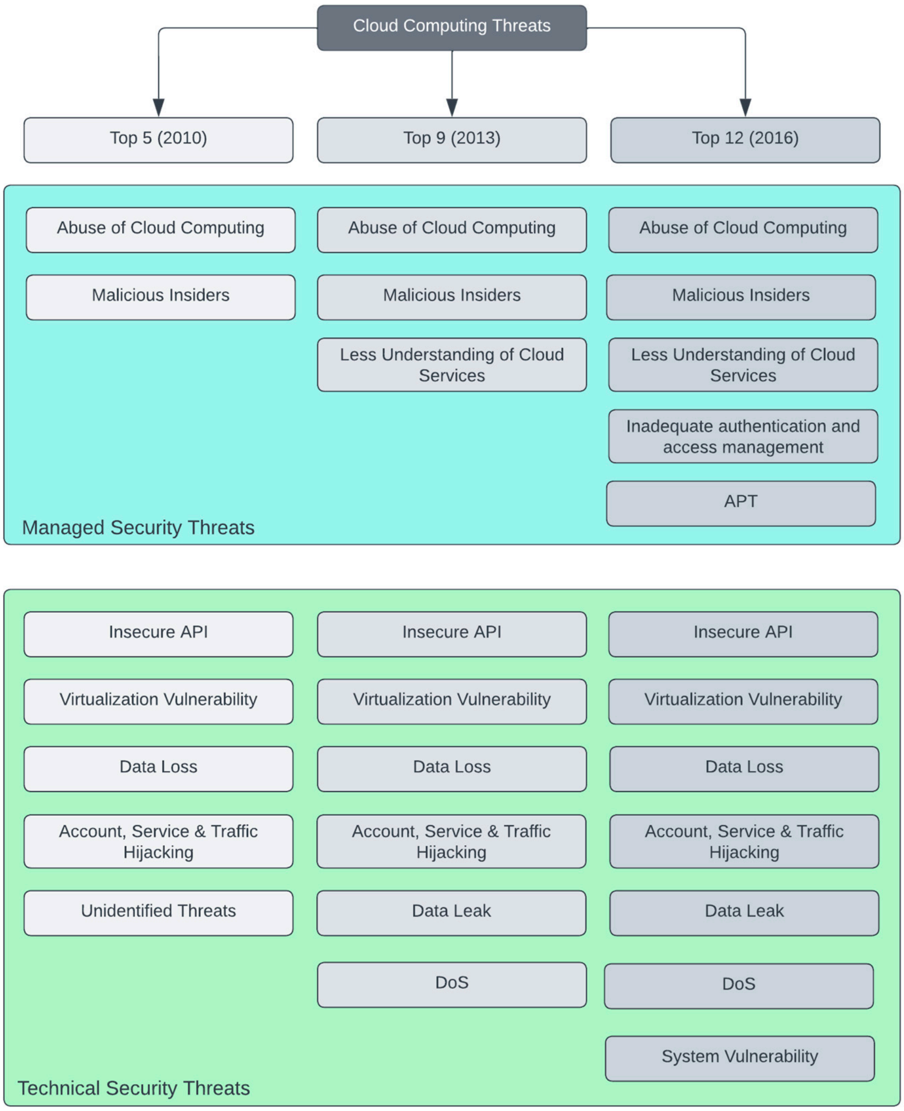

Figure 6. Top Cloud Security threats.

4.1. Managed Security Threats

4.1.1. Abuse of Cloud Computing

Criminals employ cloud computing to target victims and misappropriate cloud services. They conduct DDoS assaults, phishing, email spam, and Bitcoin mining. Breaching a user's cloud infrastructure can have serious ramifications for businesses. As a result, it is critical for businesses to monitor cloud access and apply risk mitigation measures. In the event of cloud service misuse, disaster recovery and data loss prevention techniques are critical to the recovery process. Cloud computing abuse can take various forms, including [38,39]:

- Unauthorized Access
- Data Breaches
- Resource misuse
- Cryptocurrency mining
- Spamming and phishing

Solution:

Use rigorous authentication measures such as multi-factor authentication (MFA) to ensure that only authorized users may access cloud services. Review and adjust user access rights depending on their positions and responsibilities on a regular basis.

Monitor and analyze user activities: Use security monitoring technologies to detect any unusual or suspicious activity in the cloud environment. Use log management and analysis software to track and investigate any suspected misuse or unauthorized access.

Encrypt sensitive data: Encrypt data in transit and at rest using encryption methods. Encrypt critical data before storing it in the cloud, and make sure the cloud and users have safe communication routes.

Table 9. Comparative Study of Cloud security problems.

Threats	Affected Cloud Services	Effects	Solutions
Abuse of Cloud Computing	PaaS and IaaS	Validation Loss, Service Fraud, Strong attacks due to unidentified sign-up	Network analysis, Robust registration and multifactor authentication
Insecure API	PaaS, SaaS, IaaS	Improper authentication and authorization, the wrong transmission of Content	Data Encryption, Strong access control and multi-factor authentication
Malicious Insider	PaaS, SaaS and IaaS	Assets damage, productivity loss and confidentiality break	Duty Segregation, IAM policies
Data Loss	PaaS, SaaS and IaaS	Removal, modification and stealing of confidential and personal data	Disaster, backup and recovery management
Service and Account hijacking	PaaS, SaaS and IaaS	Breaching into critical areas of cloud and server, access of root account	Adoption of strong authentication, and security policies.

4.1.2. Malicious Insider

Malicious insider threats in cloud computing relate to the hazards posed by persons who have authorized access to cloud resources but purposefully abuse their rights for malevolent objectives. Employees, contractors, or service providers having lawful access to the cloud environment may be among these insiders. Here are some important features of hostile insider attacks in cloud computing [39,40]:

- Data theft or leakage
- Unauthorized Access
- Sabotage or data manipulation

Malicious Insider Threat Prevention and Mitigation:

Implement strict access restrictions, least privilege principles, and strong identity and access management (IAM) policies. Review and adjust user access credentials based on job positions and responsibilities on a regular basis.

Implement robust monitoring and auditing systems to track user activity, system events, and data access. To detect suspicious behavior, use real-time alerting and anomaly detection technologies.

Duty segregation: Enforce duty segregation to guarantee that no single employee has disproportionate control or privileges. Separation of roles decreases the possibility of collaboration and aids in the prevention of unauthorized acts.

4.2. Technical Security Threat

4.2.1. Insecure API

In cloud computing, secure API threats relate to vulnerabilities and dangers associated with Application Programming Interfaces (APIs) used to communicate with cloud services. APIs serve as a link between distinct software components, allowing for communication and data sharing. Here are a few examples of prevalent insecure API risks in cloud computing [24,39,41].

- Unauthorized access and authentication bypass
- Injection attacks
- Insecure Data Transmission

Mitigating API Insecurity:

Implement strong authentication and authorization systems, such as strong passwords, multi-factor authentication (MFA), or token-based authentication. To guarantee that only authorized users have access to certain API functions and resources, employ fine-grained authorization rules.

API monitoring and logging: Put in place strong monitoring and logging systems to record and analyze API activity. Examine API logs for unusual or suspicious activity that might signal a security breach or unauthorized access attempt.

4.2.2. Virtualization Vulnerabilities

The risks and vulnerabilities associated with the virtualization layer that enables the construction and administration of virtual machines (VMs) in cloud settings are referred to as virtualization vulnerability threats in cloud computing. Attackers can use these vulnerabilities to compromise the virtualization infrastructure, obtain unauthorized access to VMs, or conduct malicious operations. The following are some of the most frequent virtualization security risks in cloud computing [42]:

- Vulnerabilities in the Hypervisor
- DoS attacks

Threats to Virtualization Vulnerability Mitigation:

Patching and updates on a regular basis: Keep the hypervisor software, virtual machines, and other virtualization components up to date with the most recent security patches and upgrades to address known vulnerabilities.

Strong VM isolation: Ensure strong VM isolation by establishing virtual networks, access restrictions, and resource allocation correctly. To prevent unauthorized access between VMs, use security methods like network segmentation, VLANs, and virtual firewalls.

Vulnerability scanning and assessment: Perform frequent vulnerability scans and assessments of the virtualization infrastructure, including the hypervisor and virtual machines (VMs), to discover and resolve any security flaws. Resolve detected vulnerabilities as soon as possible.

Implement correct VM lifecycle management practices to guarantee that VMs are safely generated, provisioned, and retired. To reduce the attack surface, assess and eliminate unused or superfluous VMs on a regular basis.

4.2.3. Data Loss

The possibility of permanent or unintentional loss of data stored in the cloud is referred to as the data loss threat in cloud computing. While cloud services provide numerous data redundancy and backup systems, there are still circumstances that might cause data loss. The following are some of the most typical reasons for data loss in cloud computing [39,43]:

- Failures in hardware or infrastructure
- Accidental deletion or human error
- Malicious Activity

Mitigating Data Loss Risks:

Data backup and recovery: Implement frequent and automatic data backup processes to provide redundancy and multiple copies of vital data. Periodically test data restoration techniques to ensure backups are functional [44]:

Redundant storage and replication: Use cloud services that provide data replication across several geographic locations or availability zones. This helps to defend against data loss caused by infrastructure failures or localized occurrences.

Prepare a detailed disaster recovery strategy that specifies ways to recover data in the case of hardware failures, natural catastrophes, or other catastrophic occurrences. The rehabilitation strategy should be tested and validated on a regular basis.

4.2.4. Account, Service, and Traffic High-Jacking

Threats to accounts, services, traffic, and hijacking are major security problems in cloud computing settings. Cloud account hijacking is the process by which an attacker steals or hijacks a person's or organization's cloud account. Cloud account hijacking is a typical identity theft strategy in which the attacker utilizes stolen account details to undertake harmful or unauthorized behavior. When a cloud account is hijacked, an attacker often impersonates the account owner by using a hacked email account or other credentials [45,46]. Here is a rundown of each danger category, as well as potential mitigating strategies: [47].

Account: Account dangers include unauthorized access to cloud user accounts and the compromising of user credentials. Mitigation strategies include: To improve the security of user accounts, implement robust authentication systems such as multi-factor authentication (MFA).

Enforce safe password rules, such as utilizing complicated passwords and updating them on a frequent basis.

Service Threats: Service threats are vulnerabilities or assaults that target cloud services. Mitigation strategies include Patch and upgrading cloud services on a regular basis to address known vulnerabilities.

Implement strong network and application-level firewalls to prevent unauthorized access to services. Monitor and detect any unusual activity using intrusion detection and prevention systems (IDPS) [48].

Traffic: Interception, manipulation, or interruption of network traffic inside cloud systems are examples of traffic risks. Mitigation strategies include:

Encrypt network communications using secure communication protocols such as HTTPS or Transport Layer Security (TLS).

DNSSEC (DNS Security Extensions) should be implemented to secure the integrity and authenticity of DNS answers and to prevent DNS hijacking [49].

Use network segmentation and access restrictions to limit traffic flow and mitigate the effect of any possible breach [50]. What are the risk of the discussed cloud security problems on infrastructure has been discussed in Table 10.

Table 10. Risk Level.

Problem	Risk Level
Abuse of Cloud Computing	Medium
Malicious Insider	Medium
Insecure API	High
Virtualization Vulnerabilities	High
Account, Service and traffic hijacking	High

5. Conclusions

Finally, several major results and consequences have emerged as a result of intensive study, analysis, and review. We looked at popular cloud security frameworks including the NIST Cloud Security Framework, the CSA STAR, ISO/IEC 27017, COBIT5 and AWS

Well-architected framework throughout the chapter. These frameworks give useful guidelines and controls for protecting cloud computing systems, addressing critical security concerns, and maintaining data and resource confidentiality, integrity, and availability. The investigation indicated that there are several frameworks available to meet the particular issues involved with protecting cloud systems in terms of cloud security frameworks. Each framework has its own set of characteristics, strengths, and shortcomings. When several frameworks are compared and contrasted, it becomes clear that no single framework can fully fulfill all criteria for any cloud deployment because every framework has disadvantages and limitations. To choose the best framework or mix of frameworks, organizations must carefully examine their unique demands, compliance requirements, and risk tolerance. Furthermore, the research effort provided light on typical challenges and weaknesses in cloud security. Data breaches, unauthorized access, unsecured APIs, insider risks, and insufficient security measures are examples of these. These problems highlight the crucial importance of strong security, extensive risk assessments, and constant monitoring and enhancement of cloud infrastructures. Cloud security issues offer substantial concerns for organizations that use cloud computing services. These issues, however, may be efficiently managed with proactive steps and solid security systems. Data breaches, unprotected APIs, cloud computing abuse, and hostile insider threats are just a few of the major cloud security issues. Organizations should focus on adopting solutions such as tight access restrictions, encryption of sensitive data, frequent security assessments, monitoring and analysis of user actions, and robust authentication systems such as multi-factor authentication to address these issues. Furthermore, educating users on cloud security risks and recommending and utilizing third-party security services can all help to improve cloud security.

Author Contributions: Methodology, M.C., S.S.; Formal analysis, M.C.; Investigation, M.C.; Resources M.C., S.S.; Writing—review & editing, M.C., S.S.; Visualization, M.C., S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: Special Thanks to: Hasmukhlal, Kailasben, Darpen, Sita Ma & Rushika, pals: Aayush, Divyang, Mitul, Karan, Chetav, Sooraj, Sagar Mal sen, Prateek Kumawat.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rayaprolu, A. How-Many-Companies-Use-Cloud-Computing/#gref, Techjury, February 2023. Available online: https://techjury.net/blog (accessed on 2 April 2023).
2. Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A. Cloud computing—The business perspective. *Decis. Support Syst.* **2011**, *51*, 176–189.
3. Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T. Cloud Computing—A Classification, Business Models, and Research Directions. *Bus. Inf. Syst. Eng.* **2009**, *1*, 391–399.
4. Bhushan, K.; Gupta, B.B. Security challenges in cloud computing: State-of-art. *Int. J. Big Data Intell.* **2017**, *4*, 81–107.
5. Di Giulio, C.; Sprabery, R.; Kamhoua, C.; Kwiat, K.; Campbell, R.H.; Bashir, M.N. *Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?* IEEE: Honolulu, HI, USA, 2017.
6. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58.
7. Gartner. *Cloud-Strategy*; Gartner: Stamford, CT, USA, 2020. Available online: https://www.gartner.com/en/information-technology/insights/cloud-strategy (accessed on 4 April 2023).
8. Amara, N.; Huang, Z.; Awais, A. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. In Proceedings of the 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, China, 12–14 October 2017.
9. Mohanan, S.; Sridhar, N.; Bhatia, S. Comparative Analysis of Various Cloud Security Frameworks. In Proceedings of the 6th International Congress on Information and Communication Technology, London, UK, 25–26 February 2019.
10. Popa, D.; Cremene, M.; Borda, M.; Boudaoud, K. A security framework for mobile cloud applications. In Proceedings of the 11th RoEduNet International Conference, Sinaia, Romania, 17–19 January 2013.

11. Ukil, A.; Jana, D.; Das, A. A Security Framework in Cloud Computing Infrastructure. *Int. J. Netw. Secur. Its Appl.* **2013**, *5*, 11–24. [CrossRef]
12. Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **2013**, *4*, 1–13. [CrossRef]
13. Grobauer, B.; Walloschek, T.; Stocker, E. *Understanding Cloud Computing Vulnerabilities*; IEEE: Piscataway, NJ, USA, 2011.
14. Rodero-Merino, L.; Vaquero, L.M.; Caron, E.; Muresan, A.; Desprez, F. Building Safe PaaS Clouds: A Survey on Security in Multitenant Software Platforms. *Comput. Secur.* **2012**, *31*, 96–108.
15. Tsochev, G.R.; Trifonov, R.I. Cloud computing security requirements: A Review. *IOP Conf. Ser. Mater. Sci. Eng.* **2022**, *1216*, 012001.
16. Ristenpart, T.; Tromer, E.; Shacham, H.; Savage, S. Hey you get off of my cloud: Exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
17. European Commission. MEMO_12_713. *European Commission*. 27 September 2012. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ (accessed on 4 April 2023).
18. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11.
19. Kamara, S.; Lauter, K. Cryptographic Cloud Storage. In *Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6054, pp. 136–149.
20. Sonam Sudha, M.A. Identity and Access Management in Cloud. *J. Res. Appl. Sci.* **2014**, 7.
21. Neves Calheiros, R.; Ranjan, R.; Beloglazov, A.; De Rose, C.A.; Buyya, R. CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Softw. Pract. Exp.* **2011**, *41*, 23–50.
22. You, P.; Peng, Y.; Liu, W.; Xue, S. Security Issues and Solutions in Cloud Computing. In Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012.
23. Chang, V.; Ramachandran, M. Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Trans. Serv. Comput.* **2016**, *9*, 246–258.
24. Khan, M.A. A survey of security issues for cloud computing. *J. Netw. Comput. Appl.* **2016**, *71*, 11–29.
25. Youssef, A.; Alageel, M. A Framework for Secure Cloud Computing. *Int. J. Comput. Sci. Issues* **2012**, *9*.
26. Patel, V. A framework for secure and decentralized sharing of medical imaging data. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef]
27. ISACA. *Security Considerations for Cloud Computing*; ISACA: Schaumburg, IL, USA, 2012.
28. OIlloh, O.; Aghili, S.; Butakov, S. Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates. In Proceedings of the 12th International Conference on Services Oriented Computing 2014, Paris, France, 3–6 November 2014.
29. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing (NIST Special Publication 800-145)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
30. Jansen, W.; Grance, T. *Guidelines on Security and Privacy in Public Cloud Computing*; NIST: Gaithersburg, MD, USA, 2011.
31. NIST. *NIST US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft)*; NIST: Gaithersburg, MD, USA, 2011.
32. i.governance. ISO-27017 and ISO-27018. Available online: https://www.itgovernance.co.uk/iso-27017-and-iso-27018 (accessed on 4 April 2023).
33. CSA. *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*; CSA: Toronto, ON, Canada, 2011.
34. Sharma, R.; Trivedi, R.K. Literature review: Cloud Computing—Security Issues, Solution and Technologies. *Int. J. Eng. Res.* **2014**, *3*, 221–225. [CrossRef]
35. Park, S.-J.; Lee, Y.-J.; Park, W.-H. Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network. *Commun. Secur. Soc.-Oriented Cyber Spaces* **2021**, *2021*, 3686423.
36. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Hangzhou, China, 23–25 March 2012.
37. Rittinghouse, J.W.; Ransome, J.F. *Cloud Computing: Implementation, Management, and Security*; CRC Press: Boca Raton, FL, USA, 2016.
38. Rackwareinc. Preventing-the-Top-9-Threats-in-Cloud-Computing. Rackwareinc. Available online: https://www.rackwareinc.com (accessed on 4 April 2023).
39. Kazim, M.; Zhu, S.Y. A survey on top security threats in cloud computing. *Int. J. Adv. Comput. Sci. Appl.* **2015**, *6*. [CrossRef]
40. Tessian. What-Is-a-Malicious-Insider. *Tessian*. 20 February 2023. Available online: https://www.tessian.com (accessed on 4 April 2023).
41. CSA Top Threats Working Group. Top-Threat-2-to-Cloud-Computing-Insecure-Interfaces-and-Apis. *CSA*. 30 July 2022. Available online: https://cloudsecurityalliance.org/blog/2022/07/30/top-threat-2-to-cloud-computing-insecure-interfaces-and-apis/ (accessed on 4 April 2023).
42. Zhu, G.; Yin, Y.; Cai, R.; Li, K. Detecting Virtualization Specific Vulnerabilities in Cloud Computing Environment. In Proceedings of the IEEE 10th International Conference on Cloud Computing, Honolulu, HI, USA, 25–30 June 2017.
43. Gillis, J. 10-Common-Causes-of-Data-Loss. *Newera*. 31 January 2023. Available online: https://www.neweratech.com/us/blog/10-common-causes-of-data-loss/ (accessed on 4 April 2023).

44. Tissir, N.; El Kafhali, S.; Aboutabit, N. Cybersecurity management in cloud computing: Semantic literature. *J. Reliab. Intell. Environ.* **2020**, *7*, 69–84.
45. Lord, N. What-Cloud-Account-Hijacking. *Digital Gaurdian*. 11 September 2018. Available online: https://www.digitalguardian.com/blog/ (accessed on 4 April 2023).
46. Buyya, R.; Yeo, C.S.; Venugopal, S.; Broberg, J.; Brandic, I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Gener. Comput. Syst.* **2009**, *25*, 599–616.
47. Vaquero, L.M.; Rodero-Merino, L.; Caceres, J.; Lindner, M. A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Comput. Commun. Rev.* **2009**, *35*, 50–55. [CrossRef]
48. Dinh, H.T.; Lee, C.; Niyato, D.; Wang, P. A survey of mobile cloud computing: Architecture, applications, and approaches. *Wirel. Commun. Mob. Comput.* **2013**, *13*, 1587–1611.
49. Ali, M.; Khan, S.U.; Vasilakos, A.V. Security in cloud computing: Opportunities and challenges. *Inf. Sci.* **2015**, *305*, 357–383.
50. Zhang, S.; Zhang, S.; Chen, X.; Huo, X. Cloud computing research and development trend. In Proceedings of the 2010 Second International Conference on Future Networks, Sanya, China, 22–24 January 2010.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.