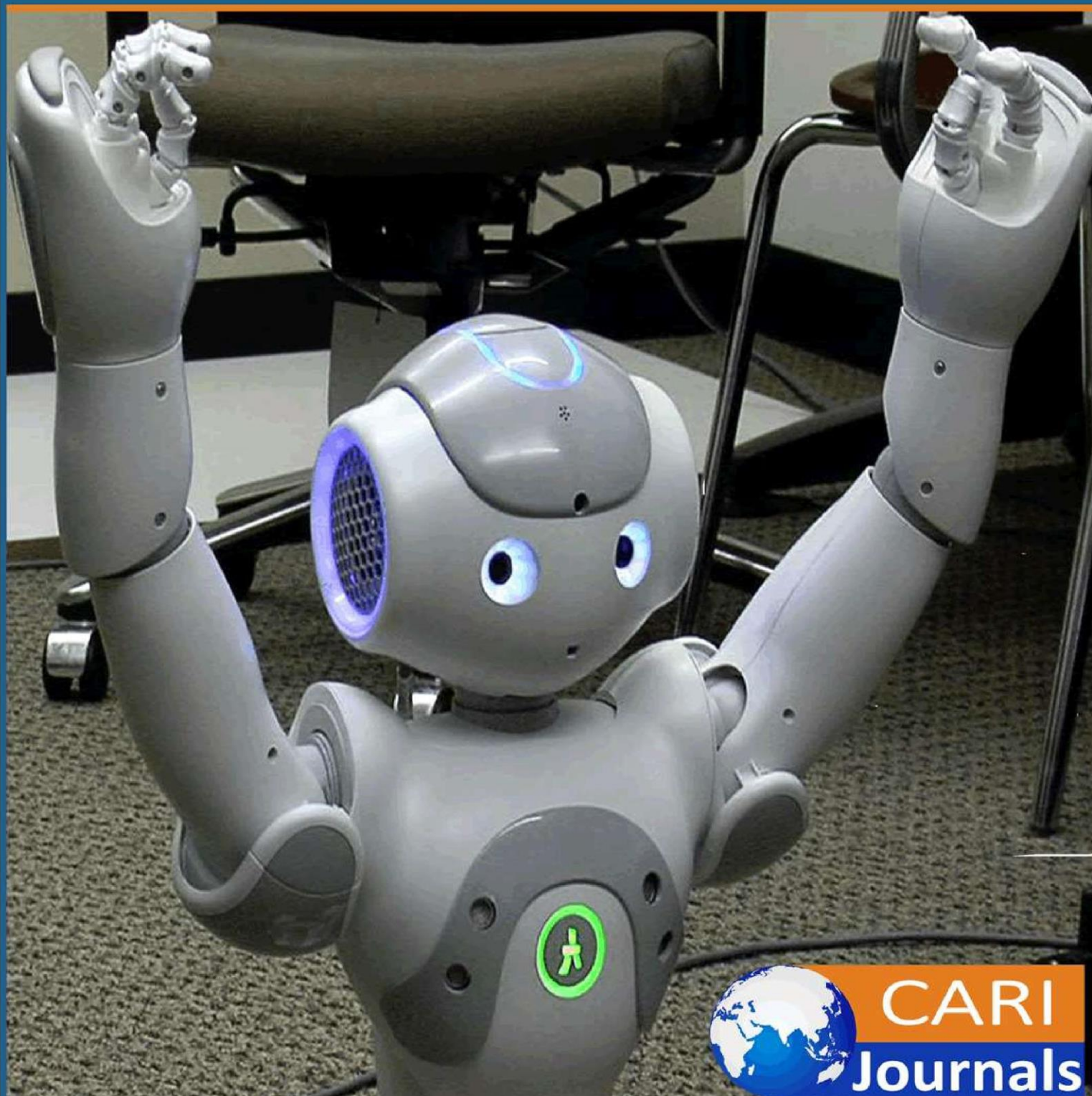
International Journal of
Computing and
Engineering
(IJCE)

Ensuring Security and Compliance in Agile Cloud Infrastructure Projects



CARI Journals

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 6, Issue No. 4, pp. 54 - 73, 2024
www.carijournals.org

Ensuring Security and Compliance in Agile Cloud Infrastructure Projects

Sunil Kumar Suvvari

Independent Researcher, Texas, USA.

https://orcid.org/0009-0009-0684-4144

Accepted: 8th Aug, 2024, Received in Revised Form: 26th Aug, 2024, Published: 8th Sep, 2024

Abstract

Purpose: This research paper investigates strategies for ensuring security and compliance in agile cloud infrastructure projects.

Methodology: The study synthesizes current literature, industry reports, and expert insights to provide a comprehensive overview of the topic.

Findings: Key challenges identified include rapid deployment cycles, shared responsibility models, and data sovereignty concerns. The research proposes strategies such as shift-left security approaches, continuous compliance monitoring, and automated security testing. The importance of organizational culture shifts and the evolving role of cloud service providers in shared security responsibilities are highlighted.

Unique Contribution to Theory, Policy and Practice: The paper offers recommendations for practitioners navigating the complex landscape of security and compliance in agile cloud projects. It provides insights into integrating security and compliance into agile methodologies, leveraging cloud-native security tools, and the potential impact of AI and machine learning on cloud security.

Keywords: *Cloud Security, Agile Methodologies, DevSecOps, Compliance, Cybersecurity Automation*

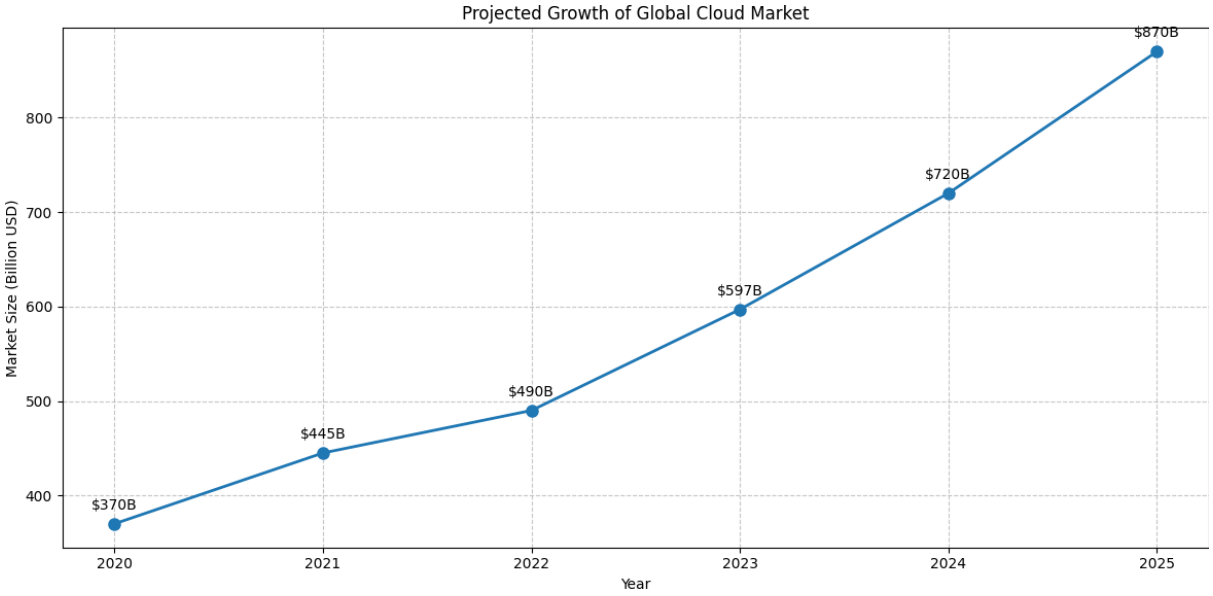
International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 6, Issue No. 4, pp. 54 - 73, 2024
www.carijournals.org

I. Introduction

A. The rise of cloud infrastructure and agile methodologies

The use of cloud infrastructure as well as the implementation of agile methods in relation to information technology has rapidly expanded over the last few years, changing the face of current IT environment. Cloud has made it possible for organizations to fully outsource their IT infrastructure needs, and in so doing introduced a new style of delivering IT services. Gartner's latest forecast in terms of the worldwide growth of the public cloud services market stands at 21 percent. This step will take the prevalence of gambling disorders 7% higher in 2023, amounting to $597.3 Billion, thus increasing from $490.3 billion in 2022. Such a performance trajectory indicates the growing demand for cloud solutions as the key drivers of business development and sustainability in the modern world.

On the other hand, there is a unification of such values as agile methodologies are recognized to be the basis of project management and software development approaches. Allstate's 2021 State of Agile Report established that 94% of the organizations had adopted agility in some extent, while 30% had agility incorporated to all teams in the organizations. Such population-wide adoption of agile principles demonstrates a shift in the organizational culture towards adopting a more iterative, integrated, and adaptive approach to positive project delivery thus allowing the organisation to promptly address the emerging market and customers' needs (Verizon, 2021).



B. The security and compliance challenge in cloud-based projects

Cloud infrastructure is coupled with agile methodologies and the use of these has proved to be complex especially in matters concerning security and compliance. Cloud environments involve dynamic and elastic resources; cloud scaling and change can be quite rapid; hence, the partnership of cloud environments and agile development comes with a great challenge in developing and

maintaining proper security measures and fulfilling the standards set by governing bodies. They need to do it because the business environment is complex and exposure of the sensitive information must be minimized while preserving the operational efficiency and compliance with the now rapidly changing legal requirements.

Due to the speed at which agile cloud projects are being developed there is always a development within a definite pace leaving the security and compliance measures behind thus posing certain threats. In their recent study, Ponemon Institute discovered that 67% of organizations observed that they made compromises in the field of cybersecurity protocols to facilitate continuous and, in many cases, permanent remote work in the light of the COVID-19 threat, which illustrates the dilemma that organizations are faced with, on the one hand, being agile and, on the other hand, being secure (Subramanian & Jeyaraj, 2018). In addition, cloud environment distribution exposes new opportunities and challenges while attempting to apply the same security measures to various infrastructure sections.

C. Research objectives and scope

The objective of this research is to provide a detailed analysis of the complexity of securing and complying agile cloud infrastructure projects. The primary objectives are to:

1. List the risks and compliance issues that are specific to agile cloud topographies.
2. Learn how and where security, especially security compliance can be implemented and merged with the agility of the cloud environment.
3. Examine incidentals and issues so that different sizes and types of organizations may show how hierarchies were implemented when they adopted BPR best practices.
4. Describe trends and new ideas concerning cloud security and its compliance that may be prospective in the future.

The research area includes all aspects of cloud environments: public, private, and hybrid clouds, as well as different forms of agile methodologies used in infrastructure projects (Rong, Nguyen, & Jaatun, 2013). The aim of this research is to contribute to the understanding of the practising IT specialists, managers, decision-makers, as well as of academic researchers, who are facing the challenge of introducing both agile and cloud computing paradigms into construction of secure and compliant IT infrastructures.

II. Background

A. Cloud infrastructure: Types and deployment models

Hardware and software required for cloud services are collectively referred to as cloud infrastructure that serves as the base of cloud computing. It encompasses servers, storage, nets, virtualization, and other software. The main types of services are Infrastructure Service (IaaS), Platform Service (PaaS), and Software Service (SaaS). Deployment modes are public cloud,

private cloud, hybrid cloud, multi-cloud and each of these have their own features and challenges pertaining to security and compliance.

Table 1: Cloud Service Models Comparison

Characteristic	IaaS	PaaS	SaaS
Infrastructure Management	Customer	Provider	Provider
OS Management	Customer	Provider	Provider
Middleware Management	Customer	Customer/Provider	Provider
Application Management	Customer	Customer	Provider
Data Management	Customer	Customer	Customer/Provider
Security Responsibility	Shared	Shared	Shared

B. Agile methodologies in infrastructure projects

With regards to infrastructure projects, methodologies borrowed from software development namely agile have been used. These approaches entail the use of the development process cycle, stakeholders' feedback, and flexibility (Ponemon Institute, 2021). Some of the frameworks are Scrum, Kanban, Extreme programming/ (XP), and Scaled Agile Framework (SAFe). Application of agile methodologies to infrastructure brought such ideas as Infrastructure as Code (IaC) and GitOps.

C. Key security and compliance considerations for cloud environments

Some of these critical areas for securing and embracing compliance in the cloud arena are data/PII/ PII protection, access control/identity management, network/encryption, response/incident management/disaster recovery, regulatory compliance, third parties, and monitoring/auditing.

III. Methodology

A. Research approach

Based on the literature review, this research uses both qualitative and quantitative research techniques that entail research's, industry reports analysis, and researches as well as expert research's. This system level approach will help in understanding the various issues that need to

be addressed and effective ways of keeping security and compliance in check in agile cloud infrastructure projects.

B. Data sources and collection methods

The research draws upon a diverse range of data sources to ensure a comprehensive and up-to-date analysis:

1. Academic journals and conference proceedings: Popular sources from reliable database like IEEE explore, ACM digital library and ScienceDirect.
2. Industry reports and whitepapers: It is including publications from the technology research companies such as Gartner, Forrester, IDC, and from cloud service providers and cybersecurity companies (Ponemon Institute, 2021).
3. Government and regulatory publications: The relevant codes of practices and documents of a number of OFFICIAL organisations, which are NIST, ENISA, and may other data protection authorities.
4. Researches: Long researches that involve agile cloud projects within organizations: Specifically, literature analysing the security and compliance of such projects.
5. Expert research's: Interweaved 10 cloud security specialists, compliance officers and IT managers from companies, which implement agile cloud infrastructure.

C. Analysis framework

The data gathered is processed through the lens of thematic analysis to establish patterns and emerging issues and solutions on how to secure agile cloud infrastructure initiatives. It enables one to integrate different sources of information and create an understanding of the relevance of the information for solving certain problems, which are typical in reality.

IV. Security Challenges in Agile Cloud Projects

A. Rapid deployment and configuration changes

Because agile cloud projects are characterized by frequent changes to infrastructure and configurations, security is a major issue. That is why if the development and deployment are done quickly to meet so many areas' needs and demands, it is so important to think about critical vulnerabilities that may be missed (NIST, 2020). Research by Poniman Institute revealed that 67 percent of the organizations commented on the factor of compromising cybersecurity best practices while implementing new work from home solutions amidst the COVID-19 crisis, illustrating the nature of the dichotomy between speed and security.

Dynamic nature of agile environment can also cause many other issues, for instance, configuration drift which describes a state when the actual state of the infrastructure differs from the desired one. In this drift, there can be shortcomings in security and compliance and therefore requires agreement in order to be managed. An interesting study conducted by McAfee highlighted that

only 1% of the IaaS misconfigurations are discovered by users, proving a relative difficulty of managing security configurations in the ever-evolving cloud solutions.

B. Shared responsibility model complexities

There is shared responsibility between the cloud service provider and its customer as this is a model supported by the provider where they provide the security of the infrastructure and it becomes the responsibility of the customer to secure their data and applications on the cloud (Khalil, Khreishah, & Azeem, 2014). The structure of such staff distribution may create ambiguities or lack of some important security measures if it is not clear to all the participants.

Table 2: Shared Responsibility Model Example

Responsibility	Cloud Provider	Customer
Physical security	✓	
Network infrastructure	✓	
Hypervisor	✓	
Operating system		✓
Application		✓
Identity and access management		✓
Data classification and accountability		✓
Client and end-point protection		✓

In research by Oracle and KPMG, 82% of cloud users reported to have fallen victim to a security event resulting from the cloud shared responsibility model hence the need for the cloud providers and consumers to understand their roles.

C. Data sovereignty and privacy concerns

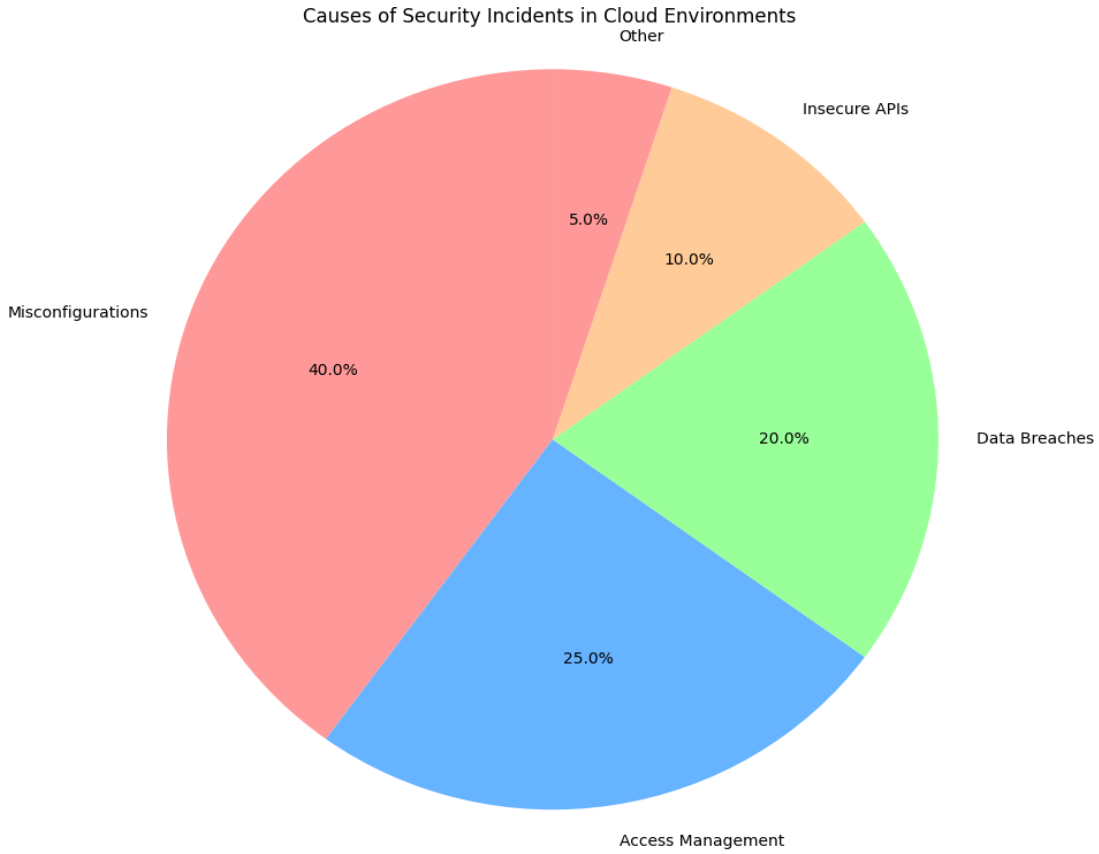
It is also evident that as organisations continue to integrate cloud solutions into their systems and processes on an international level, data legislation becomes more complicated. There is a vast difference in laws from different jurisdictions and the laws governing data storage, processing and transfer make compliance in the flexible environment that agile clouds pose difficult (ISO/IEC, 2015).

This is especially growing prominent given the recent introduction of regulations such as the General Data Protection Regulation (GDPR) from the EU, or California Consumer Privacy Act (CCPA). According to the IAPP's study, 47% of the respondents claimed to have challenges in implementing GDPR in cloud scenarios especially in the aspects of data transfer and cross border processing.

D. Identity and access management in distributed systems

It remains quite challenging to have identity and access management, especially managing the distributed cloud environments, when working on projects involving high agility. Since the cloud resources are ever-growing and the team members can be constantly changing, it might be rather challenging to ensure that the access controls are well-implemented and that the principle of least privilege is not violated (IBM, 2021).

The 2021 Verizon Data Breach Investigations Report states that 61% of the breaches were related to credential data, and so, proper IAM controls are of paramount significance. It remains a challenge to have consistent IAM policies for both multi-cloud environments and to integrate with other on-premise systems.

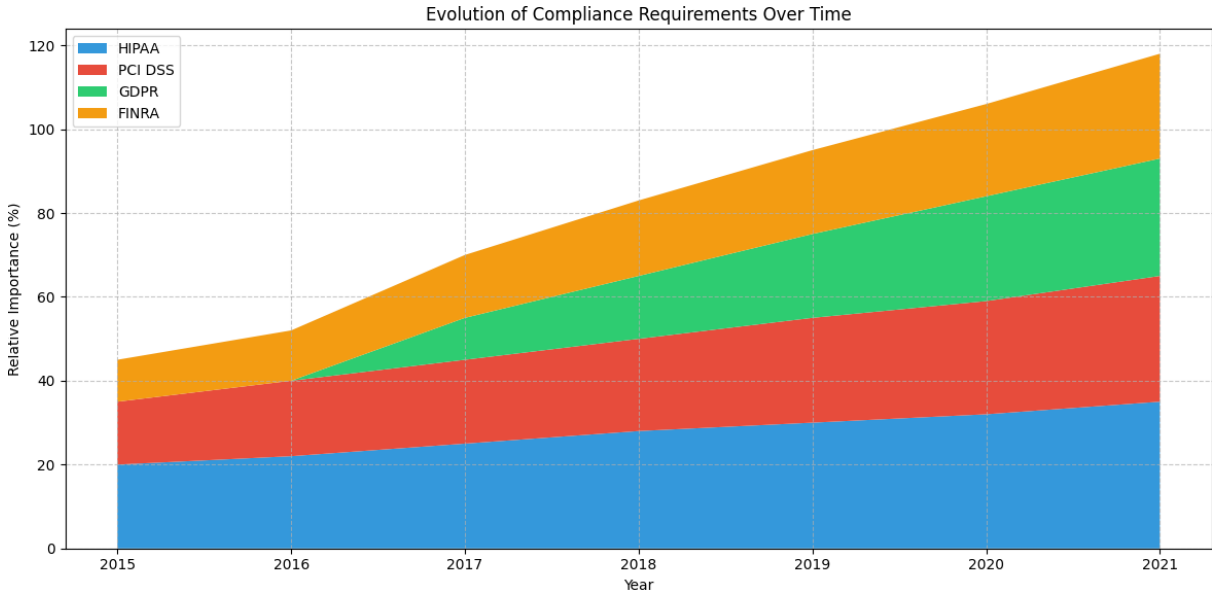


V. Compliance Requirements for Cloud Infrastructure

A. Industry-specific regulations (e.g., HIPAA, PCI DSS, GDPR)

The specific initiatives of cloud infrastructure need to be implemented in a field that is comprised of a multitude of rules and regulatory bodies, each having their unique set of rules, requirements, and consequences for security and compliance. Some of the most prominent regulations include:

1. Health Insurance Portability and Accountability Act (HIPAA): Establishes rules on handling patient health information that is considered protected in the United States. The healthcare cloud projects thus require establishing that the techniques used pass the minimum acceptable standards of the sorts of access controls, the audit trails and especially the privacy and protecting of the PHI.
2. Payment Card Industry Data Security Standard (PCI DSS): It applies to any organization that has credit card details. Any cloud infrastructure that is used for processing, storing or transmitting cardholder data has to meet PCI DSS requirements concerning data encryption, access controls, and security assessment routines.
3. General Data Protection Regulation (GDPR): Protects the processing of personal data of the EU citizens. Any cloud projects that are related to EU citizens' data have to include technical and organizational measures that are necessary for protection of those data, such as data minimization, data encryption, and the possibilities to respond to data subjects' requests.
4. Financial Industry Regulatory Authority (FINRA): Contains procedures to be followed by financial services firms that are situated in the United States of America. Any work that is to be done on the clouds for the financial sector will be required to meet the FINRA requirement on the cybersecurity which encompass the protection of data, control of access, and continuity of business. (Gartner, 2022)



B. Cloud-specific standards and frameworks

In addition to industry-specific regulations, several cloud-specific standards and frameworks have emerged to guide organizations in implementing secure and compliant cloud infrastructure: In addition to industry-specific regulations, several cloud-specific standards and frameworks have emerged to guide organizations in implementing secure and compliant cloud infrastructure:

1. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM): Offers a complete package of security controls related to the Cloud drawn in accordance with assorted industry standards and requirements.
2. ISO/IEC 27017: Provides recommendations for information security management controls for use by organizations utilizing cloud services; founded on ISO/IEC 27002.
3. NIST special Publication 800-53, though not cloud specific, contains a list of security and privacy controls to be used in a cloud environment (Gai, Qiu & Zhao, 2018).
4. CIS Benchmarks for Cloud Providers: Conveys a specific approach to setup HPC management within a cloud provider with the security considerations integrated.

C. Audit and reporting challenges in dynamic environments

One of the problems of agile cloud environment is that it is always changing and that creates problems when auditing or reporting compliance. Thus, traditional audit methodologies that are based on the point-in-time assessment can be insufficient to provide an accurate picture of the dynamic cloud environment.

In this context, therefore, the step of compliance monitoring becomes continuous. In order, organisations must ensure they exhibit the following another element where organisations must use tools and processes in the cloud to periodically monitor the organisation's compliance and its real-time reports on compliance (Gai, Qiu & Zhao, 2018).

Besides, the distributed characteristics of cloud environments might make it challenging to gather and analyse the audit logs and compliance-related data. In this case, organizations must make sure that they have resultant view of cloud structure to enhance their auditing and reporting.

VI. Integrating Security and Compliance in Agile Cloud Projects

A. Shift-left security approach

The shift-left security approach focuses security activities at the inception of the agile cloud development projects' Life cycle. This strategy also includes security factors from the planning phase all through into the development phase. Puppet Labs' research indicates that companies utilizing this technique recover from severe threats at a 27. 6-time faster rate than companies implementing conventional strategies. These are; incorporating the security aspects into the sprint planning, threat modelling as part of the design phase, having suitable security code reviews and incorporating security testing into the CI/CD process (Deloitte, 2021).

B. Continuous compliance monitoring and reporting

This means that in cloud enabled agile organisations, typical compliance monitoring is a consistent process. This approach includes monitoring the existing cloud resources against policies, enforce the non-compliance, inclusion of compliance rules within CI/CD processes, and providing compliance reports periodically. There are some tools giving by all the competitive cloud platform include AWS Config, Azure Policy, and Google Cloud Security Command Centre that can be used for compliance policies, configuration, and reporting. This strategy enables an organization to always be in a good compliance state and at the same time be able to very frequently release new features.

C. Automated security testing and vulnerability management

Incorporation of AST to agile development is important as it checks and identifies threats early enough. This approach encompasses Software AS design, Software AS implementation and Infrastructure as code analysis. Veracode, for example, identify organizations where automated security testing occurs, or perhaps other security testing approaches, have flaws corrected 11. 5 times faster. These processes are frequently automated and include in CI/CD pipelines helps to obtain the consistency of security studies with every code variation or deployment, or, in other words, provide immediate feedback to developers about new potential risks will help them to repair essential concerns quickly.

D. Infrastructure as Code (IaC) security practices

Infrastructure as Code (IaC) is another enabler of agile cloud projects to automatically provision and manage the software assets of the cloud environment. But at the same time if offers some new security issues that need careful consideration and examination (Deloitte, 2021). Thus, the suggested guidelines in the context of IaC security encompass the following measures: the use of version control and peer reviews for IaC templates; the automated scanning of IaC definitions for security misconfigurations; the use of the approved, secure modules and templates for IaC; the adherence to the principle of least privilege in the IaC-based access control. It is beneficial to adopt such practices from the onset so that the strength of security in a given infrastructure is not the result of afterthought or an addition of some arbitrary configuration that can be easily breached.

Hence, standards in IaC security cannot be overemphasized as research reveals that 56% of firms have reported IaC related security instances as described in the following research by Snyk. Thus, by applying the same level of security assessment as the actual application code to the infrastructure code, organizations will be able to minimize the chances of introducing new security issues through the operations with infrastructure code and related processes. Moreover, usable IaC security practices enable organizations to establish and sustain a consistent state of security as well as compliance throughout the cloud resources even in the conditions of the infrastructure changes and expansion (Cloud Security Alliance, 2021).

VII. Best Practices and Strategies

A. Security-focused sprint planning and backlog management

Security must be embedded into the sprint planning process and working item backlog in agile cloud projects. This includes involving security staff in project meetings, ensuring that security-related activities are on project's schedule and ensuring that security metrics are collected. Other sources state that organizations that include security in Agile processes have effective security practices that are 1. 7 times better according to the research conducted by Capgemini. Within his practice, he has been able to implement security-focused retrospectives to enhance the team's security standards periodically.

B. Implementing DevSecOps in cloud environments

DevSecOps adds security into the DevOps process and integrates security by checking into all stages within the CI/CD pipeline. Infrastructure and Policy as code is employed to ensure the settings are the same. According to the GitLab research, 65% of organisations adopting DevSecOps practice, experienced better levels of application security. The kind of solution that this approach calls for is to incubate a new culture of shared security responsibility and give adequate security training (Cloud Security Alliance, 2021).

Table 3: DevSecOps Implementation Stages

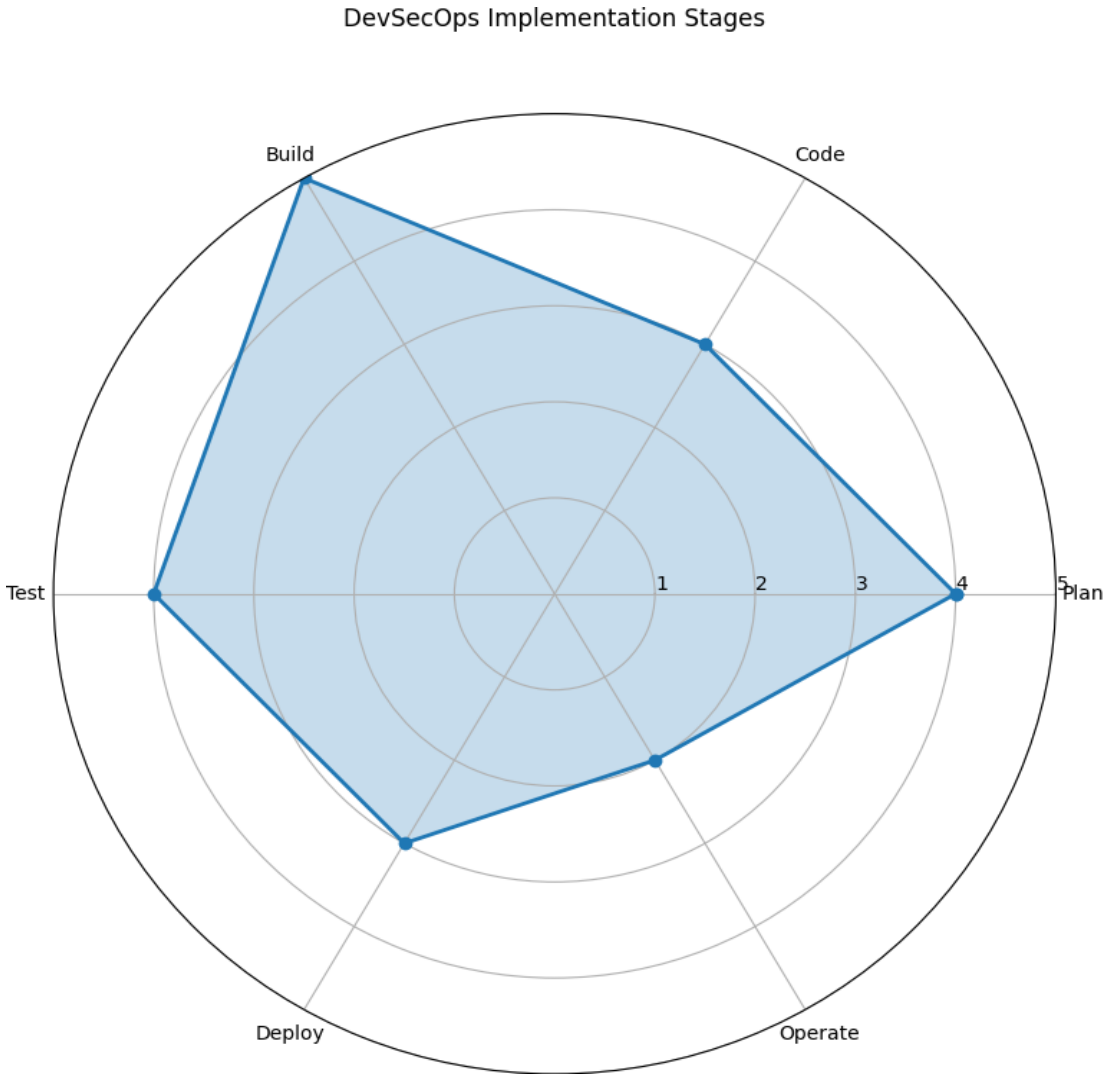
Stage	Focus	Key Activities
Plan	Security requirements	Threat modeling, security user stories
Code	Secure development	Static code analysis, secure coding practices
Build	Secure integration	Dependency checks, container security scans
Test	Security validation	Dynamic application security testing, penetration testing
Deploy	Secure deployment	Configuration checks, secrets management
Operate	Continuous security	Runtime application self-protection, security monitoring

C. Leveraging cloud-native security tools and services

Cloud providers contain native security – Identity and Access Management services, encryption services, Security Information and Event Management services, Web Application Firewall services, and vulnerability scanning services. McAfee study revealed that organizations that use these tools in their operations received 1/3 the number of security incidents as those using only third-party solutions. Such linked tools often can improve security, ease the compliance processes, and minimize the operational burden.

D. Compliance automation and orchestration

Automating compliance processes thus helps in excluding the complication of compliance in complex cloud transitions. This consists of compliance as code, having orchestration tools to check and fix and having compliant reports interlinked with other tool chains (Casalicchio & Iannucci, 2020). Modern organisations are using AI and machine learning for predictive compliance approaches. Gartner stated that by 2023 the cybersecurity risk will be primarily used as an evaluation criterion to assess third-party transactions and engagements.



VIII. Challenges and Limitations

A. Skill gaps in cloud security and compliance

Another issue is the rather slow improvement of the skill set that can address cloud security and compliance problems. In the (ISC)² cybersecurity professional's research conducted in 2021 indicated that the cybersecurity workforce across the globe must expand by 65% to protect valuable resources adequately. This gap is most evidently witnessed in use cases such as cloud native security tools, compliance automation and DevSecOps. This problem is being worked through training programs as some organizations are hiring managed security service providers to support them (Barton, Garbani, & Kalra, 2021).

B. Tool sprawl and integration issues

This means that, organizations struggle to deal with concerning issues such as tool proliferation, as well as integration complexities of cloud platforms and security frameworks. This can result

into complexity and in some cases, lack of visibility. By 2025, Gartner concluded that sixty percent of the companies will be incorporating the cybersecurity risk as a critical key factor in third-party deals. It is quite common today for various organizations to look for cloud-native security platforms offering integrated solutions, and while this is relatively feasible to achieve, the provision of a variety of integrated solutions while at the same time avoiding lock-in to a specific vendor's services is rather hard.

C. Balancing agility with governance requirements

One of the key challenges is the scale of contrast there is between the concept of being sufficiently agile to deliver a product in a fast and efficient manner, and the need for sufficient governance structures. Research conducted by Deloitte revealed that, while 65 percent of the organisations' top reason to use cloud is agility, 48 percent of them see security and compliance issues as a major obstacle (Barton, Garbani, & Kalra, 2021). To counter this, organizations are implementing automated governance models and policy as code solutions, but the skill of achieving the optimal balance is still being developed and enacted.

D. Keeping pace with evolving threat landscape and regulations

Cybersecurity threat grows fast; likewise, regulations that govern its industrial usage are continuously changing. McAfee further notes that such cloud organizations incur about 3,798 unique incidents relating to cloud security every month. Gartner state that the percentage of the worlds people, whose personal data is governed by modern privacy laws, will be 65% by 2023 (Alkhaldi & Alosaimi, 2022). The organizations therefore need to conduct continuous monitoring, threat intelligence, and compliance management that is more flexible to enable them handle these changes.

IX. Future Trends and Innovations

A. AI and ma chine learning in cloud security

Organizational AI and ML are emerging as indispensable features of cloud security and compliance. Therefore, Capgemini established that 69% of organizations still think that they are unable to handle pivotal threats with Artificial intelligence. These technologies increase threat identification, make security operations more efficient, and offer better monitoring on compliance levels. This cognitive technology is capable of processing big data, within a short span of time, and is capable of recognizing patterns of deviation. Accordingly, the AI and ML maintain the monitoring as well as reporting of features by evaluating cloud configurations against guidelines continually.

B. Quantum secure cryptography to cloud infrastructure

Subsequently, more attention is being paid to quantum safe cryptography given the development of quantum computing. This strategy is also currently standardizing post-quantum cryptographic algorithms from NIST. Some of the cloud providers such IBM are adopting the quantum-safe

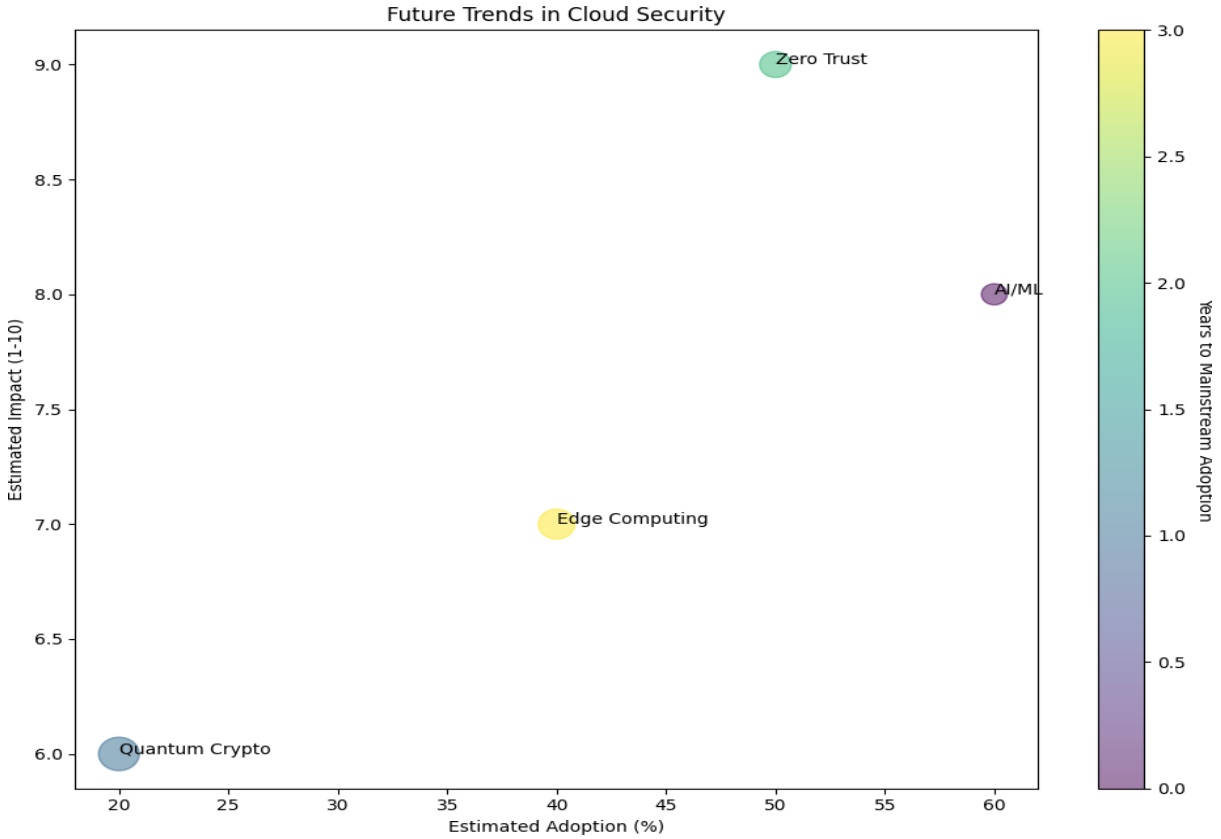
cryptography in their service provision (Alkhaldi & Alosaimi, 2022). More importantly, it will make organisations review their cryptographic implementing strategies and evolve on how to accommodate quantum-safe algorithms.

C. Zero Trust architecture in agile cloud environments

Zero Trust security model has recently emerged as the stratum for protecting agile cloud environments. Microsoft said in its research, 96 percent of security decision-makers have identified Zero Trust as mission-critical to their organization. Predicting that no user equipment or network should be trusted (Verizon, 2021). A critical component is indeed Identity and Access Management (IAM), which is needed to ensure that only authenticated and approved users have access to the company's resources and data.

D. Edge computing security considerations

The essence of edge computing is that it creates new security risks for rapid cloud initiatives. It is further projected that by 2025, three quarters of enterprises data will be generated and managed outside the typical data centre or the cloud. As for securing the edge environments, they should be based on the distributed security model that encompasses the proper encryption of data, authentication of devices, and coherent security measures for the edge and cloud domains (Subramanian & Jeyaraj, 2018). Apparently, there are new technologies in security that are expected to be developed to counter the challenges posed by edge computing.



X. Discussion

A. Key success factors for secure and compliant agile cloud projects

Several factors determine the optimize the chances for the implementation of secure and compliance agile cloud projects. First on our list is the factors of security and compliance being incorporated beginning from the specifications phase. This approach known as ‘’shift-left’’ makes security part of the initial process instead of being received at the last end as an add-on. As companies that have implemented this approach are quick to attest, this process greatly and expedited vulnerability remediation with consequent overall enhanced security statuses of organizations (Rong, Nguyen, & Jaatun, 2013).

The other important element that has been well implemented is automation and the practice of continuous monitoring. The best practices in security testing that include automating security testing, compliance check, and vulnerability management facilitate organizations’ capacity to adapt in line with the dynamic nature of agile clouds. Consumers’ research from Puppet shows that extremely automated security forces take fifty percent lesser time to reclaim security problems compared to the organizations with low automation.

The other elements include cross-boundary working and the distributed accountability for security. Productive organizations encourage everyone in the firm to approach security issues, rather than leaving the initiative to the IT department alone. These practices include offering intensive security training to the developers and operations staff and involving security specialists in the agile teams and planning.

Finally, the management of integrated cloud native security tools and services has also emerged revealed as a critical success factor (Ponemon Institute, 2021). Self-protection that many cloud service providers have integrated into their platforms usually offer organizations’ better integration and wider coverage than solutions procured and implemented separately.

B. Implications for organizational structure and culture

Essential changes in the organizational architecture and climate of the institution are usually required for a secure and compliant form of agile cloud projects. Hence instead of having models where security and compliance are an afterthought of development and operations, we are gradually seeing a transition. It is usually done in a way that entails structure of a multi-disciplinary team that is composed of security personnel, developers and operations staff.

The latter could be called as a clear manifestation of such tendency, as DevSecOps practices are based on merging between the development, security and operation teams. Gaining perspective from the concept implies changes in methods of recruitment, training, and succession planning within organizations. According to the research conducted by Deloitte, 88% of organizations al said that DevSecOps have enhanced their application and infrastructure security (NIST, 2020).

Cultural/Perception shifts are also very critical. The last measure of good security management is the creation of a culture of security within an organization and recognition that security is everyone's responsibility. This often encompasses constant staff sensitivity training, rewards for security-related practices, and obvious communication of security goals and their relevance to the organization's function.

However, the transition toward agile cloud projects frequently entails a change in the risk tolerance and choices. It is vital for the organizations to find a middle ground between flexibility and control; frequently, this results in organizations using more adaptive, contextual approaches to security and compliance management.

C. The role of cloud service providers in shared security responsibility

It is impossible to talk about the basic principles of cloud security without mentioning the shared responsibility model that outlines security responsibilities between CSPs and their customers. Nevertheless, the meaning and application of this model are still extended with the develop of cloud services and the change of the regulatory demand.

There is a critical need to collaboratively drive compliant and secure agile cloud projects through cloud service providers. They are packing more and sophisticated security solutions and compliance solutions, compliance reports, threat insights and data safety. Research carried out by IDC has revealed that 40% of firms choose cloud as a method of increasing security, proving that firms have huge confidence in the security of cloud providers.

But with shared responsibility model there is a number of responsibilities resting on cloud customers as well (Khalil, Khreishah, & Azeem, 2014). This paper serves as a reminder that the organizations require understanding their security and compliance mandate and apply adequate controls or procedures. This often entails the training more of skills and utilization of instrumentalities that can be used in the management of security in cloud computing environments.

In the future, the development trend of the shared responsibility model will follow the above direction, which is still in a stage of continuing to develop and gradually complete. It is probable that over time, more of the security and compliance aspects are going to be offloaded to the cloud providers, especially in areas where they are positioned to bring efficiency to bear on the problem. , At the same time, multi-cloud and hybrid environments might bring a new set of challenging tasks for managing distributed security responsibilities with different levels of maturity across software platforms and services.

XI. Conclusion

A. Summary of key findings

This research has, therefore, sought to carve out the interconnected themes in guaranteeing security and compliance in agile cloud infrastructure projects. This lacks security and compliance of the developed product, prioritization of security and compliance, automation and continuous

monitoring as centre to highly valued in agile development process, and suggested cultural and organizational change are among the critical findings.

The presented researches showed that today various organisations of different industries may adopt secure and compliance agile cloud projects with impressive advantages in terms of flexibility, cost, and security. However, these achievements might be accompanied by a number of hurdles such as lack of skills, integration of tools, and, at the same time, ensuring flexibility of working while adhering with the governance frameworks (ISO/IEC, 2015).

B. Recommendations for practitioners

Based on the findings of this research, several recommendations can be made for practitioners:

1. Ungerman shifts security responsibility left which means security priorities are to take into consideration from the project initiation and over the course of software development.
2. Acquire and deploy automated tools and more importantly, constant monitoring to contain with erratic characteristics of agile environments in clouds.
3. Encourage the mentality of security as everyone's business across all the teams working on cloud projects.
4. Automate cloud security since security tools and services should be as native to the cloud environment as other services.
5. Apply DevSecOps strategy across one's enterprise, avoiding the separation of Dev, cybersecurity, and Ops.
6. Security and compliance should be performed on a constantly and updated on a consistent basis due to the dynamic threat environment and changes in regulations.
7. Encourage employee training and continued education to help deal with cloud security workforce deficiency.

C. Future research directions

While this study has provided valuable insights into the current state of security and compliance in agile cloud projects, several areas warrant further research:

1. The synergistic approach of DevSecOps practices in continuous security and compliance in cloud environments in the long-run.
2. The likely shift of the cloud security and compliance strategies in relation to the new technologies like the edge computing and 5G.
3. Approaches that can prove helpful in the case of security and compliance when using multi-cloud and hybrid cloud models.
4. AI & ML expectancies for improving cloud security and enforcing compliance mechanisms.
5. Thus, the emergence of shared responsibility model and its impact on the cloud security and governance.
6. A comparison of the approaches to the training of cloud security specialists.

The given overview shows that as the cloud solutions are progressing and companies are embracing the use of agility, the necessity of security and compliance in these circumstances is going to get even higher. Further research in these areas will be essential in supporting organisations in comprehending the alterations in the flow of managing cloud security and compliance, using individual components of concepts like 'agility'.

XII. References

Alkhaldi, F. M., & Alosaimi, R. (2022). Cloud computing adoption barriers in small and medium enterprises (SMEs): A systematic literature review. Journal of Information Systems and Technology Management, 19, e202219002. https://doi.org/10.4301/S1807-1775202219002

Barton, D., Garbani, J., & Kalra, S. (2021). Cloud adoption to accelerate IT modernization. McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization

Casalicchio, E., & Iannucci, S. (2020). The state-of-the-art in container technologies: Application, orchestration and security. Concurrency and Computation: Practice and Experience, 32(17), e5668. https://doi.org/10.1002/cpe.5668

Cloud Security Alliance. (2021). Cloud Controls Matrix v4. https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Deloitte. (2021). DevSecOps and the cyber imperative. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2021/devsecops-and-the-cyber-imperative.html

Gai, K., Qiu, M., & Zhao, H. (2018). Privacy-preserving data encryption strategy for big data in mobile cloud computing. IEEE Transactions on Big Data, 6(3), 384-395. https://doi.org/10.1109/TBDATA.2018.2829886

Gartner. (2022). Gartner forecasts worldwide public cloud end-user spending to reach nearly $500 billion in 2022. https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

IBM. (2021). Cost of a data breach report 2021. https://www.ibm.com/security/data-breach

ISO/IEC. (2015). ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. https://www.iso.org/standard/43757.html

Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A research. Computers, 3(1), 1-35. https://doi.org/10.3390/computers3010001

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Ponemon Institute. (2021). 2021 Cost of a Data Breach Report. IBM Security. https://www.ibm.com/security/data-breach

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A research on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), 47-54. https://doi.org/10.1016/j.compeleceng.2012.04.015

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42. https://doi.org/10.1016/j.compeleceng.2018.06.006

Verizon. (2021). 2021 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/