Scientific Research Publishing

Journal of Information Security, 2024, 15, 1-14
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Saviynt Meets GCP: A Deep Dive into Integrated IAM for Modern Cloud Security

Sampath Talluri

Department of Computer Science, Western Michigan University, Kalamazoo, USA
Email: tsampatht1@gmail.com

How to cite this paper: Talluri, S. (2024) Saviynt Meets GCP: A Deep Dive into Integrated IAM for Modern Cloud Security. *Journal of Information Security*, **15**, 1-14.
https://doi.org/10.4236/jis.2024.151001

Received: November 14, 2022
Accepted: December 22, 2023
Published: December 25, 2023

Abstract

The Google Cloud Platform (GCP) is a popular choice for companies seeking a comprehensive cloud computing solution because it provides everything from essential computing resources to powerful data analytics and machine learning capabilities. Saviynt is a cloud-based Identity and Access Management (IAM) system that integrates with Google Cloud Platform (GCP) and other services for additional functionality. However, other problems are associated with the transition, such as the requirement to correctly integrate IAM Saviynt into current IT infrastructures and provide comprehensive training to users on the new system. The paper will give a detailed review of the advantages, disadvantages, and best practices related to this transition.

Keywords

Google Cloud Platform (GCP), Identity and Access Management (IAM), Saviynt, User Identities, Access Privileges, Authentication Processes

1. Introduction

1.1. Background

Saviynt and Google Cloud Platform (GCP) are formidable competitors in cloud computing and identity access management (IAM). Google Cloud Platform (GCP), a well-known public cloud platform, provides a wide range of computing, storage, networking, and application development services. Saviynt is an IAM platform designed for cloud environments to manage identities, restrict privileged access, and ensure cloud security. It provides a complete solution. GCP's Identity and Access Management features are called Cloud Identity and Access Management (Cloud IAM). It provides a comprehensive framework for managing user access to GCP resources. Businesses can utilize cloud-based IAM

to easily create and manage user accounts and groups, create and enforce access control policies, and manage multi-factor authentication (MFA) deployment. Saviynt enhances GCP's current identity and access management (IAM) capabilities by providing a unified platform for managing identities, access limitations, and privileges across several cloud platforms, including GCP. Provisioning, de-provisioning, and access reviews are just a few identity governance procedures Saviynt's platform can automate. It also offers fine-grained control over privileged access through automated credential rotation, just-in-time access, and password-less authentication.

The Google Cloud Platform (GCP) is a collection of cloud-based services that run on the same underlying infrastructure as Google's more well-known consumer products, such as Search and Video. Google Cloud Platform (GCP) provides various services, including computing, data storage, data analytics, and machine learning.

As illustrated in Figure 1, Saviynt is a cloud-based Identity and Access

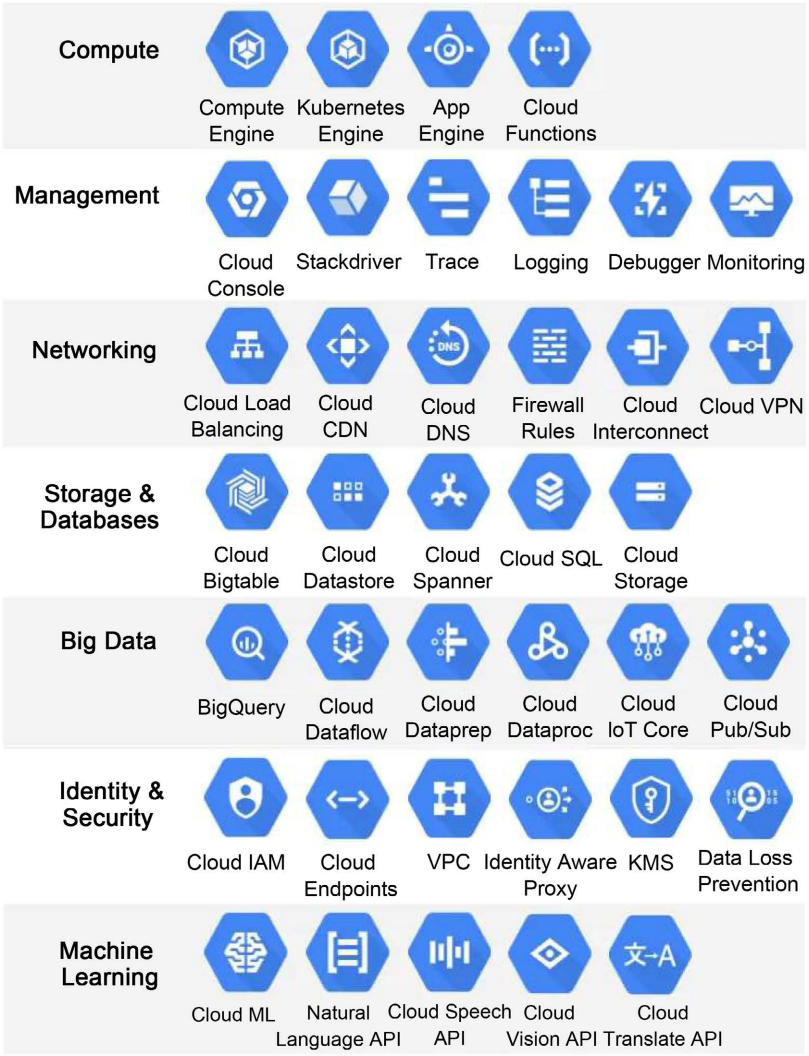

Figure 1. GCP mechanism.

Management (IAM) service that assists enterprises in managing the identities and permissions of their users across several cloud services, including GCP [1]. Saviynt delivers a consolidated view of user identities and permissions, making cloud service access easy to manage and audit. A firm's "Identity and Access Management" (IAM) is the set of policies and processes that monitor and restrict employees' access to company resources. IAM integrates various technologies, laws, and procedures to ensure the proper use of resources. Saviynt is a cloud-based Identity and Access Management (IAM) service that assists enterprises in managing the identities and permissions of their users across several cloud services, including GCP. Saviynt delivers a consolidated view of user identities and permissions, making cloud service access easy to manage and audit. Saviynt's Cloud PAM's most recent version improves in numerous critical areas, including governance, analytics, and privileged assets accessible across various enterprise apps and platforms. Rapid cloud adoption, widespread acceptance of collaboration tools, and the need for flexible and secure access for a more distributed workforce have all contributed to the increasing significance of these skills.

IAM Saviynt provides security capabilities that might help an organization's security posture. This category includes multiple authentication elements and centralized and role-based access control. IAM Saviynt delivers a system that helps businesses increase the effectiveness of their IT operations by automating and streamlining user identification and access privilege management. However, there are certain hurdles to switching from Google Cloud's native IAM to IAM Saviynt, such as the necessity to connect IAM Saviynt with existing IT infrastructure and the requirement to provide users with adequate training on the new system. This research study aims to look at the advantages and disadvantages of transitioning from Google Cloud's built-in Identity and Access Management (IAM) system to the IAM Saviynt platform. Companies can also benefit from the advice it offers on how to make this shift a success.

1.2. Aim, Objectives, and Research Questions

1.2.1. Aim

The research examines the benefits and drawbacks of moving towards IAM software like Saviynt from native Google Cloud.

1.2.2. Objectives

- To understand the differences between Google Cloud and IAM Saviynt.
- To identify the key challenges and benefits of shifting from GCP to IAM Saviynt.
- To understand the implementation errors of IAM Saviynt and their impact.
- To assess the influence of these interconnections on the company's operations.
- To develop the best practices for shifting to IAM Saviynt.

1.2.3. Research Questions

- What are the challenges and benefits of shifting from Google Cloud to IAM Saviynt?
- What best practices are for shifting from Google Cloud to IAM Saviynt?
- How can organizations make the transition to IAM Saviynt successfully?

1.3. Research Rationale

Google Cloud is a well-known cloud computing platform that offers numerous alternatives. However, the built-in IAM system only offers basic functionalities for managing user IDs and permissions. Many firms want increased centralized access management, role-based access control, and multi-factor authentication, to name a few IAM advances. Saviynt, hosted in the cloud, is a superior Identity and Access Management (IAM) solution for GCP and other cloud services. This solution can provide organizations with several benefits, including improved security, a lower risk of compliance violations, and better operational efficiency. Moving from Google Cloud's native IAM to IAM Saviynt, on the other hand, presents several hurdles, including the necessity to integrate IAM Saviynt with existing IT infrastructure and the importance of providing users with adequate training on the revolutionary technology. To assist businesses in dealing with these problems, this study investigates the advantages, disadvantages, and best practices of moving to IAM Saviynt. The information and suggestions in this guide can help ease the transfer process.

1.4. Significance of the Research

The study of transitioning from Google Cloud's native IAM to IAM Saviynt has scholarly value since it will provide critical insights to enterprises considering the transfer. The advantages of switching to IAM Saviynt are discussed, including improved security posture, reduced risk of noncompliance, and increased operational efficiency. This paper aims to foresee and overcome potential issues with using IAM Saviynt. These challenges include integrating IAM Saviynt with pre-existing IT systems and delivering user training for the new system. Furthermore, the conclusions of this study will contribute considerably to the understanding of IAM Saviynt and cloud security in general. The primary purpose of this research is to identify the best techniques for establishing IAM Saviynt and managing IAM in the cloud. In general, research studying the migration process from Google Cloud's native IAM to IAM Saviynt is an essential and relevant endeavor that can provide significant insights to enterprises and the academic community.

2. Literature Review

Successful Saviynt Identity and Access Management (IAM) solution users have a strong business case for making the switch and have appropriately planned the implementation. This section will examine the relationship between this innova-

tion and business effectiveness in the new environment.

2.1. Differences and Integration

The Google Cloud Platform (GCP) is a collection of cloud-based services that run on the same underlying infrastructure as Google's more well-known consumer products, such as Search and Video. Google Cloud Platform (GCP) provides diverse services in various categories, including solid computing resources, accessible data storage alternatives, intelligent data analysis methods, and cutting-edge machine learning systems. Saviynt, a cloud-based IAM solution, helps businesses manage user identities and access credentials efficiently across several cloud platforms, including Google Cloud Platform (GCP). Saviynt delivers a consolidated view of user identities and permissions, making cloud service access easy to manage and audit. One of the most critical parts of cloud administration is handling user identities and access privileges efficiently across many cloud platforms, such as Google Cloud Platform (GCP). This system gives a uniform picture of user identities and the permissions that go with them [2]. Finding a function's integral is crucial to the concept of integration, which is a fundamental mathematical operation in and of itself.

Integrating IAM Saviynt into the present IT architecture is critical to increasing compliance, identity management, and security. To ensure a smooth transition and minimize any delays, it is necessary to follow a systematic approach that involves rigorous testing, outstanding coordination, and meticulous preparation.

With time, an exact description of the extent of the integration must be produced, including identifying the specific IT systems, apps, and data sources that will be integrated into the Saviynt platform. Understanding the current Identity and Access Management (IAM) infrastructure and the anticipated integration outcomes is a critical aspect of this approach. The organization must thoroughly analyze the present Identity and Access Management (IAM) system, including all applicable rules, processes, technologies, and controls for user access. This review aims to identify potential integration locations and difficulties that may arise during integration.

2.2. Challenges and Benefits

Some businesses may need help transitioning from Google Cloud to IAM Saviynt due to the learning curve involved in adjusting to a new platform and all of the features and capabilities that come with it. To make the transfer, organizations must be conversant with the details of both platforms and have extensive experience with data and application migration. Furthermore, firms may need help training and re-skilling employees to make the most of new technology.

A complete problem-solving method is required to manage challenges linked to integrating IAM Saviynt and user training in practical circumstances. Methods such as surveying users, gathering feedback, and monitoring their beha-

vior can assist in identifying areas where user training is lacking, which is critical. Prioritizing the development of specific training materials that address the identified areas for improvement is critical. Task-specific user guides, interactive modules, and practical exercises could be among the educational tools provided.

Furthermore, various teaching tactics must be used to accommodate diverse learning styles. Various learning approaches may be provided, such as self-paced learning modules, video demonstrations, in-person seminars, and online tutorials. It is critical to give opportunities for ongoing training to keep users informed about new features, changes to procedures, and security best practices.

Migrating from Google Cloud's native IAM to IAM Saviynt is a challenging task that requires careful planning and execution. IAM Saviynt must be integrated with the existing IT infrastructure, user identities, and access privileges must be moved, and new system users must be educated. Acquiring and deploying IAM Saviynt may incur significant expenses. Before making a final decision, businesses should carefully assess the costs and benefits of migrating to IAM Saviynt [3]. Adoption of IAM Saviynt requires a mindset shift and reevaluation of operating methods. Obtaining buy-in from higher management and maintaining open lines of communication with end users are critical components of any transformation.

Benefits

Businesses may utilize IAM Saviynt to streamline existing security procedures, provide role-based access control, and make multi-factor authentication easy to use. Implementing this strategy can significantly reduce the risk of unwanted access to personal information and valuable resources. Businesses can lower their compliance risk by utilizing IAM Saviynt, which assists with the specialized management of user identities and access entitlements, as needed by government and industry standards. IAM Saviynt, for example, can make it easier for enterprises to implement least privilege access and role separation [4]. Saviynt offers a unified platform for managing identities, permissions, and access controls in various cloud environments, including those with on-premises, hybrid, or multi-cloud infrastructures. This streamlines identity management across the organization and eliminates the need for separate IAM solutions. Businesses can strengthen security posture and meet regulatory requirements by utilizing Saviynt's sophisticated identity and access management (IAM) features. As shown in **Figure 2**, the system includes many features, such as automated reporting, continuous monitoring, fine-grained access control, and on-demand access.

IAM Saviynt delivers a system that helps businesses increase the effectiveness of their IT operations by automating and streamlining user identification and access privilege management. As a result, IT staff may be able to focus on other activities.

However, the advantages do not end there. Saviynt increases visibility and control by giving a consolidated picture of user identities and rights. This capability simplifies access control and auditing in the cloud.

Figure 2. Saviynt mechanism.

2.3. Best Practices

To ensure a smooth transition and avoid any potential disruptions, the effective deployment of IAM Saviynt necessitates careful planning, collaboration, and adherence to acknowledged best practices. Thorough testing is required to ensure the integration works correctly and without mistakes. Validating automated workflows or procedures, access control restrictions, and data synchronization is equally crucial. Foremost, there is a need to be aware of the current login credentials, permissions, and security settings. The implementation necessitates looking into the current Identity and Access Management (IAM) infrastructure that must be addressed before implementing IAM Saviynt. The security posture has improved, compliance issues are less likely, and IT operations are more efficient. It is choosing the best IAM Saviynt solution for the company. There are numerous IAM Saviynt alternatives, each with its own set of advantages and disadvantages. It is critical to choose a solution that is tailored to the company's specific requirements. There is a need to create a detailed project strategy to ensure the IAM Saviynt platform's successful implementation [5]. When developing a project plan, it is critical to incorporate a timeframe, budget, and risk management strategy—maintaining ongoing communication with the users during installation. This step will help users learn the new system and adjust to its ongoing modifications. Thorough testing is strongly advised before deploying

IAM Saviynt in a live environment. This will help ensure the system functions as intended and meets the security and compliance requirements. Users should be given detailed instructions on how to use IAM Saviynt. This will let users manage their identities and access privileges more effectively. It is maintaining constant proactive monitoring and maintenance of IAM Saviynt. This includes ensuring all usernames and permissions are current, and the system is configured correctly.

2.4. Integrating the Shift

Expanding a company's available resources is proportional to the number of programs authorized users require access to. The rise of SaaS services has been linked to an increase in the number of resources that require authentication. Many modern firms employ an active directory system as a consolidated database for all user information. All vital identifiers are kept in one place by the active directory. Once the directory is operational, it will seamlessly integrate into their existing infrastructure. Multi-factor authentication (MFA) must be activated to comply with the rules. Individuals must use various authentication methods to satisfy the requirements of Multi-Factor Authentication (MFA) systems. This category includes knowledge-based authentication mechanisms (passwords), possession-based (smartphones/tokens), and inherence-based (biometrics).

After identities have been established, gaining access may become more complicated. A university professor may have a variety of roles inside the institution, each with its own set of duties and benefits. As shown in Figure 3 for MFA, authorized access to confidential university data, such as students' academic grades and advising records, is required for professors to effectively carry out their educational responsibilities. Furthermore, numerous schools waive tuition for personnel such as teachers and administrative assistants. It is critical in the classroom that teachers only have access to information about their pupils rather than other teachers' records.

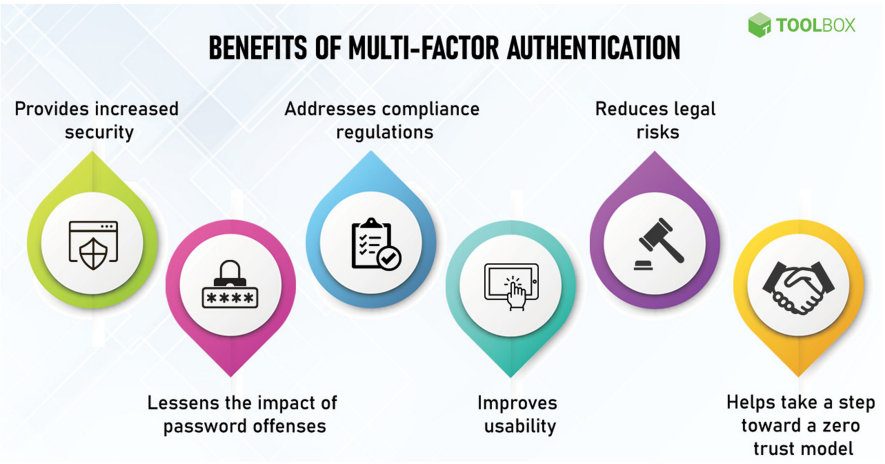

Figure 3. Benefits of multi-factor authentication.

3. Methodology

3.1. Use Tools and Techniques

The benefits of implementing Identity and Access Management (IAM) over Information Technology (IT) were investigated. This theoretical framework bases knowledge on observable occurrences and quantifiable facts. Adopting a positivist worldview in this context entails taking a systematic and objective approach. The number of errors, rate of integration success, and system efficiency are qualitative measures that will be critical in determining the solution.

The investigation's conclusions were derived using secondary qualitative analysis and theme analysis. The accompanying graphic depicts the benefits and current trends of secondary research. Instead of starting from scratch, it is best to focus on studying current facts. Data from many sources, such as databases, scholarly articles, case studies, and official reports, have been meticulously evaluated. We also studied relevant reviews and articles for our inquiry. Secondary data collection methodology has been beneficial, and a thematic approach has been demonstrated to help discover themes and patterns within qualitative data. Extensive theoretical frameworks have been established based on current literature on the relationship between Google Cloud and IAM systems and their integration. This method can be used to find relationships and hypotheses that can be tested using data analysis. This inquiry employed a logical technique to confirm past hypotheses while providing a new perspective backed by qualitative evidence.

3.2. Data Collection

This analysis relied entirely on secondary sources such as books, papers, reports, and research produced by other institutions.

As illustrated in **Figure 4**, the sources above offered quantifiable outcomes connected to the adoption of Saviynt-IAM technology. The study is based on current literature and uses databases and digital libraries to ensure accuracy and relevance. The meticulous collecting, classification, and organization of the data enabled a complete qualitative thematic analysis of the topic.

3.3. Data Analysis

Following data collection, a complete qualitative thematic analysis was carried out. The adoption of statistical tools aided both data analysis and data presentation. Descriptive statistics have repeatedly demonstrated their utility in uncovering underlying tendencies and patterns. The researchers used inferential methodologies to investigate connections and evaluate ideas generated by the current body of literature. The qualitative data has been organized by topic. Much research has been conducted in numerous domains to identify regularities, outliers, and trends. The revealed themes are congruent with the study's stated goals since they were created after thoroughly examining those goals. The team employed the strategies above to extract usable data from the large dataset.

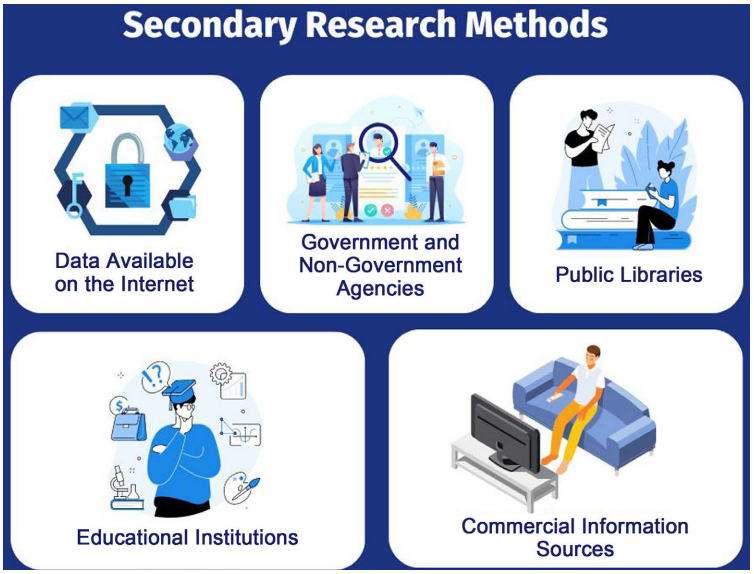

Figure 4. Secondary data collection.

3.4. Ethical Consideration

Maintaining ethical standards has been of utmost concern throughout this research. All primary sources were correctly recognized and attributed by academic traditions, decreasing the risk of plagiarism claims caused by using secondary sources. No sensitive or secret material was used to ensure the privacy of the information. An attempt was needed to make the statistics in the study match the anecdotes better. Every natural or possible conflict of interest has also been disclosed.

4. Findings and Analysis

4.1. The Implementation Basics

Saviynt is a cloud-native IAM framework that enables the centralized management of user identities and access rights across various cloud services, including Google Cloud. Saviynt consolidates user identities and permissions, making administration and auditing easier. Accurate integration requirements, such as user identity and access credential management, must be defined, as must the required security and compliance standards.

Data synchronization mechanisms and protocols for sharing information between IAM Saviynt and Google Cloud are being developed.

Carry out the part-merging method. Integrating IAM Saviynt with Google Cloud necessitates configuring both platforms. Thorough integration testing ensures correct operation and reliable maintenance of user IDs and access credentials. The integration can be deployed to the live environment when thoroughly tested and verified.

4.2. Provisioning and De-Provisioning

Provisioning is supplying something to someone who needs it, such as supplies,

labor, or technology. The process of generating users, allocating accounts, and assigning suitable rights is called provisioning. The following part discusses de-provisioning essentials when one connects the IAM Saviynt platform to Google Cloud. The IAM Saviynt system can provision user accounts on the Google Cloud Platform (GCP). SCIM synchronization, CSV data input, and manual provisioning are all possible possibilities. One may configure permissions for Google Cloud services using IAM Saviynt. The Identity and Access Management (IAM) system, in this case Saviynt, enables users to be assigned roles. Saviynt will then synchronize these roles with the Google Cloud Platform (GCP), providing users with the necessary access.

The process of removing user accounts and related credentials is known as de-provisioning. The following actions must be taken to revoke users' access to Google resources after connecting Saviynt's IAM solution with Google Cloud. The IAM Saviynt platform allows users to schedule the de-provisioning of their GCP accounts. SCIM synchronization, CSV data import, and manual de-provisioning are just a few available techniques. IAM Saviynt allows one to establish de-provisioning rights for Google Cloud resources. Permissions are withdrawn when a user is removed from a role in IAM Saviynt. After that, Saviynt, an identity and access management solution, will synchronize these adjustments with the Google Cloud Platform (GCP), thus removing users' access privileges.

4.3. Integration

Since the interaction between Google Cloud and IAM Saviynt is inherently complicated, careful design and execution are required. The first step determines the precise requirements for the integration method. This includes the administration of security and compliance procedures, as well as the identification and permission of users. The design phase of the integration process begins after the requirements have been identified. This necessitates an examination of the protocols used to exchange information between the two platforms and developing a technique for maintaining them in sync. Carry out the processes required to integrate numerous pieces into a single whole; this integration process must be carried out.

To accomplish this method, the two systems must be configured and linked. Once the integration has been developed, it must be thoroughly tested to ensure it performs as expected. To guarantee effective management, all user identities and rights must be reviewed. Make the connection function. The integration can be used in the production environment after extensive testing and verification [6].

4.4. Implementation Errors and Best Practices

The configuration of IAM Saviynt is complex, with numerous choices. A lot is riding on correctly configuring IAM Saviynt for a company's needs. Problems, on the other hand, may develop due to unlawful access to resources or needing help keeping track of individual users' identities and permissions. The likelihood

of a partial or failed migration of user identities and access permissions is a severe issue when switching from an existing IAM system to an IAM system. All user identity and rights information must be reliably and thoroughly communicated [7].

Conversely, some users may need help obtaining the necessary materials, while others may unintentionally acquire access to critical information. Because of the concerns identified by the lack of pre-implementation testing, comprehensive post-deployment evaluations of IAM Saviynt are required. The lack of sufficient user training is a severe concern that requires full training on deploying IAM Saviynt. This will assist in guaranteeing that users understand how to obtain and manage access privileges, as well as the other aspects of IAM Saviynt. Alternatively, users making frequent access requests or experiencing issues with system functionality may present challenges.

4.5. Benefits

Combining IAM Saviynt and Google Cloud is a wise decision. Some security features made feasible by adopting IAM Saviynt include centralized access management, role-based access control, and multi-factor authentication. Overall, these enhancements increase Google Cloud's security. Businesses can use IAM Saviynt to lower their risk of non-compliance with requirements such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard. IAM Saviynt delivers a system that helps businesses increase the effectiveness of their IT operations by automating and streamlining user identification and access privilege management.

To summarize, IAM Saviynt is a powerful IAM solution that may improve network security, reduce the chance of regulatory violations, and increase the efficiency of IT operations. Businesses that link IAM Saviynt with Google Cloud reap various benefits. One is centralized management, which may be accomplished by centralizing user identity and access permission management across all their cloud resources.

5. Conclusion

Businesses have numerous challenges and opportunities when transitioning from Google Cloud Native to Identity and Access Management (IAM), and installing Saviynt's IAM platform is no easy process. However, the benefits of IAM Saviynt are significant, including improved security posture, reduced noncompliance risk, and increased IT operational efficiency. As a result, more and more businesses understand the value of investing in information technology.

Recommendation

Integrating the following recommendations will ensure a successful deployment of IAM Saviynt and limit the chance of installation errors:

- The documentation provided by IAM Saviynt is quite helpful in configuring and operating the system. It is critical to carefully study the instructions before putting IAM Saviynt into production.
- The pre-implementation checklist from IAM Saviynt provides a complete summary of everything that has to be done before the program is installed [3].
- After implementation, it is vital to thoroughly test the IAM Saviynt system to confirm its functioning as planned. IAM Saviynt's features and capabilities must be extensively tested, and the system's performance must be validated over a wide range of use cases.
- It is critical to train users on how to use IAM Saviynt. The training program should cover many system-related concerns, including acquiring and managing access privileges.

Author's Contributions

Sampath Talluri exclusively conceived and designed the study, collected and analyzed the data, and wrote the manuscript.

References

[1] Saviynt (2022) Digital Transformation: Identity is GCP's Security Perimeter. https://saviynt.com/webinars/digital-transformation-why-identity-as-your-security-perimeter-is-vital-for-gcp/

[2] Konstantinidis, G. (2021) Identity and Access Management for E-Government Services in the European Union–State of the Art Review. https://hellanicus.lib.aegean.gr/bitstream/handle/11610/23968/Thesis.pdf?sequence=1&isAllowed=y

[3] Saviynt (2022) Intelligent Identity and Smarter Security—Saviynt. Identity and Access Management (IAM). https://saviynt.com/glossary/identity-access-management-iam/

[4] Blum, D. and Blum, D. (2020) Control Access with Minimal Drag on the Business. In: Blum, D., Ed., *Rational Cybersecurity for Business*: *The Security Leaders' Guide to Business Alignment*, Apress Berkeley, CA, 227-257. https://doi.org/10.1007/978-1-4842-5952-8_8

[5] Takabi, H., Joshi, J.B.D. and Ahn, G.-J. (2010) Security and Privacy Challenges in Cloud Computing Environments. *Journal of IEEE Security and Privacy*, **8**, 24-31. https://doi.org/10.1109/MSP.2010.186

[6] Gayatri, I.A.M. and Suriata, I.N. (2020) Challenges and Opportunities of Blind Masseurs in Increasing Competency through Implementation Business Standards of Massage Parlor. *ADI Journal on Recent Innovation* (*AJRI*), **1**, 107-120. https://doi.org/10.34306/ajri.v1i2.40

[7] Spiceworks (2021) What Is Multi-Factor Authentication? Definition, Key Components, and Best Practices. https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-multi-factor-authentication/

Abbreviations

IAM: identity access management; MFA: Multi-Factor Authentication; SaaS: Software as a Service; GCP: Google Cloud Platform.