**Significance of Cloud Security Posture Management in Cyber Security Cloud Networks: A Study from SMB Business**

# **Abstract**

Cloud computing has transformed the business landscape, enabling organizations to achieve unprecedented levels of scalability, flexibility, and operational efficiency. However, this shift to cloud environments introduces significant security challenges, particularly for small and medium-sized businesses (SMBs) that often lack the resources to manage complex cybersecurity needs. Cloud Security Posture Management (CSPM) has emerged as a vital strategy for addressing these challenges, offering continuous monitoring, automated compliance management, and the remediation of security misconfigurations across cloud infrastructures. This thesis investigates the critical role of CSPM in enhancing cybersecurity for SMBs, exploring its effectiveness in identifying and mitigating vulnerabilities, ensuring adherence to regulatory requirements, and protecting sensitive data. By examining the deployment of CSPM tools such as Microsoft Defender for Cloud, Azure Policy, and Microsoft Compliance Manager, this research demonstrates how these technologies contribute to a robust security posture, fostering greater resilience against evolving cyber threats.

Contents

[**Abstract** 1](#_Toc174984061)

[**Chapter 1 Introduction** 3](#_Toc174984062)

[1.a. Overview: 3](#_Toc174984063)

[**1.b. Problem Statement:** 6](#_Toc174984064)

[**1.c. Research Questions:** 9](#_Toc174984065)

[**1.d. Research Objectives:** 9](#_Toc174984066)

[**1.e. Hypothesis** 9](#_Toc174984067)

[**1.f. Scope and Limitation:** 10](#_Toc174984068)

[**1.g. Ethical Issues:** 11](#_Toc174984069)

[**1.h.Structure of the Thesis** 12](#_Toc174984070)

[**1.i. Conclusion** 13](#_Toc174984071)

[**Chapter 2 Literature reviews** 14](#_Toc174984072)

[**2.a Cloud Security:** 14](#_Toc174984073)

[**2.b. CSPM:** 15](#_Toc174984074)

[**2.c. SMB Cybersecurity:** 16](#_Toc174984075)

[**2.d. Cloud Computing and SMBs:** 17](#_Toc174984076)

[**2.e. Cybersecurity Challenges in Cloud Environments:** 18](#_Toc174984077)

[**2.f. CSPM in Azure Cloud Platform:** 20](#_Toc174984078)

[**2.g. Challenges and Limitations of CSPM:** 22](#_Toc174984079)

[**2.i. Gaps Analysis:** 24](#_Toc174984080)

[**2.f Conclusions** 25](#_Toc174984081)

[**Chapter 3 Research Methodology** 26](#_Toc174984082)

[**3.a Research Design** 26](#_Toc174984083)

[**3.b Research Flow charts** 27](#_Toc174984084)

[**3.c Data Collection Methods** 28](#_Toc174984085)

[**3.d Selecting and implementing a CSPM tool:** 29](#_Toc174984086)

[**3.e Data Analysis and Security Posture Assessment: Evaluating Your Cloud Security** 30](#_Toc174984087)

[**3.f Recommendations and Action Plan: Taking Action to Improve Security** 30](#_Toc174984088)

[**3.g Evaluation and Impact Assessment: Measuring the Benefits of CSPM** 30](#_Toc174984089)

[**3.h Conclusions** 30](#_Toc174984090)

[**Chapter 4 Implementation** 31](#_Toc174984091)

[**4.1 Introduction** 31](#_Toc174984092)

[**4.2 Data Sources** 33](#_Toc174984093)

[**4.2.1 Azure Security Center** 33](#_Toc174984094)

[**4.2.2 Microsoft 365 Security Center** 33](#_Toc174984095)

[**4.2.3 Log Analytics** 33](#_Toc174984096)

[**4.3 Security Benchmarks** 33](#_Toc174984097)

[**4.3.1 ISO/IEC 27001** 33](#_Toc174984098)

[**4.4 CSPM Tools** 34](#_Toc174984099)

[**4.5 Implementation Steps** 35](#_Toc174984100)

[**Set Up Microsoft Defender for Cloud** 35](#_Toc174984101)

[**2. Configure Azure Policy** 36](#_Toc174984102)

[**3. Enable Log Analytics** 39](#_Toc174984103)

[**4. Use Compliance Manager** 44](#_Toc174984104)

[**Chapter 5: Results and Discussion** 49](#_Toc174984105)

[**5.a Introduction** 49](#_Toc174984106)

[**5.b Results of Compliance Assessments** 50](#_Toc174984107)

[**Summary of Assessments:** 50](#_Toc174984108)

[**UK GDPR Assessment:** In progress with 27% completion. 50](#_Toc174984109)

[**ISO/IEC 27001:2013 Assessment:** Incomplete with 70% completion. 51](#_Toc174984110)

[**Compliance Score and Progress:** 51](#_Toc174984111)

[**5.c Analysis of Key Findings** 53](#_Toc174984112)

[**UK GDPR Assessment for Microsoft office 365:** 53](#_Toc174984113)

[**ISO/IEC 27001:2013 Assessment for Microsoft 365** 55](#_Toc174984114)

[**5.d Impact of Completed Actions:** 58](#_Toc174984115)

[**5.e Challenges in Completing Assessments:** 58](#_Toc174984116)

[**5.f Significance for SMBs:** 59](#_Toc174984117)

[**5.g Conclusions:** 60](#_Toc174984118)

[**Chapter 6 Conclusion and Future work** 60](#_Toc174984119)

[**6.a Conclusions** 60](#_Toc174984120)

[6.b Future Work 61](#_Toc174984121)

# **Chapter 1 Introduction**

## 1.a. Overview:

Cloud computing has transformed the landscape of modern business operations, offering scalability, agility, and cost-efficiency. However, along with its benefits, cloud adoption presents significant cybersecurity challenges, particularly for small and medium-sized businesses (SMBs). In response to these challenges, Cloud Security Posture Management (CSPM) emerges as a crucial approach to enhancing cybersecurity in cloud environments (Bar-Haim, 2023). This study focuses on exploring the implementation of CSPM specifically within the Azure cloud platform, aiming to provide insights into its effectiveness in mitigating security risks and ensuring compliance for SMBs.

In the interconnected world of the internet, IT systems play a pivotal role in connecting various aspects of society. However, this connectivity also exposes systems to numerous threats and breaches, as different systems often have varying security measures in place. (Manns, 2021) highlight the continuous pursuit of innovations by cybersecurity and forensic specialists to address a wide range of cyber threats in real-time. It is increasingly recognized that human agents alone cannot effectively handle all requests in real-time. Therefore, reliable systems require inputs from machine learning techniques, big data, and threat intelligence to enhance detection, analysis, and defense capabilities (Barlette, 2015).

For instance the extensive data generated by monitoring solutions necessitates advanced analytical tools for mining and interpretation to maximize its utility in cybersecurity (Öhman, 2023), however a critical challenge hindering effective cybersecurity systems is the lack of collaboration between different stakeholders leading to capital constraints nonetheless cloud security posture management cspm emerges as a crucial security measure in cloud computing due to its ability to enforce continuous threat monitoring and real time risk assessment (Olaoye, 2024).

One of the prevalent security issues in cloud computing is inadequate change control and misconfiguration (Tomai, 2007). Many vendors prioritize ease of use and data sharing over security, resulting in inadequate strategies and policies for securing cloud-based infrastructure. Furthermore, the existing architecture of cloud-based infrastructure often does not provide clients with complete visibility or control of resources, leaving them reliant on the vendor's security measures. This reliance on vendor-provided security controls exacerbates misconfigurations, particularly among clients with multi-cloud deployments who may lack knowledge of suitable security mechanisms across all deployments (Bhattacharya, 2022). Consequently, enhancing cloud computing security architecture enables clients to be more aware of available measures for mitigating threats and their impact on cloud-hosted data and applications. Moreover, organizations can effectively evaluate individual vendors based on their ability to secure their infrastructure and customer data (Tam, 2022).

The adoption of cloud computing facilitates widespread access to data enabling employees to access corporate data and applications from virtually any location worldwide cloud computing thus plays a critical role in enabling flexible work arrangements global procurement practices remote workplaces and global teamwork as such advancements in security measures in cloud computing not only enhance remote workforce management but also contribute to disaster recovery through business continuity planning consequentlyCSPM facilitates high-level configuration of cloud storage and proactive cloud monitoring and audit leading to improved risk monitoring and management, as well as intensified cloud management and deployment automation (Rizvi, 2023).

But SMBs have difficulties in securing themselves as they don't usually have enough resources to be invested on staff training. And most of these times, that results in flawed security posture and makes easier for them to get attacked. CSPM implementation in SMBs can largely moderate these risks by offering a platform for constant monitoring, detecting misconfigurations and enforcing security policies throughout the hybrid cloud environment. These SMBs can now automate their security management, ensuring that security practices are in line with the dynamic nature of cloud environments (Ghosh 2024) through CSPM.

In addition, CSPM tools can help SMBs adhere to compliance requirements based on individual regulatory standards (GDPR, HIPAA and PCI-DSS.) They provide you the bird-eye view to cloud infrastructure and your resources which helps in detecting non-compliant configurations for swift actions. Moreover, SMBs would then be able to more easily meet compliance during an audit via detailed reporting and records which prevents any fines or penalties (Wang, 2023).

Integrating CSPM with the Azure cloud platform provides this edge for SMBs too, through Microsoft's enterprise-class security natively developed and hence can follow best practices. Azure has native CSPM tools, like Azure Security Center which offers a unified view of the security posture and recommendations for best practices plus automated remediation. The integration guarantees SMBs that they have a safe and compliant fully automated cloud environment, reducing the time it requires to maintain secure setups which in turn allows resources free to focus on core business operations (Johnson 2023).

In short, CSPM is a game-changer when it comes to SMB cybersecurity. As we continue along this path of increased cloud adoption, so too will the focus on how to implement strong security effectively and efficiently. CSPM as a solution has catered to the specific needs of small- and medium-sized businesses, ensuring uninterrupted security monitoring along with compliance management processes. This study takes a deeper look at CSPM on Azure Cloud Platform, offering insights and actionable suggestions to small-to-mid organizations looking toward strengthening their cybersecurity.

## **1.b. Problem Statement:**

Nowadays, small and medium-sized businesses are also increasingly adopting cloud computing to benefit from its scalability, agility, and, most important, cost-efficiency. Unfortunately, the transition to the cloud also poses significant cybersecurity challenges to SMBs. Having fewer financial, human, and technological resources and, as a result, less-developed security infrastructure, small and medium-sized businesses are more exposed to various cyber threats, such as data breaches, unauthorized access, and compliance violations. At the same time, the complexity of managing security in multiple cloud environments and constant changes posed more challenges to businesses.

One of the most critical SMBs-related problems is poor change control and misconfiguration of cloud infrastructures . Many cloud services are deployed quickly and with few or even none security policies, which makes it vulnerable to a wide range of external threats. For example, many CSPs prioritize data sharing and ease of use, paying less attention to the security of created configurations. However, many SMBs rely heavily on the vendor-provided settings, which results in a visibility gap — the provider has a better understanding of the environment than the customer. This situation leads to a higher risk of misconfiguration and breach.

Additionally, the current cybersecurity offerings for cloud environments are frequently siloed and need to be stitched together with a combination of tools/gateways supporting multi vendors in order to get complete security. This siloed approach represents a huge problem for small to medium enterprises (SMEs) which have less of an edge when it comes to tech expertise and financial resources- ultimately leading cyber security disarray, un-integrated solutions and delayed detection. The insufficient coordination and communication between other players in the cloud eco-system like Cloud service provider, Security vendors as well SMBs themselves making this entire process tough to crack. That split approach means having the money to build a better security strategy but somewhat wasting that capital because there are two places for it and what half should be built in one place is not always clear).

In addition, SMBs also struggle to maintain regulatory compliance such as GDPR, HIPAA and PCI-DSS. Cloud environments are ever-changing, and require constant vigilance to compliance requirements - in other words, they can really tie up resources. Businesses with limited time and resources in areas such as information security end up in scenarios where they may not have current configurations or evidence to prove compliance, subsequently paying hefty fines and receiving a black mark on their reputation for non-compliance injuries.

Despite the advantages of cloud computing, SMBs often lack the resources and expertise to effectively manage the security of their cloud environments. This exposes them to various cybersecurity threats, including data breaches, compliance violations, and unauthorized access. The lack of proper security controls and monitoring mechanisms further exacerbates these risks. Thus, there is a pressing need to implement robust security measures, such as CSPM, to safeguard SMBs' cloud infrastructure and sensitive data hosted on Azure.

Cloud computing offers significant benefits for small and medium-sized businesses smbs including scalability cost efficiency and flexibility however despite these advantages many smbs struggle with effectively managing the security of their cloud environments particularly when using platforms like Microsoft Azure this challenge exposes them to a range of cybersecurity threats such as data breaches compliance violations and unauthorized access one of the primary issues facing sm bs is the lack of resources and expertise needed to implement and maintain robust security measures within their azure cloud deployments unlike large enterprises that often have dedicated security teams and significant budgets for cybersecurity sm bs may rely on limited in house expertise or external consultants to manage their cloud security (Moyo, 2020).

This gap in security capability can lead to several vulnerabilities within the Azure environment inadequate configuration of improperly configured cloud resources can inadvertently expose sensitive data or services to the internet. Increasing the risk of unauthorized access or data breaches and lack of monitoring without proper monitoring tools and practices sm bs may struggle to detect and respond to suspicious activities or security incidents promptly compliance challenges meeting regulatory and compliance requirements such as gdpr or HIPAA can be complex and resource intensive for sm bs without specialized expertise.

To address these challenges and enhance the security posture of sm bs on azure implementing a cloud security posture management cspm solution is recommended cspm tools are designed to provide automated security monitoring compliance checks and risk assessment capabilities specific to cloud environments like azure here s how cspm can benefit SMBS:

* Continuous monitoring: cspm solutions continuously scan azure configurations and resources identifying security gaps or misconfigurations that could expose sm bs to risks
* automated remediation many CSPM platforms offer automated remediation features allowing sm bs to quickly address security issues based on predefined policies or best practices
* compliance assurance cspm tools help sm bs adhere to industry specific regulations and standards by providing compliance checks and recommendations
* centralized visibility by consolidating security monitoring and management into a single platform cspm solutions offer sm bs a comprehensive view of their azure security posture.

Implementing cspm is a proactive step towards enhancing the security of smbs cloud infrastructure and protecting sensitive data hosted on azure it not only helps identify and mitigate security risks but also enables sm bs to demonstrate a commitment to data protection and compliance.

This is where Cloud Security Posture Management (CSPM) can step in as a solution for the unknown challenges that emerge from being always-on. CSPM tools provide real-time threat monitoring, automated security issue detection and remediation.codehaus SMBs can leverage CSPM to get a centralized view of the security posture, detect and remediate misconfigurations, enforce security policies along with maintaining alignment with regulatory standards. Though, the proven efficacy of CSPM in risk mitigation and compliance enforcement is limited to SMBs on the Azure cloud.

In this study, the implementation and impact of CSPM on Microsoft Azure cloud platform is explored primarily as a means to strengthen SMB cybersecurity posture. This study attempts to identify the challenges faced by SMBs and examine how CSPM tools help in overcoming them, which can be helpful for those who want implement a security monitoring system into cloud environments of small businesses.

## **1.c. Research Questions:**

1. What are the specific security challenges faced by SMBs in managing their cloud environments on Azure?
2. How can CSPM be effectively implemented within Azure to address these security challenges?
3. What are the key factors influencing the successful adoption and implementation of CSPM among SMB on Azure?
4. What impact does the implementation of CSPM have on enhancing cybersecurity posture and regulatory compliance for SMBs operating on Azure?

## **1.d. Research Objectives:**

1. To identify and analyze the unique security challenges encountered by SMBs in managing their cloud environments on Azure.
2. To explore the implementation process of CSPM within the Azure cloud platform, focusing on configuration, integration, and optimization.
3. To assess the effectiveness of CSPM in mitigating security risks and ensuring compliance for SMBs operating on Azure.
4. To provide recommendations and best practices for SMB to enhance their cloud security posture through the adoption of CSPM on Azure.

## **1.e. Hypothesis**

This thesis has been based on the hypothesis that the implementation of CSPM tools significantly influences the security status of SMBs and mainly strengthens security assessing and compliances, and reduces the risk of cyber threats. Specifically, it is hypothesized that:In particular, it is anticipated that the following variables will be significant:

1. CSPM tools improve compliance: CSPM tools like Microsoft compliance manager are effective since it will lower the compliance level of industries regulation/standard (For Example; ISO;IEC 27001: 2013) among SMBs through compliance management and reporting.
2. CSPM tools enhance threat detection and remediation: Thanks to Microsoft Defender for Cloud complementing with Azure Policy, SMBs will be able to respond to security risks better and swifter and will manage to prevent the actual execution of cyber threats most of the time.
3. CSPM tools are crucial for resource-constrained SMBs: Since SMBs cannot afford the prime resources and employ specialists to manage the cloud security systematically, the CSPM tools are affordable and capable solution. It is assumed that these tools have a tendency of lowering the technical challenges of achieving a good security posture by enabling work and real time audits.
4. Continuous use of CSPM tools leads to sustained security improvements: In the long run, the stability of CSPM tools will result in the better position of SMBs’ cloud security as well as the capacity to modify the security for the new threats encountered and the changes in compliance that are integrated into the organization’s policies.

With these hypotheses, this thesis will shed light to the extent CSPM tools can be employed to safeguard cloud environments for SMBs and the right strategies for the implementation and utilization of CSPM tools.

## **1.f. Scope and Limitation:**

In terms of the subject, the primary concern of this thesis is to assess the capability of CSPM tools in improving the cloud security and compliance of SMBs (Pawar, 2016). The research focuses on the CSPM tools used in the cloud environment such as Microsoft Defender for Cloud, Azure Policy, Microsoft Compliance Manager in particular in scope of compliance with adopted norms closer to ISO/IEC 27001:2013 standard. The objectives of the study will seek to explore on how these tools can be used in the automation of the security assessments, in management of compliance and enhancing the security posture of SMBs.  
  
However, the research is not without limitations and may be biased in some of the following ways: First, the conclusions have been made based on a certain configuration of CSPM tools and certain cloud environment namely Microsoft Azure so it may not reveal the whole lot about the general capabilities of a variety of other tools or difficulties connected with other platforms. In the same regard, the study is limited to SMBs and thus might not offer a perfect lesson for large organizations that have more secure requirements. It also has the weakness of assuming that the SMBs under study have a minimum level of knowledge and procurement in-house or readily obtainable resources. At last, the nature of threat and emerging and contemporaneous regulatory standards, make the conclusion dependable of time and therefore a constant revision on the ever-emerging issue in cloud security could be the way forward.

## **1.g. Ethical Issues:**

Ethical considerations play a significant role in conducting research on cybersecurity and cloud computing this study adheres to ethical principles ensuring the protection of sensitive information confidentiality of data and respect for participants privacy rights ethical considerations also include transparency in data collection informed consent from participants and responsible reporting of findings additionally the study emphasizes the importance of maintaining the integrity and security of cloud environments throughout the research process thereby minimizing potential risks and vulnerabilities (Pawar, 2022).

Ethical considerations are fundamental when conducting research in cybersecurity and cloud computing this study adheres to ethical principles to ensure the protection of sensitive information maintain data confidentiality and respect participants privacy rights in the realm of cybersecurity research often involves analyzing vulnerabilities threat landscapes and security controls (Tam, 2021), it is crucial to handle such information with care to prevent unintended disclosure or misuse moreover in cloud computing research where data is stored and processed remotely researchers must be vigilant about safeguarding access to cloud based resources and data ethical considerations also encompass transparency in data collection and analysis researchers must clearly articulate the purpose of data collection,n the methods used and how the data will be utilized this transparency fosters trust and allows participants to make informed decisions about their involvement in the research informed consent is another critical ethical principle that this study upholds participants must willingly agree to participate in the research after understanding its purpose potential risks and how their data will be used respecting participants autonomy and right to withdraw from the study at any time is essential (Masoud, 2024).

Additionally responsible reporting of research findings is vital in cybersecurity and cloud computing studies researchers must accurately represent their findings and avoid sensationalizing or misinterpreting data to create false impressions transparent reporting helps ensure the credibility of research outcomes and contributes to the advancement of knowledge in the field lastly emphasizing the importance of maintaining the integrity and security of cloud environments throughout the research process is crucial researchers should implement appropriate security measures to protect data and infrastructure from potential risks and vulnerabilities this proactive approach minimizes the likelihood of data breaches or unauthorized access thereby upholding ethical standards and promoting the responsible conduct of research in cybersecurity and cloud computing by incorporating these ethical considerations into the research process this study aims to contribute meaningful insights while safeguarding the rights and well being of participants and stakeholders involved in cybersecurity and cloud computing research (Thamrongthanakit, 2023).

## **1.h.Structure of the Thesis**

This thesis is divided into six chapters which covers the various elements of the research on CSPM for SMBs.

Chapter 1: Introduction

This chapter gives an introduction to the research, and covers the following subtopics: background to the study, statement of the research problem, research objectives, hypotheses, scope and limitations of the study, and the rationale/justification of the study.

Chapter 2: Literature Review

In the literature review section, the work reviews other prior research and developments in the area of cloud security, CSPM tools, and their applicability to SMBs. This section showcases some of the main theories, frameworks and methodologies of the current study

Chapter 3: Methodology

This chapter provides the information on how the study on the CSPM tools’ effectiveness will be conducted through the following: It describes the manner in which strategies were used to meet the research goals and objectives that have been laid down.

Chapter 4: Implementation

The implementation chapter gives an account of how best the CSPM tools can be practiced within a cloud setting. It explains the implementation process of Microsoft Defender for Cloud, Azure Policy as well as Microsoft Compliance Manager for security and compliance improvements.

Chapter 5 is Results and Discussion.

This chapter also features a discussion of the results obtained in the course of the research concerning the influence of CSPM tools on the cloud security of SMBs. This entails a discourse of the problems encountered, the efficacy of the tools expounded, and the ramifications to SMBs.

Chapter 6: Conclusion

Consequently, the last chapter provides conclusions about the implication of CSPM tools for SMBs, incorporating the major findings of the research drawn throughout the book. It also highlights the directions for future studies and the possible enhancements of the approaches used in cloud security.

## **1.i. Conclusion**

By addressing each section in detail within chapter 1 introduction this proposal provides a comprehensive overview of the research topic objectives scope and ethical considerations setting the stage for the subsequent chapters.

Firstly the introduction section outlines the significance and relevance of the research topic which focuses on cybersecurity challenges faced by small and medium sized businesses sm bs in managing cloud environments particularly in microsoft azure it highlights the growing importance of cloud computing for sm bs and underscores the critical need to address security concerns within this context the research objectives are clearly defined emphasizing the aim to identify and analyze specific security vulnerabilities and risks that sm bs encounter in azure deployments these objectives provide a roadmap for the study guiding the selection of research methodologies and data collection techniques.

Furthermore the scope of the research is delineated to clarify the boundaries and focus areas of the study by specifying the target audience sm bs using azure the geographical scope potentially global but with a focus on specific regions and the types of security issues to be investigated e g data breaches compliance gaps the proposal ensures a structured and manageable research approach ethical considerations are prominently addressed throughout the proposal reflecting a commitment to protecting sensitive information ensuring participant confidentiality and upholding ethical standards in data collection and reporting by prioritizing transparency informed consent and responsible data management practices the research aims to maintain integrity and respect for participants rights.

Chapter 1 of this proposal serves as a comprehensive introduction to the research topic laying the groundwork for subsequent chapters it establishes a clear understanding of the research context objectives scope and ethical framework providing a solid basis for conducting a rigorous and ethically sound investigation into cybersecurity challenges in sm bs azure cloud environments the thorough exploration of these foundational elements sets the stage for the detailed analysis and findings that will be presented in the ensuing chapters ultimately contributing valuable insights to the field of cybersecurity and cloud computing.

# **Chapter 2 Literature reviews**

Begin by providing an overview of the current state of research on cloud security, Cloud Security Posture Management (CSPM), and cybersecurity challenges faced by small and medium-sized businesses (SMBs). Summarize key findings and trends from relevant scholarly articles, reports, and industry publications.

## **2.a Cloud Security:**

Cloud computing has its roots in several fundamental concepts and technologies. In (Ouma, 2024) study presents a specialized framework tailored to enhance secure cloud computing adoption within the kenyan banking sector addressing distinct challenges such as data abstraction multitenancy concerns and escalating phishing threats by leveraging foundational principles of identity and access management security reference architecture and an integrated intrusion detection and prevention system idps the framework offers a comprehensive solution it emphasizes regulatory compliance resilience and disaster recovery planning providing a blueprint to fortify cloud security while ensuring robust access control and proactive threat detection.

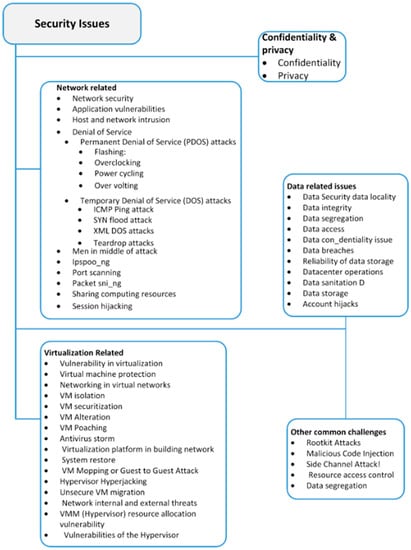


Figure 1 Cloud security issues

(Patel, 2023) Study addresses a market gap by developing an application utilizing sd ks to analyze cloud security misconfigurations and compliance focusing on iam policies as crucial parameters it aims to provide cost effective access to cloud security posture and compliance management for small and mid scale companies through api and sdk utilization ensuring efficient and economical cloud environment security.

## **2.b. CSPM:**

(Chauhan, 2023) study provides an overview of cloud technology, examines various cloud security frameworks such as COBIT5, NIST, ISO, CSA STAR, and AWS Well-Architected Framework, comparing their focus, scope, strengths, and limitations. It also analyzes prevalent cloud security issues, including inherent attack vectors and top threats, while proposing countermeasures to mitigate these challenges. In the dynamic landscape of cyber threats, the manufacturing sector's intricate Information Systems (ISs) and interconnected supply chains pose significant vulnerabilities, impacting financial, economic, and societal realms. (Del Vecchio, 2024) introduces the Theory of Cybersecurity Footprint to illustrate the interconnectedness of entities and proposes future research utilizing the Delphi method to develop a cybersecurity posture index tailored to the manufacturing industry, considering the interconnected entities' influence and specific risk weights.

CSPM tools are evolving as a critical remedy to these cybersecurity challenges in the cloud room. ( Cloud Security Alliance, 2021 )CSPM is the practice of continuously monitoring cloud infrastructure security for risks and compliance issues while automatically remediating discovered problems, as well as providing evidence-based compliance reporting. The Expensify Team's WorkmatesTools not only help organizations to find and correct misconfigurations, it also enforce pre-configured security policies on all the supply chain endpoint source code in real time.Tasks for enforcing adherence with regulatory requirements such as EULA signing can be carried out by an agent monitoring traffic going through a network device that is transparently deployed.

CSPM offers a centralized perspective of the security posture over multi-cloud environments. Subscription visibility, important so SMBs can proactively SEE where their security is lacking and take care of the gaps. The use of machine learning and big data analytics within CSPM tools can help amplify threat detection as well strengthening response capabilities, thus bolstering the overall cyber security posture (Bar-Haim, 2023).

## **2.c. SMB Cybersecurity:**

Small and medium sized businesses face unique cybersecurity challenges especially during cloud adoption limited resources expertise and budget constraints significantly impact smb cybersecurity practices the lack of dedicated it staff and financial constraints often result in insufficient investment in cybersecurity measures leaving vulnerable to cyber threats such as data breaches malware attacks and phishing scams (Pei, 2023). In (Jung, 2022) SMBS may lack the expertise to effectively configure and manage security controls in cloud environments increasing the risk of misconfigurations and security gaps the implications of these challenges are profound SMBS may struggle to implement comprehensive security measures. (Vo, 2023) leaving them exposed to cyber threats that can disrupt business operations compromise sensitive data and damage their reputation furthermore compliance with industry regulations and data protection standards becomes increasingly challenging for SMBS with limited resources and expertise tailored security solutions are essential for SMBS operating in cloud environments to address these challenges effectively these solutions should prioritize simplicity affordability and ease of implementation enabling SMBS to enhance their cybersecurity posture without imposing excessive financial or operational burdens cloud security posture management cspm tools tailored for SMBS can provide continuous monitoring automated compliance checks and remediation of security misconfigurations helping SMBS to mitigate risks and ensure regulatory compliance additionally managed security service providers mss ps specializing in serving SMBS can offer cost effective security solutions and expertise to augment sm bs cybersecurity capabilities (Kunduru, 2023).

(Gafni, 2023) introduces the universal cybersecurity footprint index ucfi as an organizational measure to quantify cybersecurity posture and assess supply chain cybersecurity risks by validating 20 elements and calculating their weights the ucfi offers organizations a practical tool to prioritize partners and mitigate cyber risks with implications for both organizational and societal cybersecurity resilience.

The rapid evolution of technology including big data infrastructure and applications has brought forth numerous opportunities and business models for entrepreneurs however many entrepreneurs and the supporting entities like policymakers and industry groups often lack preparedness for cybersecurity needs through a literature review (Saha, 2024) research underscores the imperative for further investigation to assist small businesses in safeguarding their sensitive data and client information from cyber threats mitigating risks of business shutdown.

## **2.d. Cloud Computing and SMBs:**

Cloud computing has changed the way enterprises do business by delivering unparalleled scalability, flexibility and cost reduction opportunities. The biggest beneficiaries of cloud adoption has been small and medium-sized businesses (SMBs), which all of a sudden can compete with larger enterprises without the requirement for considerable upfront investments in IT infrastructure (Armbrust et al., 2010). SMBs can tap into high-end applications and storage solutions that would be out of reach if not for the cloud. Yet, as small- and medium-sized businesses (SMBs) continue to adopt the cloud for data sharing, storage or software solutions they run into a new set of cybersecurity issues that need to be addressed if SMBs are truly going toe fully realize viele benefits of cloud computing.

This technology greatly increases the availability of powerful applications and storage solutions once relegated to enterprises, enabling collaboration even further for SMBs. This gives them powerful tools for improving operations, and possibly a competitive edge. But cloud migration is not without its problems. We have already seen that businesses might be targeted with different types of cyber threats and small business cloud security is crucial for securing your assets using the power or robustness provided by the Cloud. These challenges will be discussed in-depth later on.

## **2.e. Cybersecurity Challenges in Cloud Environments:**

One thing is clear, the cloud computing landscape does come with its fair share of new cybersecurity threats that organizations particularly small and medium-sized enterprises (SMEs) will be forced to face. Among the top concerns has to do with security, especially - and not surprisingly-data breaches. The average cost of a data breach in 2022 was $4.35 million, with cloud misconfigurations playing an important role, according to Ponemon Institute (2022). Cloud environments may be exposed to unauthorized access and data leakage due to a number of misconfigurations, like open storage buckets or improperly secured APIs. These misconfigurations are root causes of cloud security incidents, according to Verizon's 2021 Data Breach Investigations Report (DBIR), and they often arise from ignorance or neglect on the part of employees who do not see an error in their department.

Besides misconfigurations SMBs also suffer with poor change controls in their cloud environments. Consistency and Security: Because of the rapid deployment (and changes) nature that characterizes cloud operations, there might be inconsistencies and holes. For instance, security group changes (including access control lists) or alterations to cloud resource settings can introduce new attack surfaces when left unguarded. The dynamic and elastic nature of the cloud infrastructure requires around-the-clock monitoring and management to keep security settings in place. This need for continuous monitoring is especially difficult on small and medium-sized businesses (SMBs), who are normally rather scarce in cybersecurity knowledge and resources(Gartner, 2020).

n addition, the cloud shared responsibility model where a cloud service provider is responsible for some parts of its own security and places others on the customer side complicates matters. However, SMBs may find it difficult to pinpoint exactly what their own security obligations are within this model and end up with gaps in how they protect themselves. For example, cloud providers are responsible for security of the cloud infrastructure, whereas customers secure their data and manage access controls. Such a division of tasks can be complicated, leading to any vulnerabilities being overlooked if SMBs do not have solid security processes or policies.

This is further complicated by compliance to multiple regulatory standards like GDPR, HIPAA and PCI-DSS. They are also quite strict when it comes to data protection and any non-compliance can lead enormous fines among other legal complications. To adhere to the high degree of sensitivity in data handling when operating on a dynamic cloud, security controls need to be explicit and stiff across applications and can become labor-intensive for SMBs. This gap leaves organizations to rely on manual, error-prone and inefficient processes for ongoing compliance monitoring solutions.

Furthermore, the cybersecurity world is always changing with new tas well asts and vectors of those attacks appearing all the time. Because of the vast stores of data and potential for massive disruption, cloud environments represent top-tier targets to cybercriminals256 The smaller security budgets, along with less advanced protection than those of larger enterprises leaves SMBs particularly susceptible to attacks such as ransomware and phising campaigns from nation-state APT groups. The growing threat landscape requires sophisticated security solutions, as well as proactive cyber intelligence - processes that many small- and mid-sized businesses struggle to keep up-to-date.

Third, the more a cloud environment is expanded by including third party services and applications over complicates security. Every third-party service that connects to an SMBs clouds infrastructure is a potential doorway for attackers. Vetting, monitoring and incident response strategies for the security of these third-party integrations need to be put in place. These activities are costly when it comes to limited budgeted resources SMBs are usually dealing with.

The above is by no means a comprehensive list, and cloud computing offers far more benefits than risks; but these are just some of the cybersecurity challenges SMBs face in their transition to cloud-based app deployment. These challenges, categorized as follows: managing cloud misconfiguration, enabling sufficient change control, understanding and responding to shared security responsibilities, maintaining regulatory compliance in public clouds (she called out financial being most difficult), keeping pace with rapidly evolving threats - hell she even included third-party integrations. Addressing these hurdles involves a blend of sophisticated security tools, broad policies, persistent vigilance and most importantly an understanding of the unique cyber-security requirements and capabilities pertaining to SMBs.

## **2.f. CSPM in Azure Cloud Platform:**

Azure is no exceptional here: Azure CSPM (Cloud Security Posture Management) helps secure and make compliant the cloud environment ideal for small-mid sized businesses. Microsoft Azure - The complete cloud service from Microsoft, comes with a range of native CSPM tools that help in monitoring managing and securing the resources at optimal ways for the it resource (Loaiza Enriquez, 2021).

Azure Security Center as part of CSPM in Azure This is a robust solution that allows firms to conduct continuous security assessment and provides advanced threat protection in order for organizations to identify vulnerabilities, assess threats and risks as well as effectively respond all at real-time. Here, the Azure Security Center gives you a single view of protection status for all your services in AZure to take care from one dashboard itself if necessary for such SMB. This centralized method only eases the burden of managing security and guarantees that safety policies are enforced uniformly concealed in your entire cloud atmosphere (Suriya, 2024).

Azure Security Center uses machine learning and AI to increase threat detection and response abilities. Azure Safety Center reviews the huge data-flows produced by actions in the cloud and examines them. It can identify patterns that suggest security threats since it can be unusual login or resource usage attempts, odd network communications, or modifications to a resource’s configuration. This is critical for SMBs because they lack the capacity to devote the time and effort required to be continuously reactive without such a remedy. The machine learning model used by Azure Safety Center and AI helps it to be predictively reactive. It obtains better at identifying dangers to the SMBs it serves as time passes (Coppola, 2024).

Azure Safety Center sends warnings to allow businesses to address the issue before anything occurs. It might be previous Microsoft emails or shutting certain devices down.. Azure also provides another solution, CSPM, which is Azure’s hallmark service that supports policy examination, control, and compliance, aids businesses in administering cloud security. Few resources can probe Azure Security Center to address risks. Azure Safety Center sends alerts and advice on how to tackle the problem. Hence, the firm does not have to be very responsive..yaml video(actions).. baseline hearings are checked by.federal, corporate, and private compliance laws.. Detail failure entitled zone, root variables.

In addition to all its advantages, Azure's CSPM tools also work together with other native and third-party security solutions for an efficient cloud security approach. As an example, you could onboard the Security Information and Event Management System (SIEM) Azure Sentinel with a more comprehensive feature-set that is also integrated with the Microsoft-flavored intrusion detection capability of Azure as depicted in this architecture diagram. This integration allows small and mid-size businesses (SMBs) to tie together security events from multiple sources, gain greater visibility into their cybersecurity posture, and respond more efficiently. Integrated solutions like these enable SMBs to implement a layered cloud security strategy, which tackles aspects of the problem from different angles (Riley, 2017).

Azure Security Center also helps to promote continued security by featuring a secure score feature. This feature gives a quantitative score to represent the security posture of an organization taking in view how well they have implemented the recommended and necessary security controls. Small and medium businesses can leverage the secure score to pinpoint where they are weakest, determine which security increases to make first - as well as follow along in time how these rescores go. It also offers a secure score and suggestions for actionable recommendations to improve overall security - making it more approachable by small businesses looking to understand and enact industry best practices.

This makes CSPM one of the most flexible, scalable Azure tools available to smaller and midsized businesses. Scale security and compliance protection with your businessAzure Security Center scales as your resources scale, no matter how large. Being able to tailor security policies and configurations down to the specific business need, SMBs can continue effectively protect their cloud-based apps as they grow.

CSPM in Azure can deliver a holistic solution for cloud security and compliance to the customers of our services. With tools such as Azure Security Center, SMBs can find continuous security monitoring; proactive threat detection with automated remediation and compliance across the board. These abilities enable SMBs to tackle some of the factors in cloud security for their environment from procurement, so they can get all benefits of Cloud computing without compromising Security will be ensured.

## **2.g. Challenges and Limitations of CSPM:**

CSPM in the Real WorldOf course, as good and generally understandable is CSPM, this approach has its limitations and pitfalls. How to stay in compliance with your infrastructure is one of these challenges, and first-time installation & integration process (CSPM tools). Small to Medium businesses have difficulty in configuring these tools as per the specific security requirements and also integrating with existing security solutions (Ghosh, 2024).

Moreover, even though CSPM tools offer automated fix capabilities human oversight and intervention are necessary. As some false-positives, as well s true-alerts will occur it is always good to have manual review and actions back into the system. In addition, as CSPM is an operation-like exercise run in loops all day long and every day of the year, alerts created by any system produce a large number alarms; this may cause alert fatigue to security teams. (Wang).

2.h Importance of Compliance and Regulatory Standards:

Regulatory compliance are a must for security purposes., mainly focused on GDPR, HIPAA and PCI-DSS.. especially SMBs. These require strong data protection, privacy safeguards to ensure that organizations are responsible in processing such sensitive data responsibly securely. If you ignore these norms, it may also attract huge financial fines and lawsuits in addition to reputational damage of an organization. Hence, for SMBs looking to secure their assets and create customer/partner credibility; non-compliance is more than a legal liability but also an important business mandate.

Such as General Data Protection Regulation (GDPR) is highly comprehensive data protection law that applies to all organizations handling the personal data of EU (European Union) citizens, irrespective of its location. GDPR requires companies to track only key information and practice strong security over the entire process of data collection, processing, and storage. Failure to comply with GDPR can result in fines up to 4% of a company's annual global turnover or €20 million, whichever is higher. SMBs will be crippled by such fines, highlighting the importance of matching GDPR standards.

For example, the Health Insurance Portability and Accountability Act (HIPAA) establishes rules for protecting health information in the United States. HIPAA compliance - all companies in the healthcare sector including SMBs which have to deal with data related a patient. The rule mandates administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information (ePHI). HIPAA violations carry steep fines and even criminal charges, so compliance is vital for SMBs dealing with healthcare data.

Another critical standard is the Payment Card Industry Data Security Standard (PCI-DSS) which applies to any organization that processes, stores or transmits credit card information. PCI-DSS is a global standard that includes measures to ensure the security of cardholder data and minimize the risk of fraud. For businesses in the retail and e-commerce sector, ensuring compliance with PCI-DSS allows small to medium-sized SMBs like yours to continue processing credit card payments without paying hefty fines, higher transaction fees or being permanently banned from transacting on services.

Ensuring organizations adhere to these and other regulatory standards is where Cloud Security Posture Management (CSPM) tools come into play. CSPM tools keep an eye on configurations in the cloud and make sure that all of them are up to par based on security & compliance policy. The intelligence provided by CSPM tools into the security posture of cloud environments in real-time allows SMBs to quickly detect and remediate compliance violations.

Detailed compliance reports: CSPM tools provide detailed compliance reports. The information the reports produce neatly show an organizations coverage percentage and non-compliant areas encouraging controllers to take any necessary corrective actions. This proves to be of high significance that SMBs can now show their compliance commitment in audits withregulators and auditors. Automated compliance reporting reduces the administrative burden on SMBs, allowing them to get back to running their business with an assurance that they remain compliant.

In addition, CSPM tools provide out-of-the-box compliance templates and frameworks based on regulatory standards. However, these templates make the process of setting security controls and policies to comply with certain regulations easier. As an example, a GDPR compliance template may be offered by results of CSPM tool which will consist the precise set up for locking personal data or a HIPAA templates that aligns with directive on requirements protecting PHI. These templates enable SMBs to quickly and effectively address associated security controls, in order to maintain compliance.

Research indicates that companies with stronger compliance programs do bring up the rear less at prospecting data breaches or fix penalties. Organizations with a greater focus on compliance and use of CSPM tools experience less frequent security incidents, according to a report by PwC (2022) The strong relationship further highlights the value of maintaining compliance - as a security best practice, not just legal obligation.

To sum up, regulatory compliance with GDPR, HIPAA, and PCI-DSS is vital for SMBs to safeguard their sensitive data, mitigate possible legal and financial repercussions, and earn their stakeholders’ trust. CSPM tools integrate compliance management in cloud environments and guarantee continuous monitoring, automated reporting, and predefined compliance templates. As such, SMBs can employ CSPM tools to guarantee the ongoing compliance of their cloud configurations to satisfy regulatory requirements and, in this manner, further protect themselves from data breaches and strengthen their security stance.

## **2.i. Gaps Analysis:**

The literature review reveals several gaps and areas for further research in the field of cloud security cloud security posture management cspm and smb cybersecurity (Mansfield-Devine, 2023). Firstly there is a need for more comprehensive studies examining the effectiveness of cspm solutions in mitigating security risks and ensuring compliance specifically tailored to the needs and constraints of small and medium sized businesses sm bs research could focus on evaluating the scalability affordability and ease of implementation of cspm tools for smbs considering their limited resources and expertise in cybersecurity. There is a lack of research on the impact of emerging technologies such as AI ML and blockchain on cloud security and CSPM (Johnsen, 2021). Future studies could explore how these technologies can enhance cspm capabilities automate threat detection and response and improve overall cybersecurity posture in cloud environments there is a need for more in depth investigations into the unique cybersecurity challenges faced by sm bs during cloud adoption particularly in terms of data privacy compliance with industry regulation and protection against advanced cyber threats. Research could also explore the role of managed security service providers in offering tailored security solutions and expertise to SMBs operating in cloud environments. There is limited research on the human factors and organizational behavior aspects of cloud security and CSPM. Future studies could examine how employee awareness, training, and organizational culture impact cloud security practices and the effectiveness of CSPM implementation.

With the increasing complexity and interconnectivity of cloud environments and supply chains, there is a need for research on supply chain cybersecurity and its implications for SMB. Studies could investigate how vulnerabilities in interconnected supply chains pose risks to SMB cloud security and explore strategies for mitigating these risks effectively.

## **2.f Conclusions**

In conclusion, the literature review encapsulates the pivotal role of cloud security posture management cspm within the cybersecurity landscape of cloud networks with a particular emphasis on its implications for small and medium-sized businesses sm bs through an extensive exploration of existing literature several key insights have been unearthed firstly the significance of cspm in mitigating security risks and ensuring compliance across cloud environments has been underscored however alongside its importance the review also sheds light on the myriad challenges inherent in cspm implementation especially concerning sm bs these challenges encompass the complexities of configuration limited visibility into cloud infrastructures and resource constraints. Despite these obstacles emerging trends and best practices in cspm offer promising avenues for enhancing security posture such as the integration of machine learning and automation technologies adoption of cloud native security solutions and proactive risk management strategies moreover the review emphasizes the crucial role of regulatory compliance and governance frameworks like nist iso and csa star in guiding organizations particularly sm bs towards adherence to regulatory requirements looking ahead the literature points towards a multitude of future research opportunities including the development of tailored cspm frameworks for sm bs exploration of cloud native security solutions and examination of the impact of emerging technologies on cspm efficacy ultimately by addressing the identified challenges and leveraging emerging trends sm bs can fortify their security posture and navigate the dynamic landscape of cloud environments with greater resilience and confidence.

# **Chapter 3 Research Methodology**

## **3.a Research Design**

This study adopts a mixed methods approach involving both qualitative and quantitative techniques qualitative methods such as interviews will be utilized to explore the unique security challenges faced by SMBS in managing their cloud environments on azure and to gain insights into CSPM implementation processes quantitative methods including surveys and data analysis will be employed to assess the effectiveness of cspm in mitigating security risks and ensuring compliance for SMBS operating on azure.

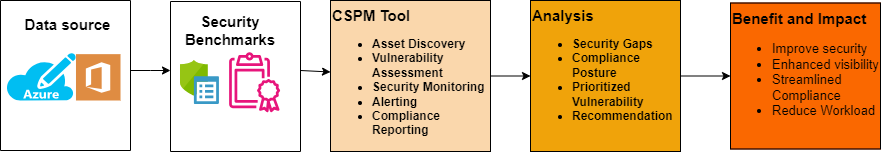


Figure 2 System design

The system design in figure 2 represent the significance of Cloud Security Posture Management (CSPM) in cybersecurity for cloud networks, particularly in the context of SMBs. It outlines the data sources, security benchmarks, CSPM tools, analysis processes, and the resulting benefits and impact, all of which are crucial components in understanding and implementing CSPM within SMBs. The integration with Microsoft Azure and Microsoft 365 emphasizes the relevance of CSPM within cloud environments commonly utilized by SMBs. This diagram effectively captures the essence of the study on CSPM in SMB business cybersecurity.

This research outlines a step by step approach to evaluate the value of cloud security posture management cspm in securing a small and medium sized business s smb cloud network built on microsoft azure and microsoft 365.

## **3.b Research Flow charts**

1. Start with Problem Statement: The flowchart should start with the definition of the research problem or the question that your thesis is going to answer.
2. Literature Review: The following activity in the flow chart should be the identification of existing literature sources wherein you collate some data on CSPM tools and cloud security of SMBs.
3. Hypothesis Formulation: Next to the literature review, the flowchart needs to contain the creation of the research hypothesis because of the existing gaps in the literature.
4. Methodology: The flowchart should then split into the flow of design and methodology of doing the research. As part of the prep work, CSPM tools, the data acquisition techniques, and the analytical techniques to be used are chosen.
5. Implementation: Secondly, warfare-illustrate how the identified CSPM tools will be practically implemented in the chosen cloud environment as described in chapter 4.
6. Data Analysis: The next step that the flowchart could then go to should be the analysis of the data that would have been collected from the implementation phase. This entails considering the effects of the CSPM tools both on security position and compliance.
7. Results and Discussion: It is important to highlight on how the findings are presented with regards to the research objectives and hypothesis in the flowchart.
8. Conclusion and Future Work: Last of them, the flowchart should end with the integration of the study results and the future research implications.

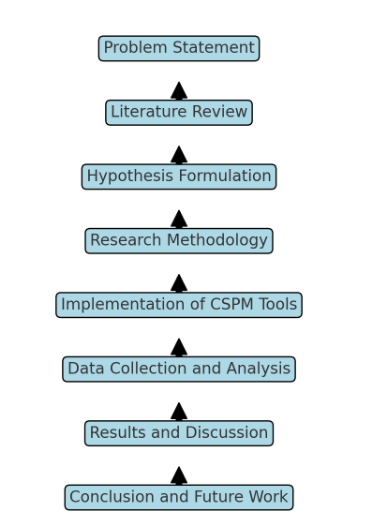


Figure 3 Research Flowchart

## **3.c Data Collection Methods**

The first step involves collecting data from two primary sources your cloud environment and relevant security benchmarks.

In Cloud environment data will leverage azure management tools and API to gather details on deployed resources like virtual machines storage and databases this data will also include the security configuration settings associated with these resources microsoft 365 security and reporting tools will be used to extract data on utilized services exchange one drive share point and their configurations

In security benchmarks compliance requirements identifying relevant security benchmarks for azure and microsoft 365 is crucial examples include the microsoft security baseline for azure and microsoft 365 security defaults best practices if your SMB operates in a specific industry you may also need to consider industry specific compliance standards like hipaa for healthcare or PCI DSS for credit card processing.

## **3.d Selecting and implementing a CSPM tool:**

After collecting data the next step is to choose and implement a cspm tool this tool should seamlessly integrate with azure and microsoft 365 for efficient data collection and analysis.

The implementation of cloud security posture management CSPM within your azure and microsoft 365 environment entails several essential functionalities to ensure robust security and compliance measures are upheld seamlessly firstly an automated cloud asset discovery and inventory capability is paramount this feature enables the tool to autonomously identify and catalog all cloud resources across your azure and microsoft 365 platforms providing a comprehensive overview of your digital assets moreover a robust vulnerability assessment and misconfiguration detection capability are indispensable the cspm tool should continuously scan and evaluate your cloud resources for vulnerabilities and misconfigurations in security settings by proactively identifying potential weaknesses organizations can preemptively mitigate security risks and fortify their cloud environments against cyber threats furthermore continuous security posture monitoring and alerting mechanisms are critical components of an effective cspm solution real time monitoring ensures that any deviations from the desired security posture are promptly detected allowing for swift action to address potential security threats or suspicious activities timely alerts enable organizations to respond proactively and mitigate security incidents before they escalate additionally compliance reporting functionalities are essential for demonstrating adherence to chosen security benchmarks and industry standards the cspm tool should generate comprehensive reports that provide insights into compliance status facilitating audits and regulatory assessments with ease lastly remediation recommendations play a pivotal role in enhancing security resilience based on identified security gaps and vulnerabilities the cspm tool should offer actionable recommendations for remediation these recommendations empower organizations to implement appropriate security measures and address identified issues effectively thereby bolstering overall security posture and resilience in cloud environments.

## **3.e Data Analysis and Security Posture Assessment: Evaluating Your Cloud Security**

With the data collected and the cspm tool in place we can now analyze the information to assess your overall cloud security posture the cspm tool will be used to analyze data from azure microsoft 365 and the chosen security benchmarks this analysis will help identify.

* Security Gaps and Misconfigurations: The tool will pinpoint weaknesses in your cloud environment's security configuration.
* Compliance Posture: The analysis will assess how well your cloud network adheres to chosen security benchmarks and compliance standards.
* Prioritized Vulnerabilities: Based on severity, exploitability, and potential business impact, vulnerabilities will be prioritized for remediation.

## **3.f Recommendations and Action Plan: Taking Action to Improve Security**

Following the analysis a comprehensive action plan will be developed to strengthen your smb s cloud security posture this plan will prioritize remediation efforts for critical vulnerabilities and misconfigurations identified by the cspm tool additionally the plan will recommend implementing security best practices from the chosen security benchmarks finally an ongoing monitoring and improvement process will be established to ensure the continued security of your cloud environment.

## **3.g Evaluation and Impact Assessment: Measuring the Benefits of CSPM**

Once the recommendations are implemented the effectiveness of the cspm tool and the improved security posture will be monitored this evaluation will involve measuring the impact of cspm on security metrics like the number of vulnerabilities security incidents and compliance adherence finally the overall benefits of cspm for the smb will be assessed including improved security enhanced visibility into your cloud environment streamlined compliance processes and a reduced workload for your it staff.

## **3.h Conclusions**

Throughout the research process it is imperative to remain cognizant of the unique requirements and constraints inherent to small and medium sized business smb environments this entails considering factors such as limited resources expertise and budgetary constraints when designing the research methodology and interpreting findings additionally comprehensive documentation of the research methodology is essential to ensure transparency reproducibility and accountability in the study s outcomes ethical considerations including data privacy confidentiality and informed consent must be carefully addressed throughout all stages of data collection and analysis to uphold ethical standards and protect participant rights by incorporating these additional considerations into the research framework the study can effectively address the specific needs and challenges faced by sm bs while ensuring the integrity and ethical rigor of the research process

By following this research methodology, this research effectively assesses the value of CSPM in securing your SMB's cloud network built on Azure and Microsoft 365. This research will provide valuable insights into how CSPM tools can enhance your cloud security posture and protect your business from cyber threats.

# **Chapter 4 Implementation**

## **4.1 Introduction**

Small & Medium sized business (SMBs) are increasingly using cloud services, and this has implications for the field of cybersecurity in terms of threat and opportunity. This is a process where organizations transfer the structures for their IT operations to the cloud and therefore gain increased scalability, flexibility and lower costs. Though, this transition also brings new and sophisticated security issues that require proper measures to ensure security of the data and adherence to the standards of the various industries. As a result, there is a need to find solutions that would help to overcome these challenges and Cloud Security Posture Management or CSPM turns into a necessary solution that uses automated methods for perpetuous monitoring, evaluation, and optimization of the cloud environments security.

This chapter is dedicated to presenting the main aspects of approach CSPM using the practical consideration of the SMBs and reflecting on how the tools and methods related to CSPM can contribute to improving the cloud security and compliance. CSPM, therefore, is not the technical process of deploying security technologies but a strategic process of ensuring that security initiatives are in harmony with the organization objectives as well as the legal frameworks. CSPM provides an opportunity for SMBs to avoid threats by determining security issues systematically, checking compliance with the regulations automatically, and enforcing security regulations to maintain the integrity of cloud operations.

This process’s primary goals include the evaluation of potential threats and risks and the adherence to standards in the implementation of CSPM initiatives to enhance the cloud environment’s security posture. From this chapter, the reader will understand the goals, data sources, security standards, CSPM solutions, analysis procedures, and a plan for CSPM. Hence, by offering a detailed outline of the CSPM procedure in this chapter, it is expected to prepare SMBs to face the challenges of CS and build an effective and compliant CS infrastructure.

In the next sections, we will review the data sources that give the essential information about the resistance of the cloud environments, namely, Azure Security Center, Microsoft 365 Security Centre, and Log Analytics. We will also look at the CIS Controls, the NIST Framework for CSPM, as well as the ISO/IEC 27001, which offer a framework that acts as a benchmark for CSPM implementation. The chapter will then consider the tools such as CSPM that can be used to automate the security and compliance assessments including Microsoft Defender for Cloud, Azure policy, and Microsoft Compliance Manager. Last but not the least; the method that has been discussed here for the analysis processes and the implementation steps will be thoroughly described in this section, which delineates the procedure in an easy to follow step-by-step manner to help the SMBs to adopt the CSPM for improving cloud security.

At the end of this chapter, will acquire an appreciation and understanding of CSPM as a means for ensuring compliance, monitoring of the cloud environment and risk management for the SMB company. This knowledge is important to either organisations that are willing to take advantage of cloud computing and at the same time ensure that the have strong security and compliance measures.

## **4.2 Data Sources**

Effective cspm implementation relies on various data sources that provide critical insights into the security posture of cloud environments the key data sources used in this implementation are:

### **4.2.1 Azure Security Center**

The azure security center provides security recommendations and compliance information for resources hosted on microsoft azure it offers a unified view of security across azure services helping to identify potential vulnerabilities and areas for improvement.

### **4.2.2 Microsoft 365 Security Center**

The microsoft 365 security center offers insights into the security posture of microsoft 365 services including email share point one drive and teams it provides detailed reports and alerts on security incidents and compliance status.

### **4.2.3 Log Analytics**

Log analytics collects and analyzes logs from various sources enabling the detection of security incidents and anomalies it integrates with other azure services to provide a comprehensive view of security events and trends.

## **4.3 Security Benchmarks**

Several established security benchmarks guide the CSPM implementation, ensuring that security measures align with industry best practices and standards. The key benchmarks used are:

### **4.3.1 ISO/IEC 27001**

ISO/IEC 27001 is an international standard for information security management. It outlines a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability.

## **4.4 CSPM Tools**

The implementation of cloud security posture management cspm solutions involved the use of several specialized tools designed to automate security assessments and compliance checks these tools played a crucial role in enhancing the overall security posture of the companys cloud environment by providing continuous monitoring real-time insights and automated remediation capabilities the key cspm tools employed in this implementation are Microsoft defender for cloud azure policy and Microsoft compliance manager.

Microsoft defender for cloud is a comprehensive security management tool that monitors and manages the security of cloud resources it provides real time insights into the security posture of the cloud environment offering detailed alerts and recommendations to address potential vulnerabilities and compliance issues by leveraging Microsoft Defender for cloud solutions was able to gain a unified view of their security status across all azure services and microsoft 365 applications this tool facilitated the identification of critical security risks and enabled proactive measures to mitigate these threats thereby improving the overall security and compliance of the cloud infrastructure.

Azure policy is another vital tool used in the cspm implementation azure policy enforces organizational standards and assesses compliance at scale ensuring that security policies are consistently applied across the entire cloud environment one of the key features of azure policy is its ability to automatically remediate non compliant resources which significantly reduces the manual effort required to maintain compliance by defining and assigning policies that encapsulate security best practices and compliance requirements azure policy helped solutions maintain a robust security posture and ensure adherence to industry standards and regulatory requirements.

Microsoft compliance manager is an essential tool for managing compliance activities and meeting data protection regulations it provides a centralized platform for tracking compliance status offering a comprehensive view of the organization s compliance with various industry standards and regulations microsoft compliance manager generates detailed reports that are crucial for regulatory audits and internal assessments by using this tool was able to streamline their compliance management processes ensure ongoing adherence to regulatory requirements and effectively manage compliance activities across their cloud environment.

## **4.5 Implementation Steps**

The implementation of the cspm solution involved several detailed steps each contributing to the overall security and compliance of the cloud environment the key implementation steps are.

### **Set Up Microsoft Defender for Cloud**

Microsoft defender for cloud was enabled on the azure subscription and microsoft 365 services this step ensured continuous monitoring and real time insights into the security posture of all cloud resources.

#### **Step 1: Enable Microsoft Defender for Cloud on Azure Subscription**

To enable microsoft defender for cloud on your azure subscription start by navigating to the azure portal at https portal azure com once you re logged in locate the left hand menu and select microsoft defender for cloud next click on the get started button to begin the setup process you will then be prompted to choose the subscription you wish to enable microsoft defender for cloud on after selecting the appropriate subscription click upgrade to activate the service this process will enable enhanced security features for your chosen subscription helping to protect your cloud resources from threats.

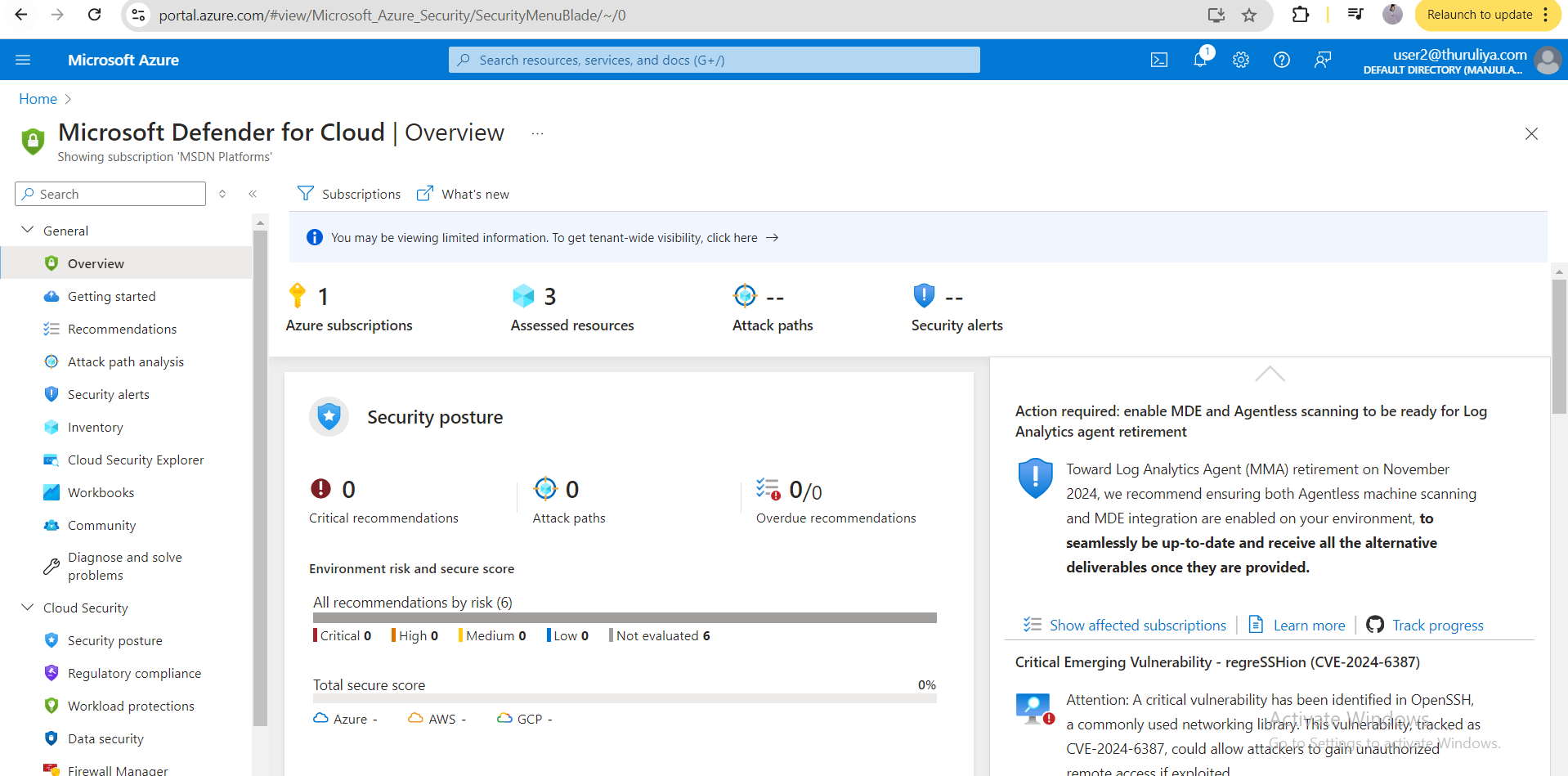


Figure 4 Microsoft defender for cloud

#### **Step 2: Enable Microsoft Defender for Cloud on Microsoft 365**

To configure microsoft defender for cloud apps within the microsoft 365 security center begin by navigating to the microsoft 365 security center at https security microsoft com once inside the portal locate the left hand menu and select settings followed by microsoft 365 defender within the settings find the defender for cloud apps section to enable this feature simply turn on the microsoft defender for cloud apps toggle this action integrates advanced cloud security into your microsoft 365 environment providing comprehensive protection and enhanced visibility into cloud app activities.

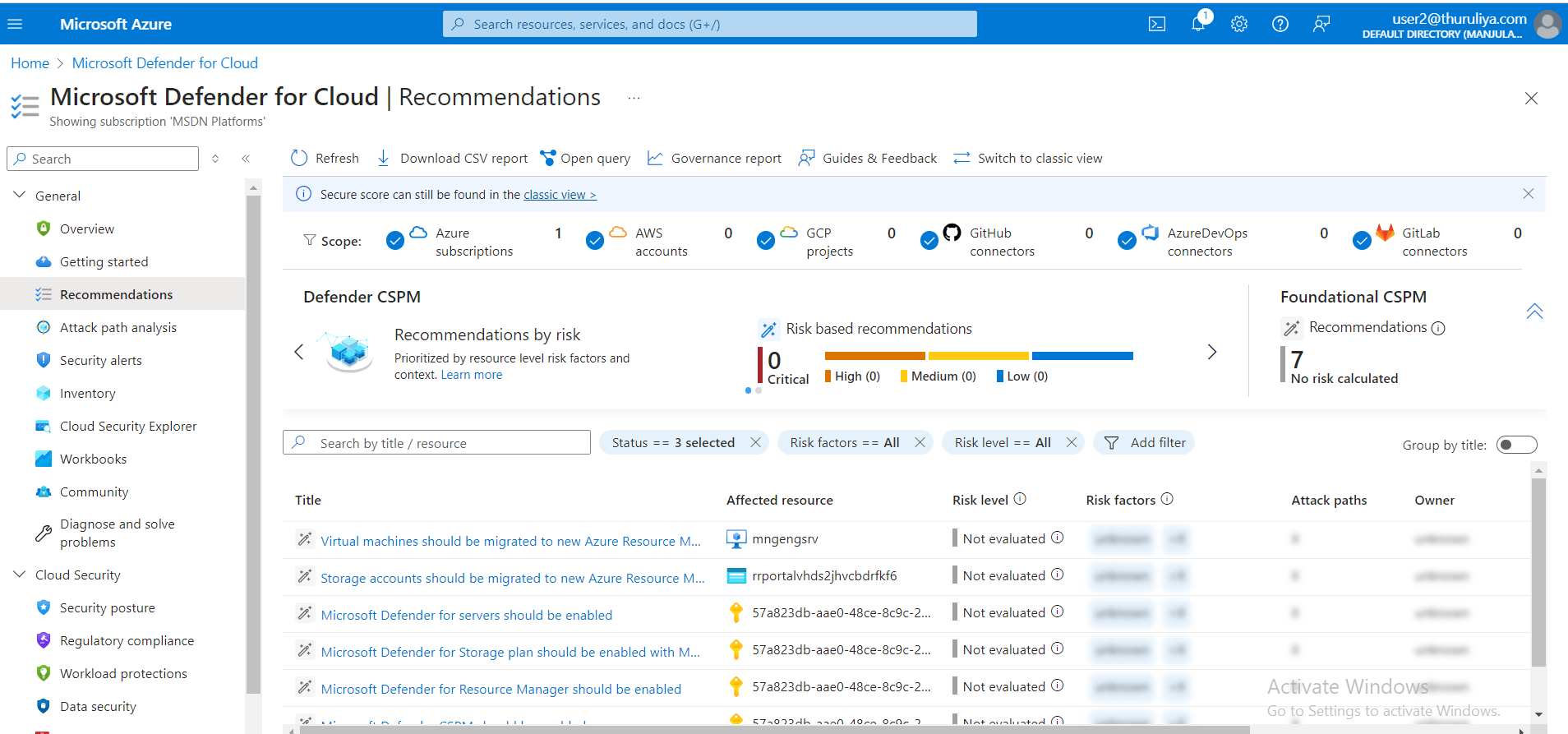


Figure 5 Microsoft Defender for cloud and recommendation

### **2. Configure Azure Policy**

#### **Step 1: Define Policies**

To enforce security best practices using azure policy start by navigating to the azure portal and selecting policy from the left hand menu in the policy section click on definitions to access a comprehensive list of available policy definitions to locate specific security-related policies such as those that audit virtual machines not using managed disks use the search bar by entering relevant keywords once you ve found the appropriate policy select it and click assign this action will apply the policy to your selected scope helping to ensure that your azure environment adheres to security best practices.

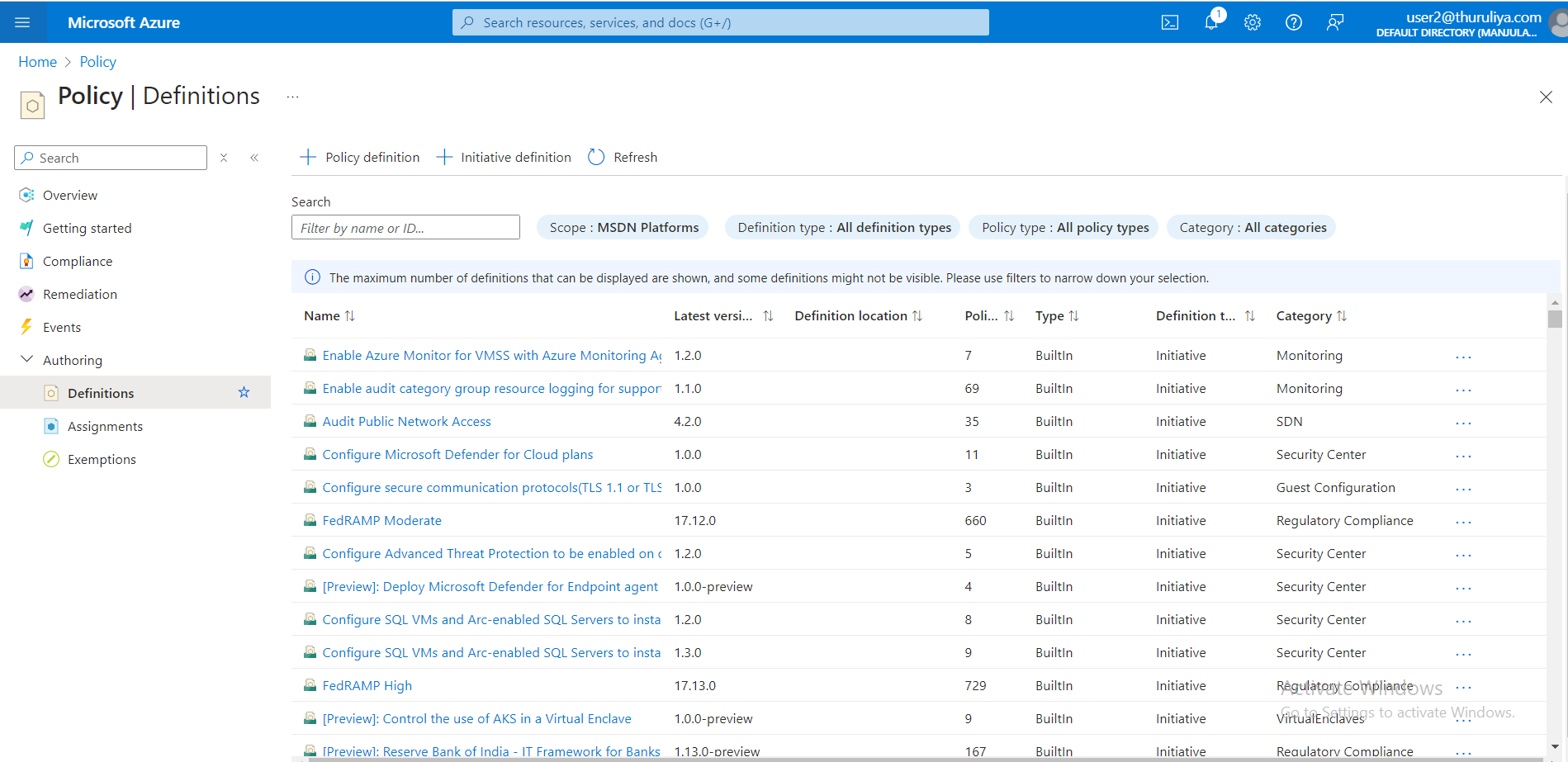


Figure 6 Policy definitions

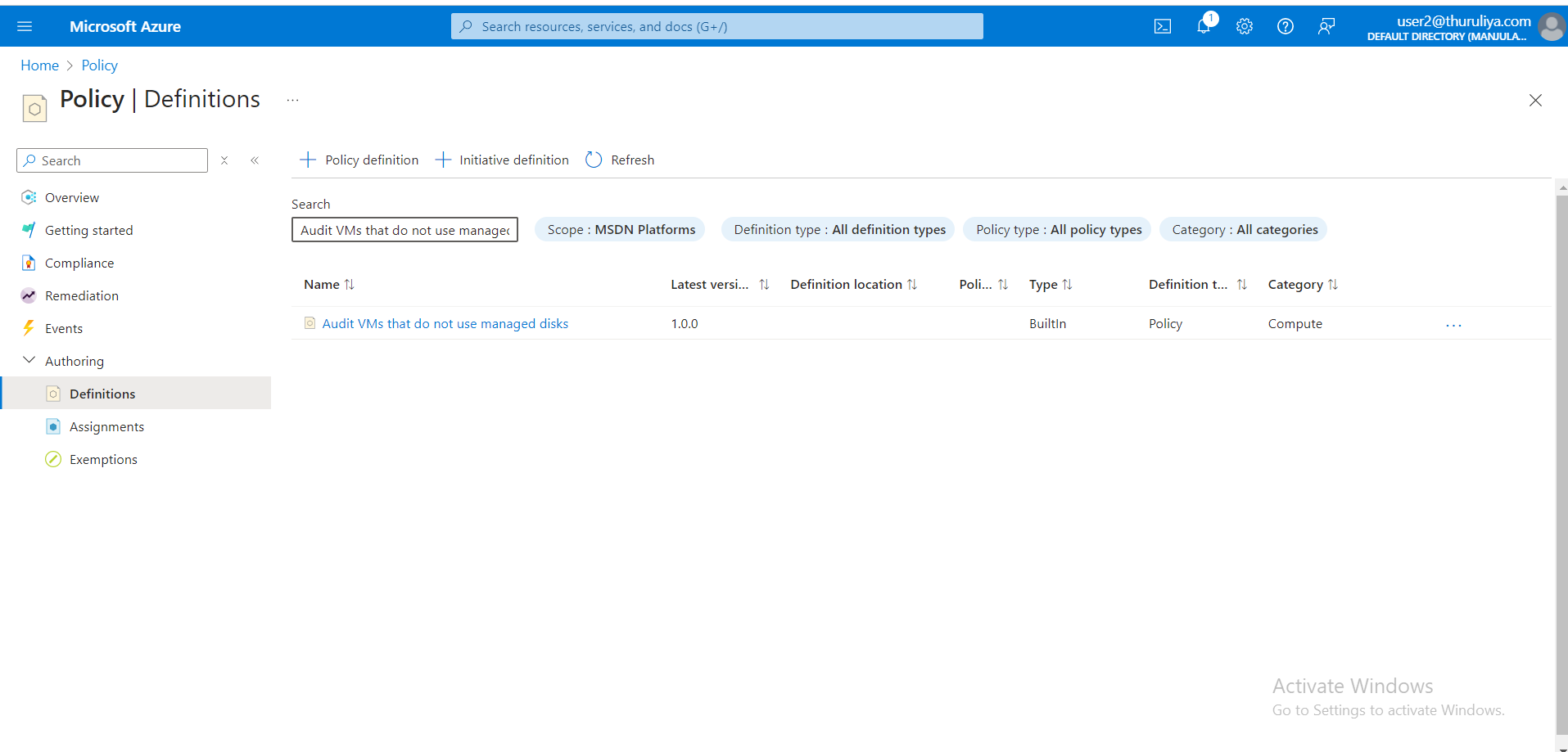


Figure 7 Select policy

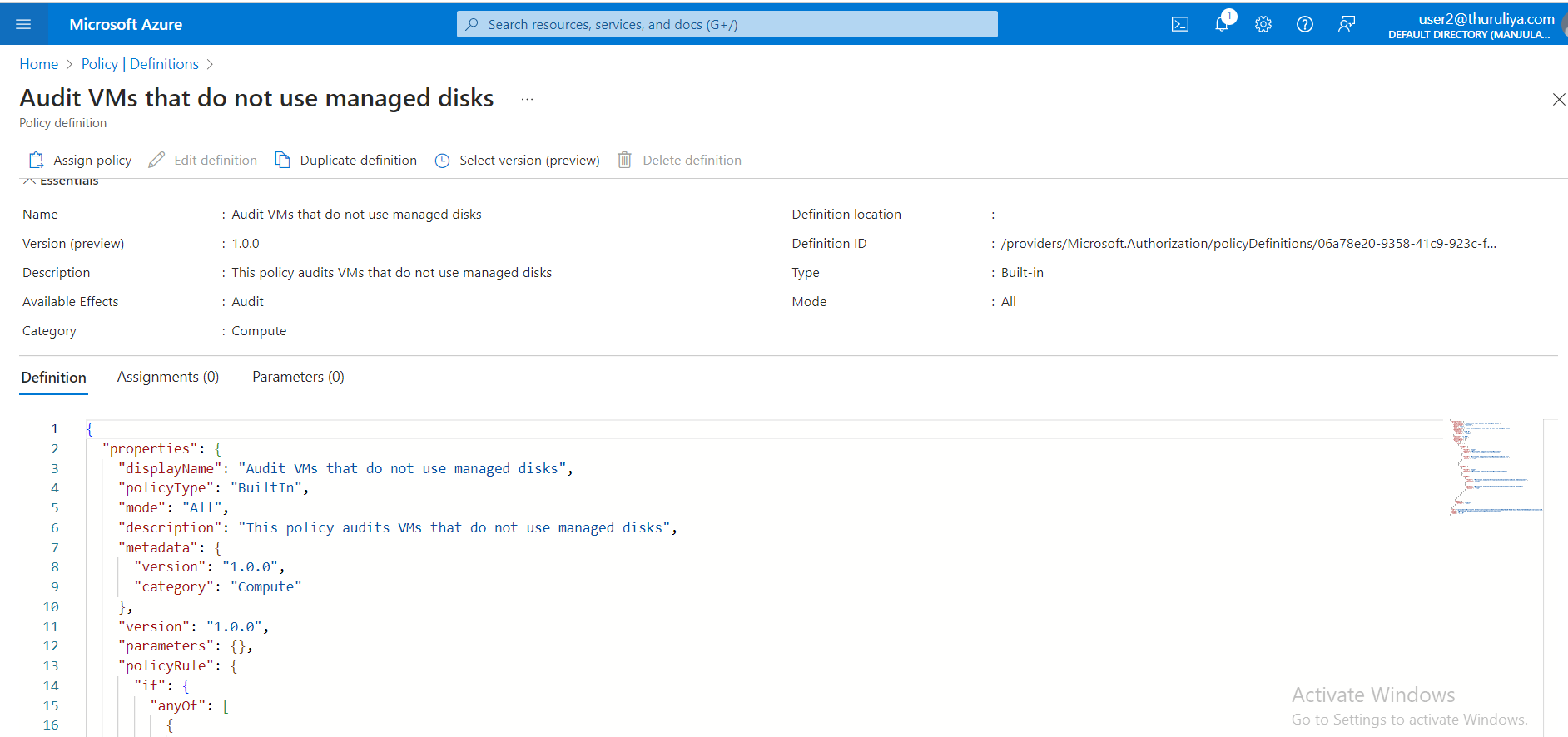


Figure 8 assign policy

#### **Step 2: Assign Policies**

In the process of assigning a policy within the azure portal navigate to the assign policy pane where we will need to select the appropriate scope for the policy assignment such as a specific subscription or resource group if the chosen policy requires configuration of parameters ensure these settings are adjusted according to your compliance or security requirements once the configuration is complete proceed by clicking review create to review your settings and then finalize the process by clicking create to assign the policy this assignment ensures that the specified policy is actively enforced within the selected scope contributing to a more secure and compliant azure environment.

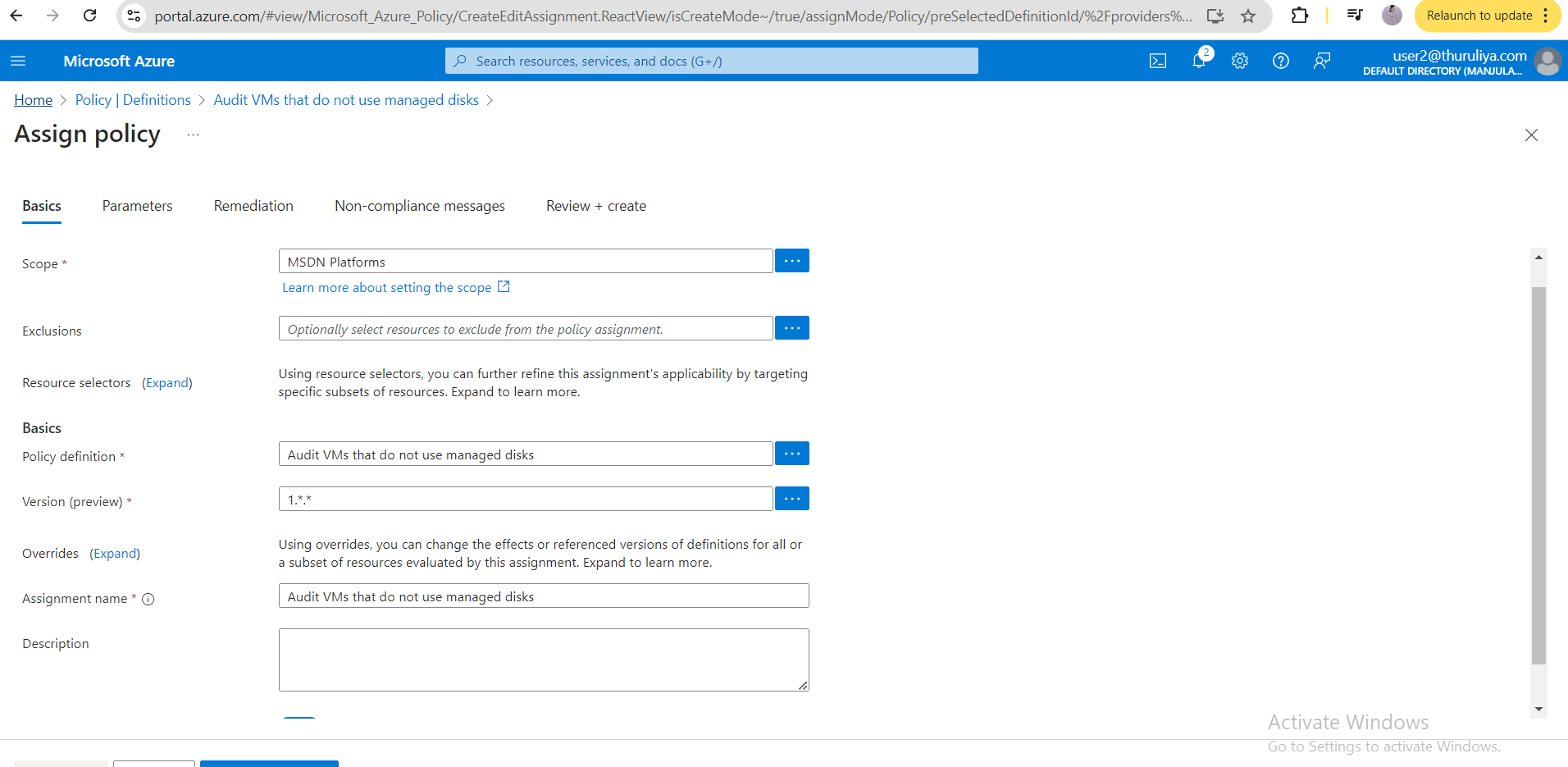


Figure 9 Assign Policy pane

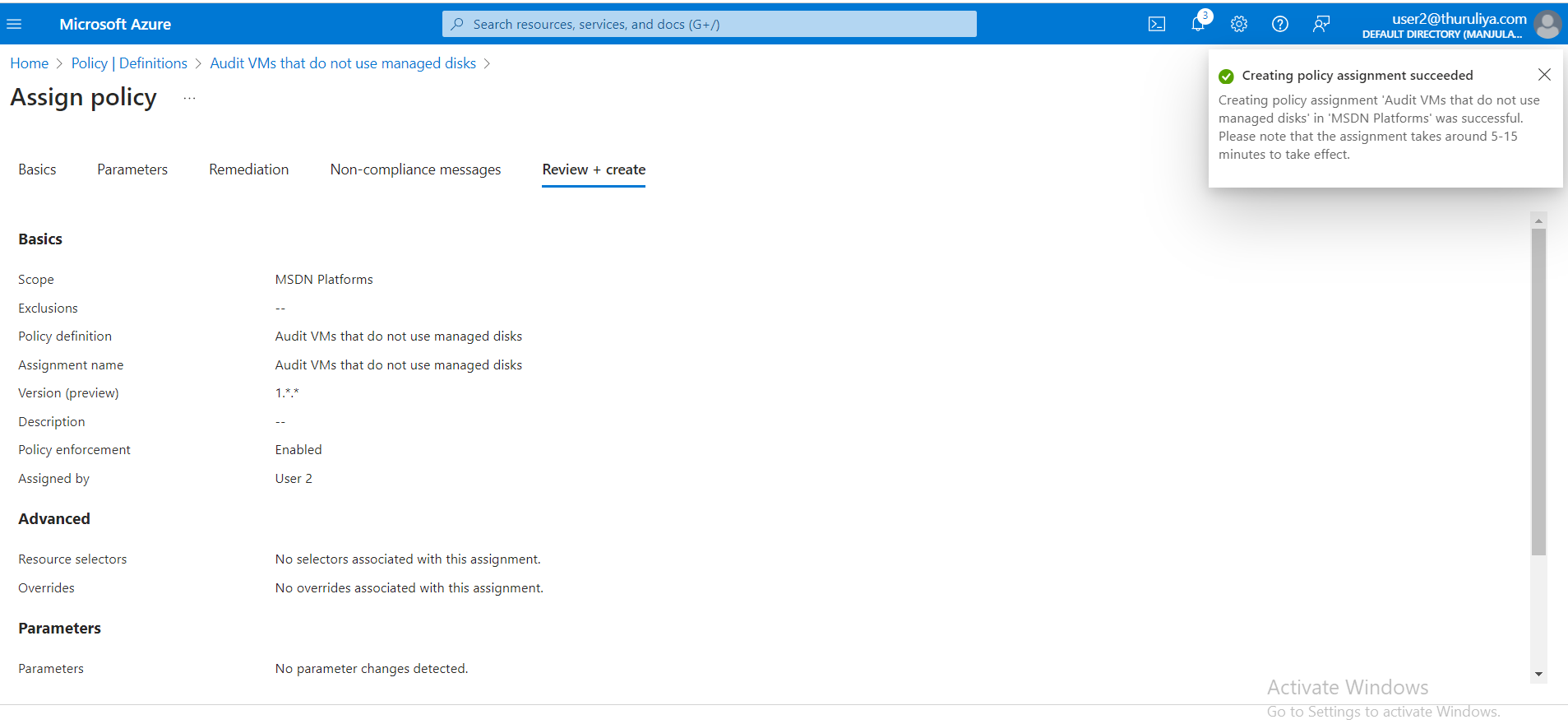


Figure 10 Assign policy

### **3. Enable Log Analytics**

#### **Step 1: Create a Log Analytics Workspace**

To establish a log analytics workspace in azure begin by searching for log analytics workspaces using the top search bar within the azure portal once located select add to initiate the creation of a new workspace you will then be prompted to provide essential details including the subscription under which the workspace will reside the associated resource group a unique name for the workspace and the desired region for deployment after entering the required information click review create to validate your configurations finally complete the process by clicking create which will provision the log analytics workspace enabling you to collect analyze and gain insights from your azure resource data.

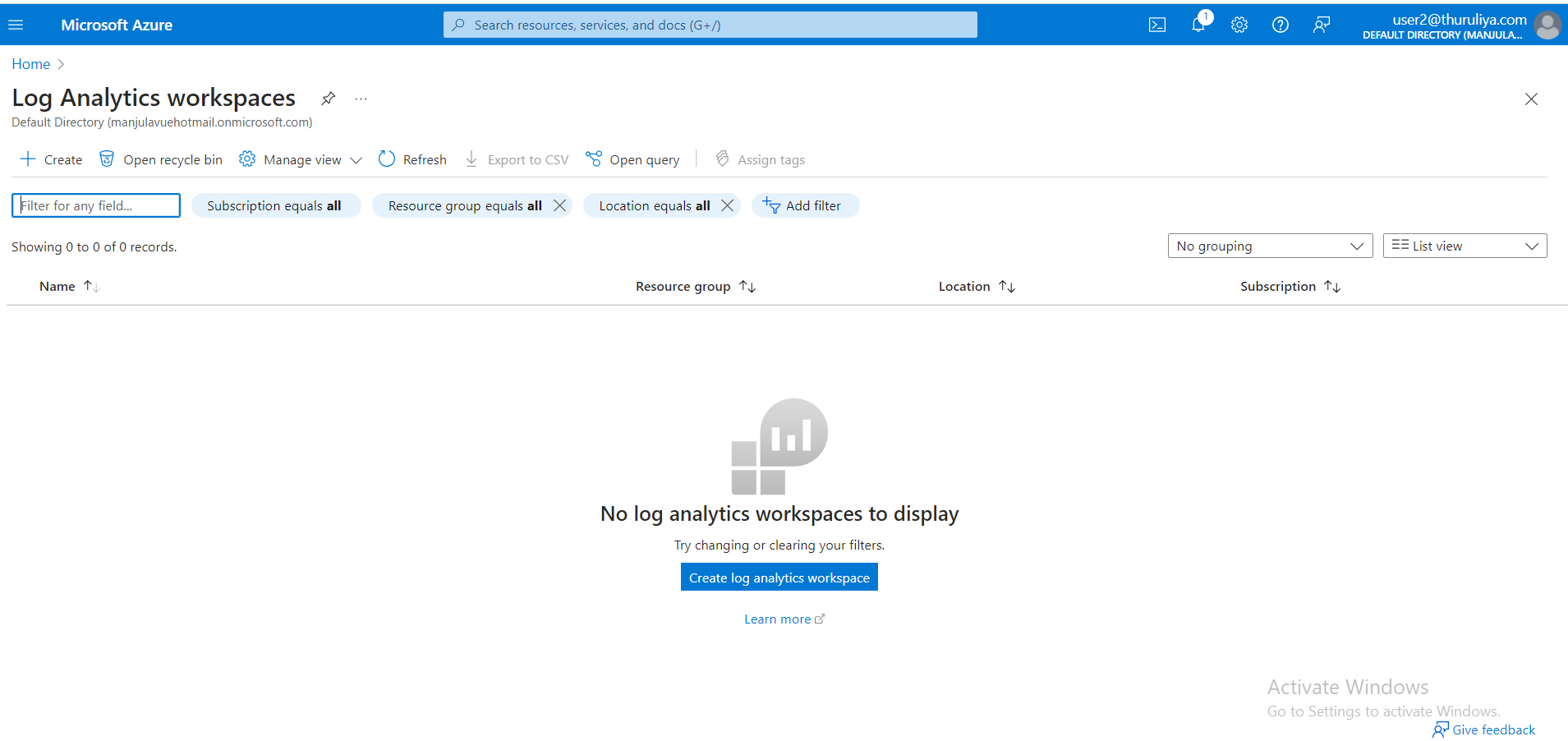


Figure 11 log Analytics workspaces

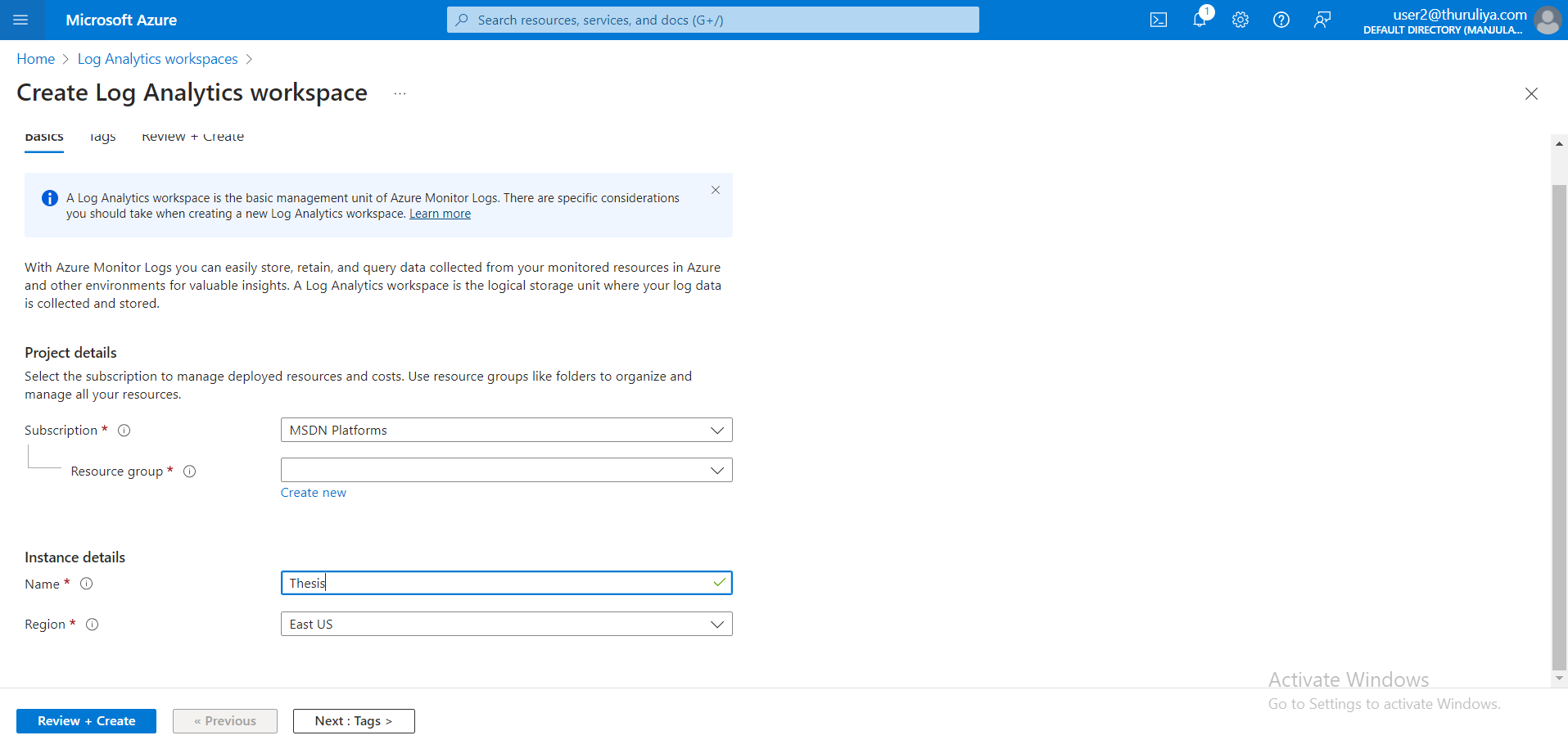


Figure 12 Create Log Analytics workspace

#### **Step 2: Link Azure Resources to Log Analytics**

To configure data collection for microsoft defender for cloud in the azure portal first navigate to microsoft defender for cloud from the left hand menu select environment settings to access the configuration options choose the subscription you want to configure and then click on data collection in the data collection settings select the log analytics workspace that you wish to use for storing and analyzing security data once you have made your selection click save to apply the settings this action ensures that security related data from Microsoft defender for cloud is systematically collected and stored in the specified log analytics workspace for further analysis and monitoring.

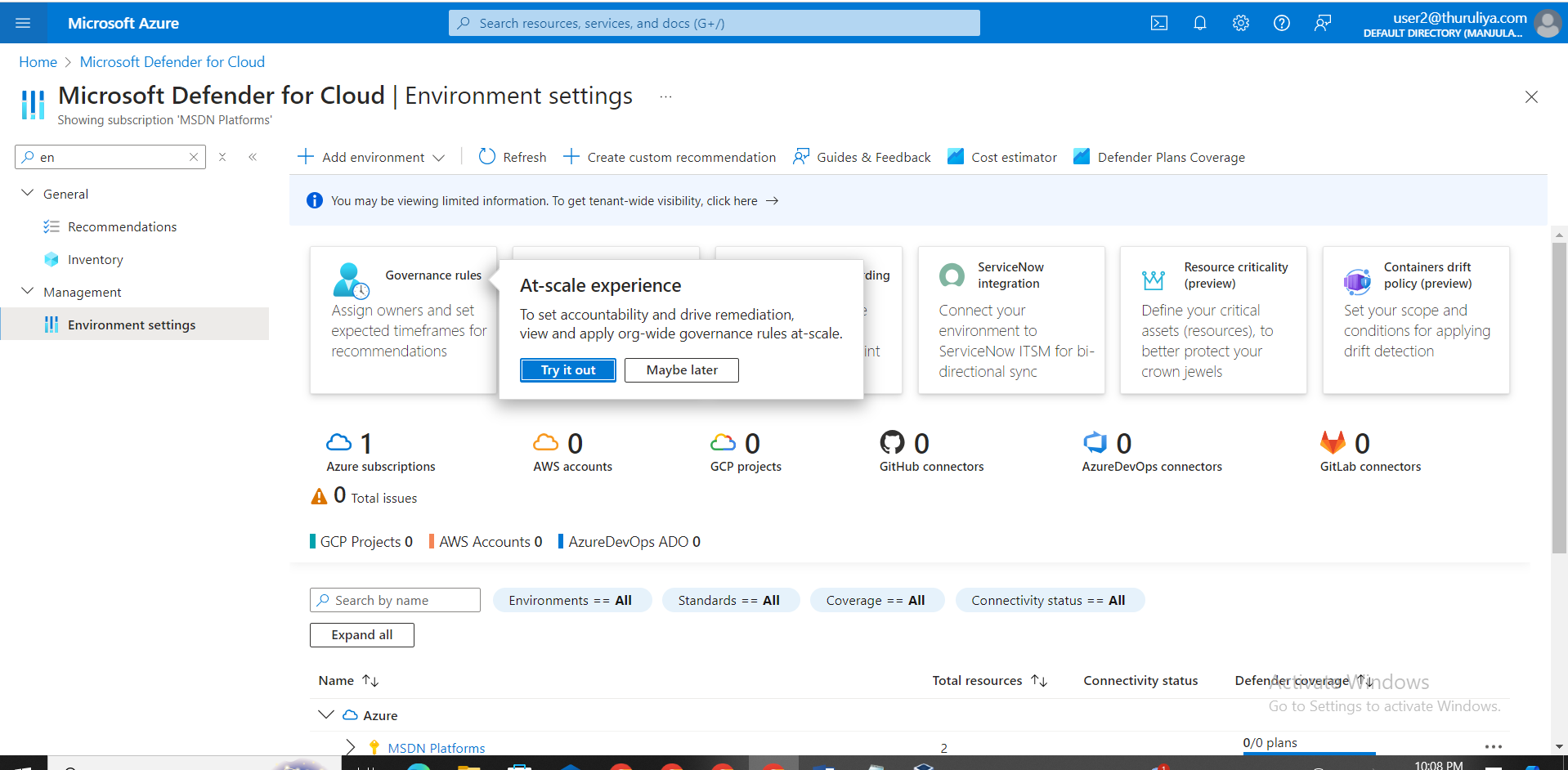


Figure 13 Environment setting

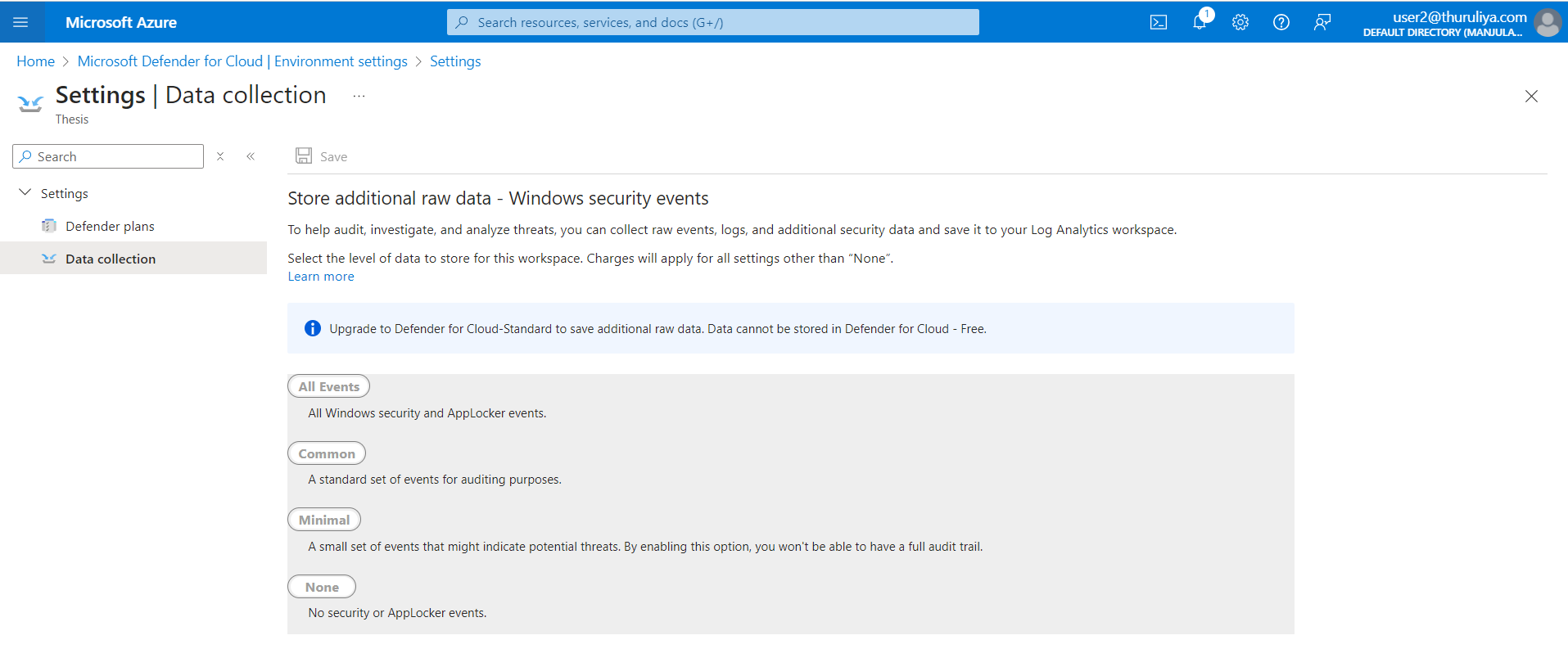


Figure 14 data collection setting

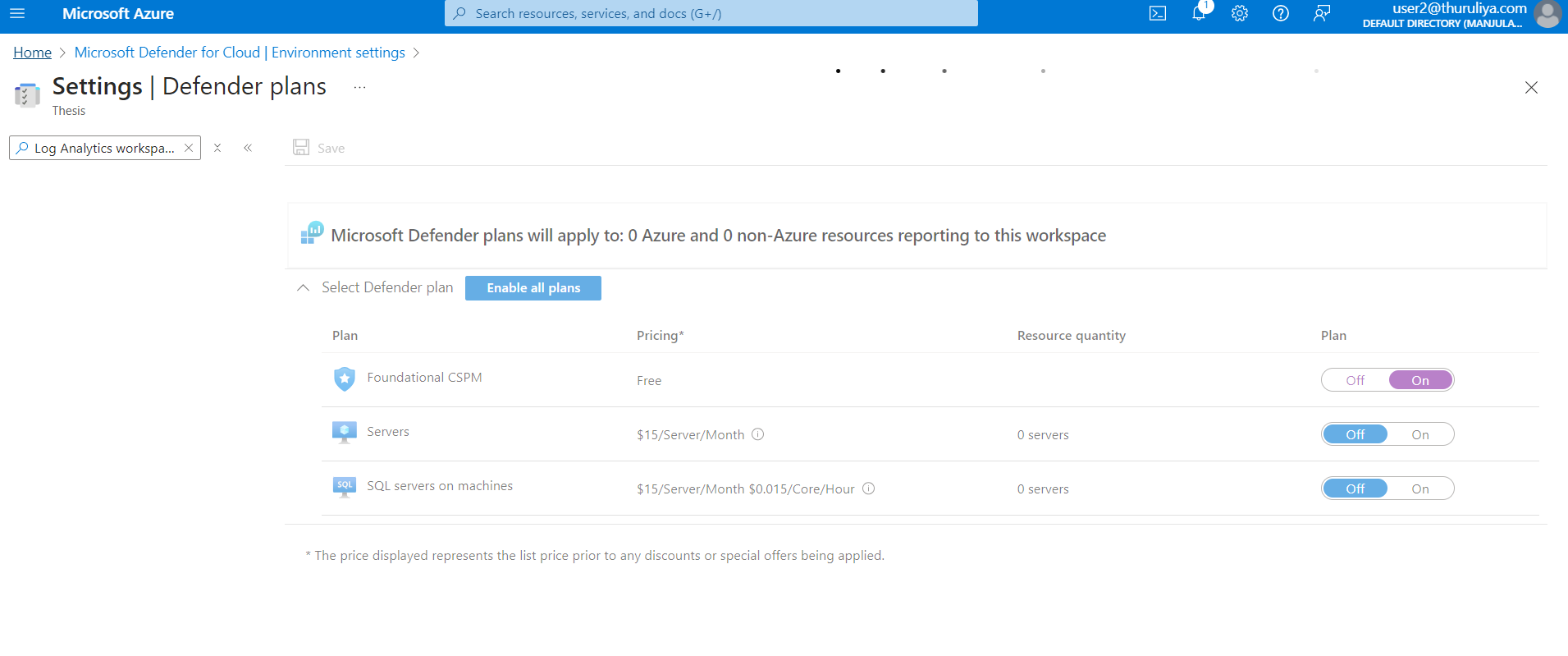


Figure 15 Defender Plans

#### **Step 3: Configure Data Collection**

Azure monitor combined with log analytics provides a powerful solution for collecting analyzing and acting on telemetry data from both azure and on premises environments to enable this start by setting up diagnostic settings for your azure resources such as virtual machines storage accounts and key vaults navigate to the specific resource in the azure portal go to diagnostic settings and enable diagnostics configure the settings to send logs to an existing log analytics workspace storage account or event hub once diagnostics are enabled you can navigate to your log analytics workspaces within the azure portal to query and analyze the collected logs this integrated approach allows for comprehensive monitoring and insights across your cloud infrastructure enhancing visibility and operational efficiency

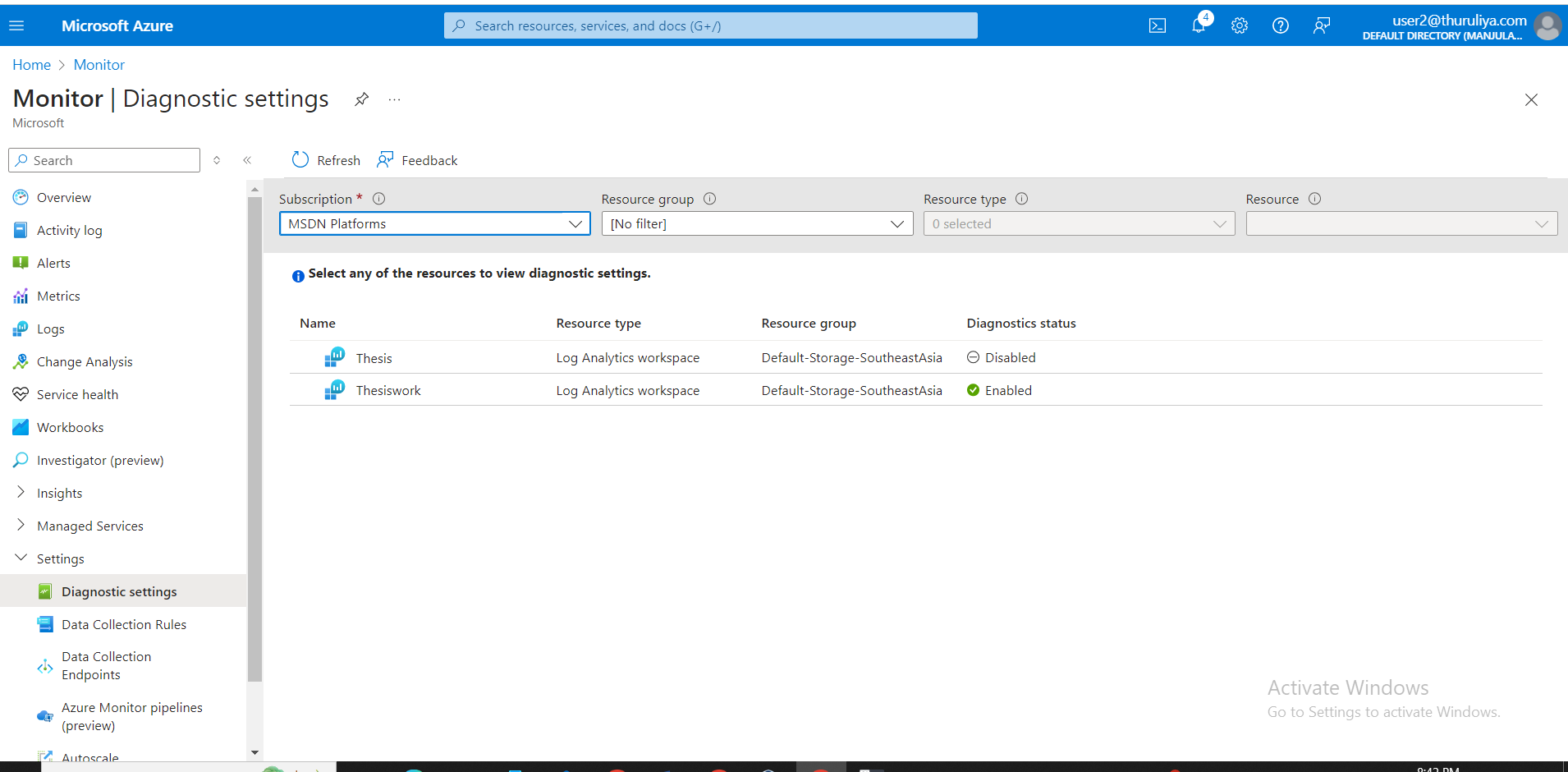


Figure 16 Enable dianostic setting for log

### **4. Use Compliance Manager**

#### **Step 1: Access Compliance Manager**

To access Compliance Manager begin by navigating to the microsoft compliance center at https compliance microsoft com once there locate the left hand menu and select compliance manager this tool provides a centralized platform for managing compliance across your microsoft 365 environment offering insights and actions to help meet regulatory requirements and improve your organization s compliance posture

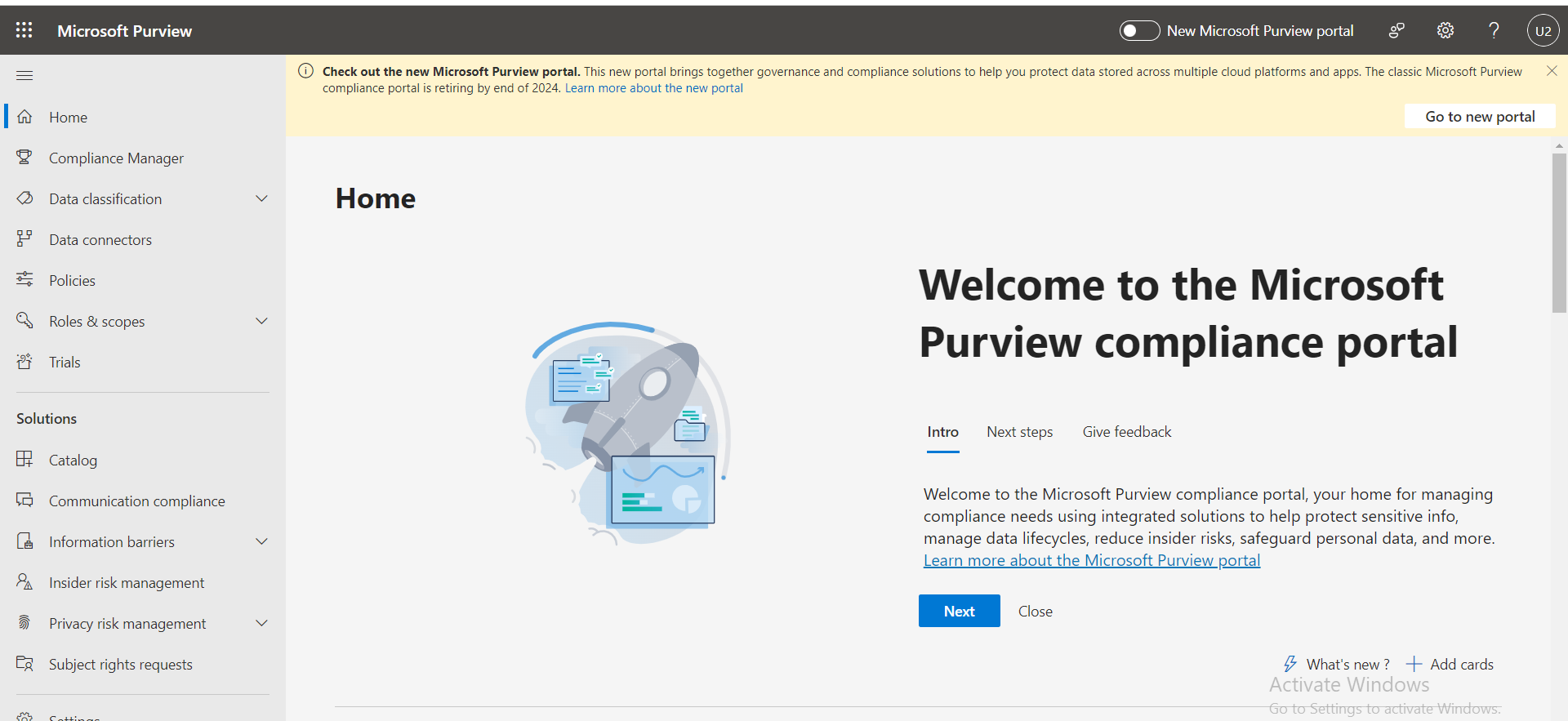


Figure 17 compliance management dashboard

#### **Step 2: Set Up Compliance Manager**

On the compliance manager dashboard navigate to the assessments section and click on add assessment to begin the process of creating a new compliance assessment select the template that corresponds to the specific industry standard or regulation your organization needs to adhere to such as gdpr or iso iec 27001 after selecting the appropriate template fill in the necessary details and click next to proceed you will then be prompted to assign roles and responsibilities to relevant team members ensuring that the compliance tasks are managed effectively once all details are entered click create assessment to finalize the process initiating a structured approach to tracking and managing compliance efforts within your organization

For ISO 27001

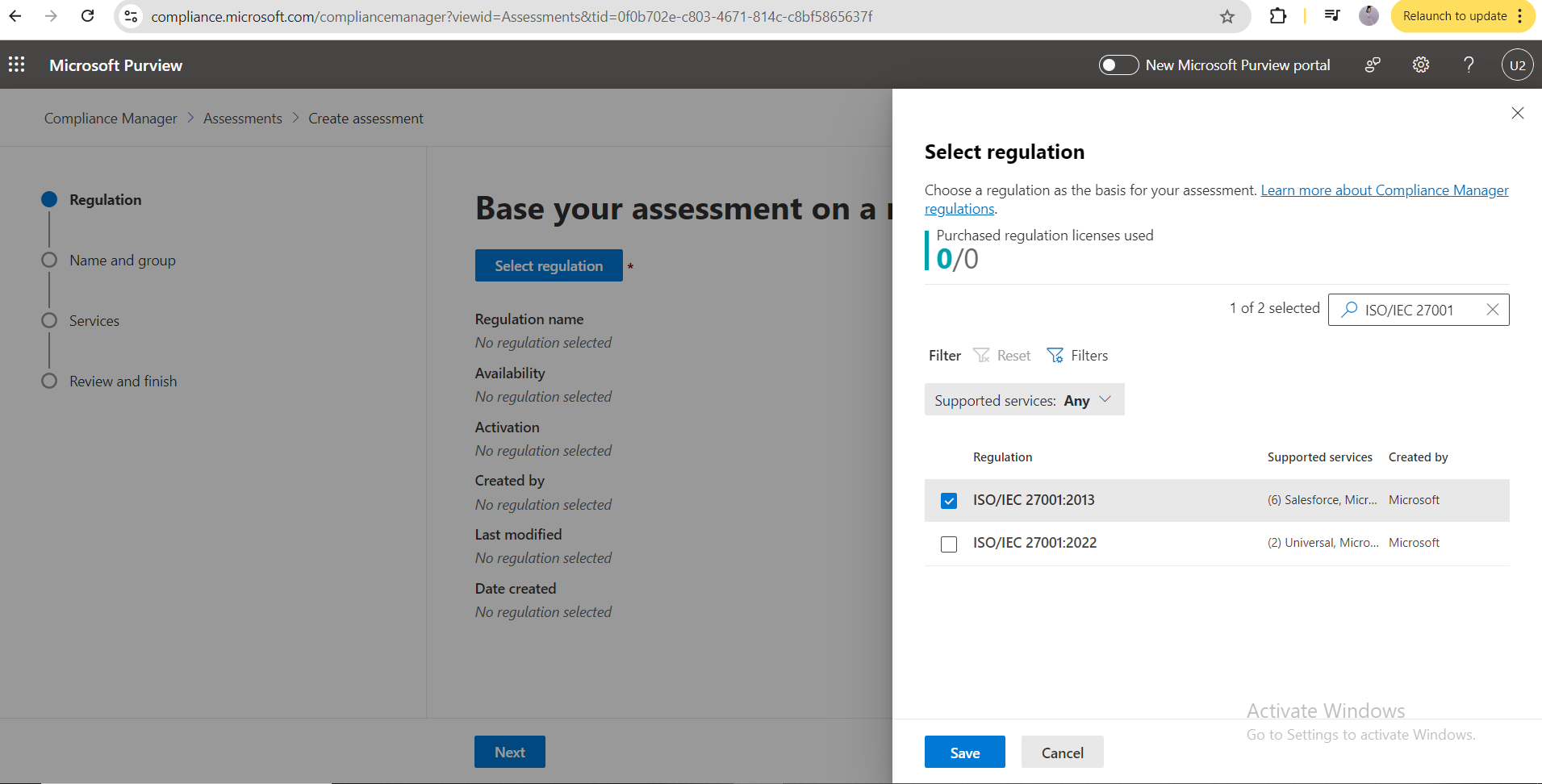


Figure 18 Select iso 27001

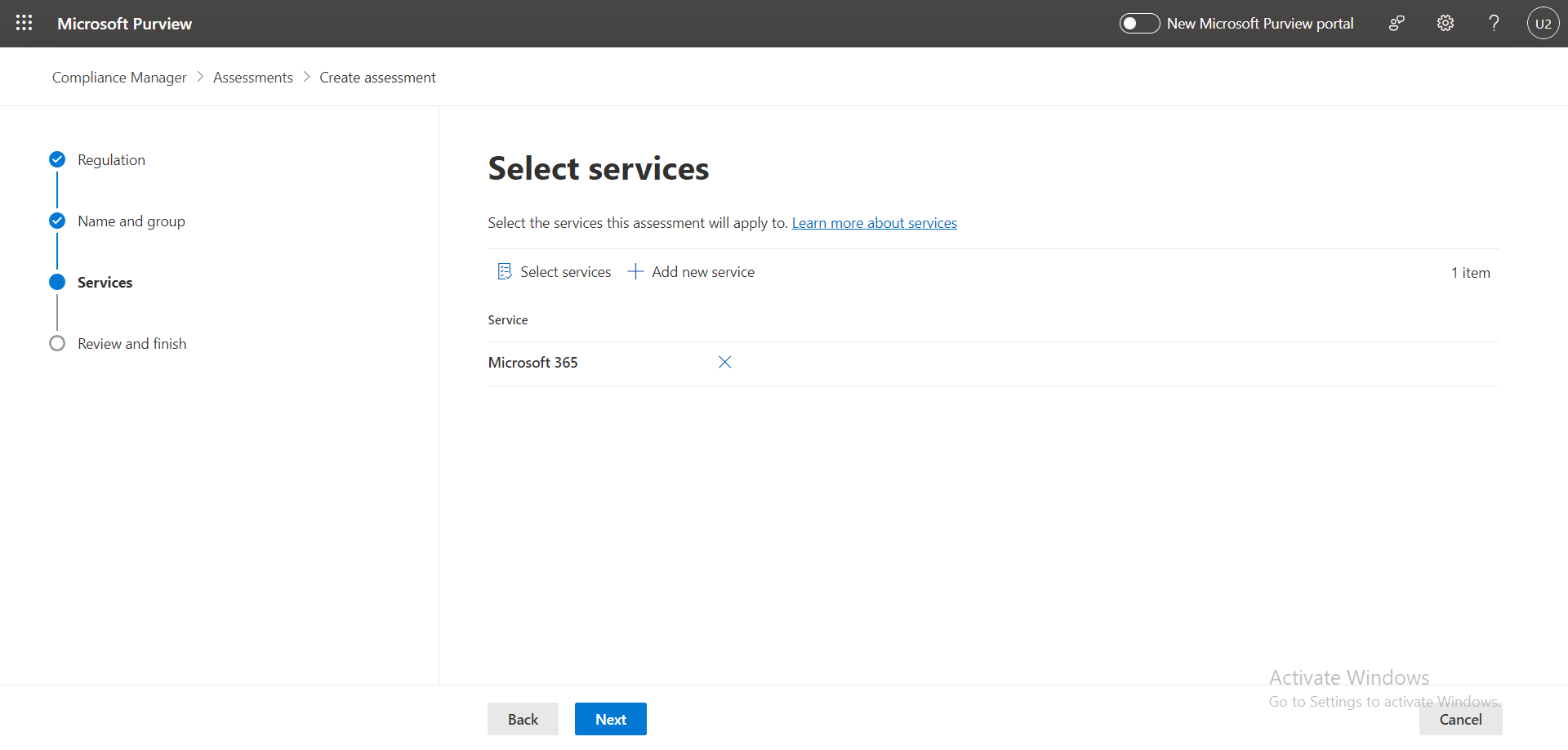


Figure 19 Microsoft 365 as services

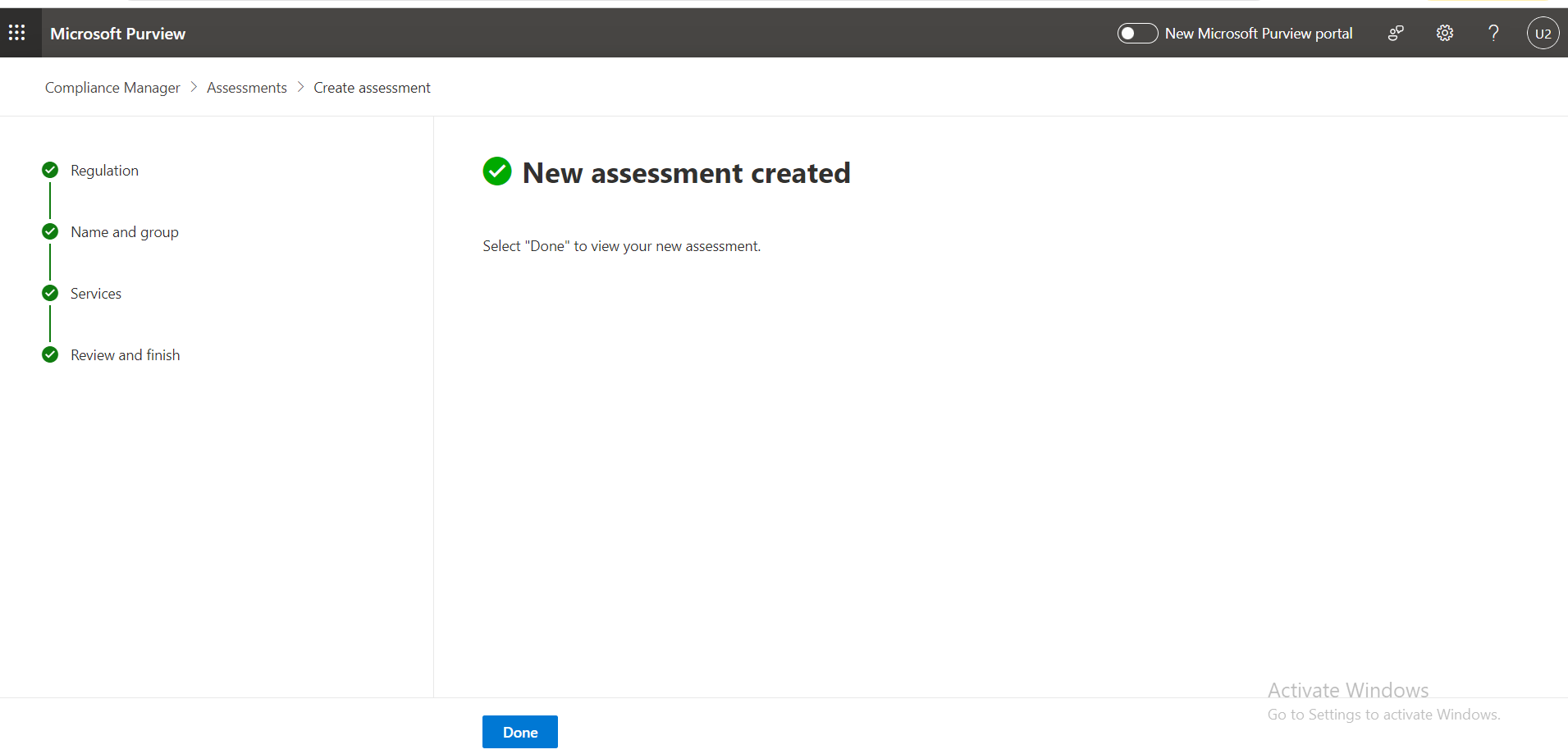


Figure 20 ISo27001 assessment created

For GDPR

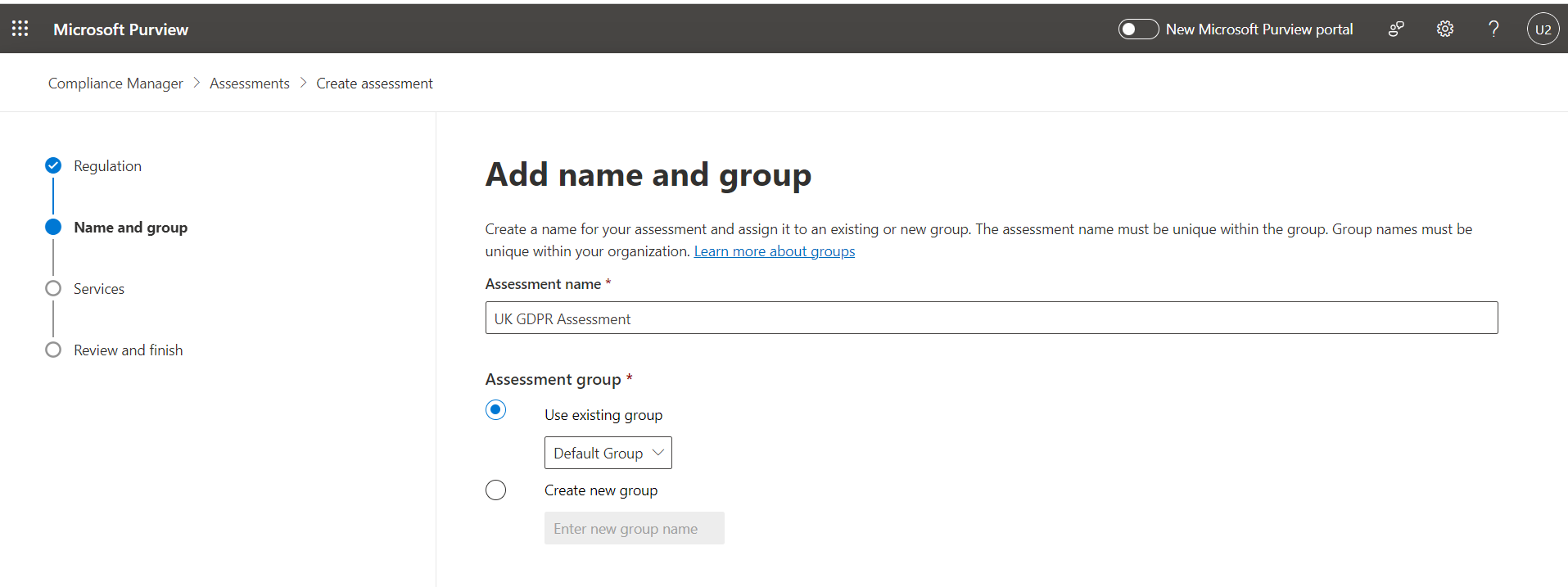


Figure 21 Add GDPR compliance

#### **Step 3: Track Compliance**

Once the assessment is created, can view the compliance score and improvement actions on the dashboard regularly update the status of actions as you implement controls and achieve compliance generate reports from the reports section to share with stakeholders.

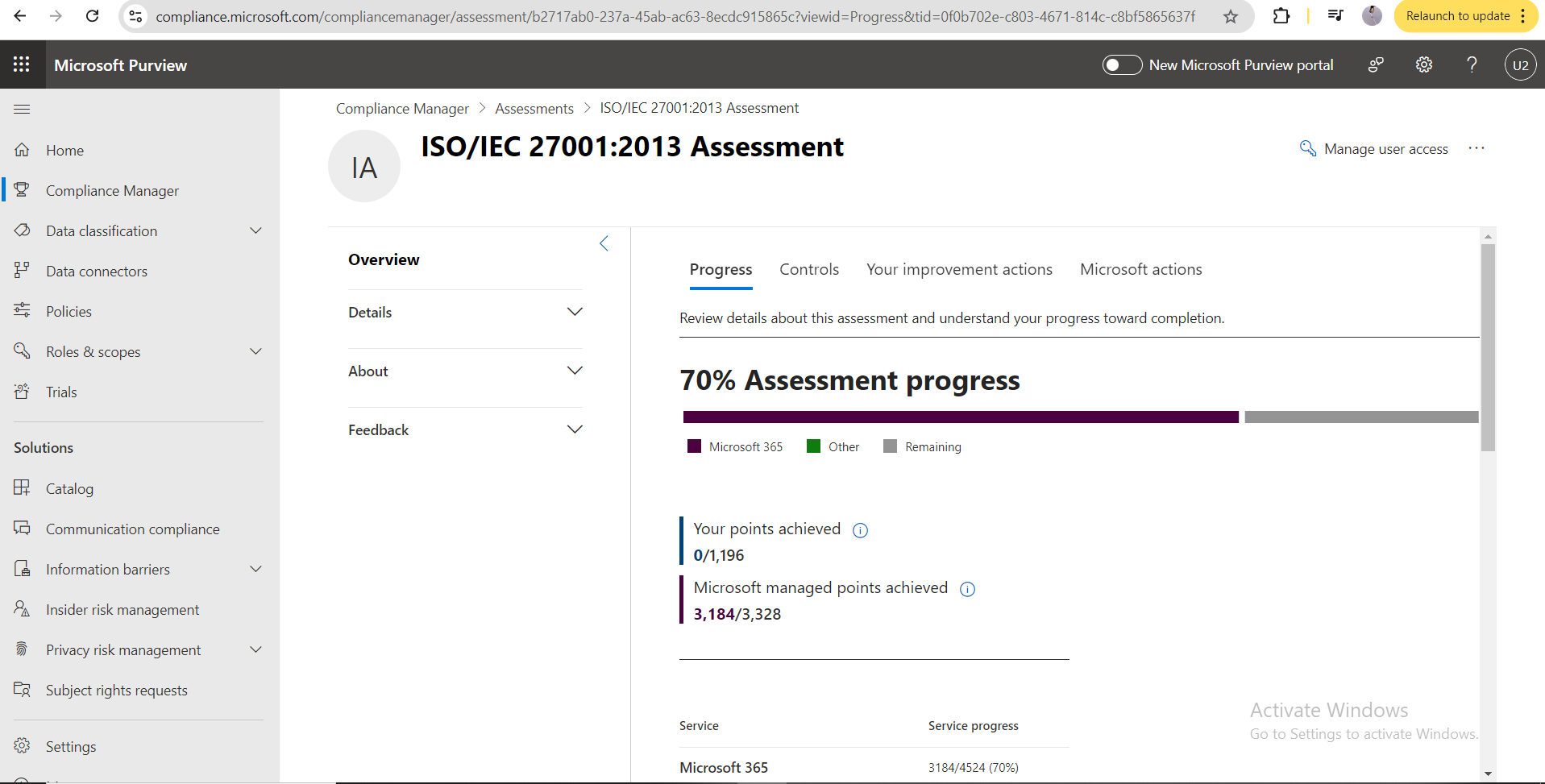


Figure 22 Assessment progress

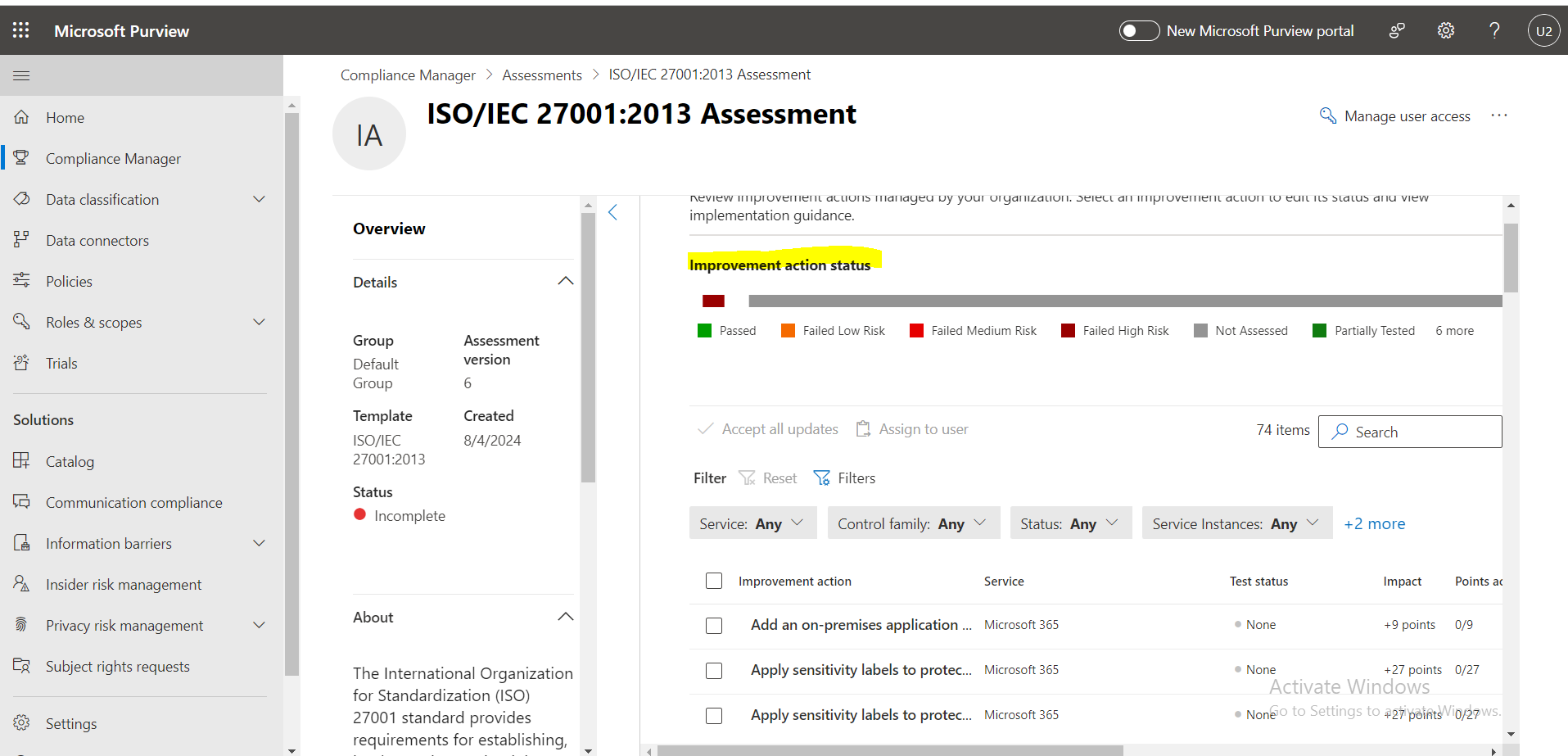


Figure 23 Improvement section

By following these steps and utilizing the provided tools, can effectively implement and manage Cloud Security Posture Management (CSPM) within SMB’s Microsoft Azure and Microsoft 365 environments. This will enhance your security posture, ensure compliance, and provide valuable insights for continuous improvement.

# **Chapter 5: Results and Discussion**

## **5.a Introduction**

In this chapter, presents the findings of the research and presents a detailed analysis of the findings when it comes to CSPM for SMBs. The analysis shows how Automated CSPM tools can advance cloud security, compliance, and risk minimisation across cloud settings in light of the above. These tools will be discussed in the context of their contribution to enhancing the overall security of SMBs; the real-life experiences reviewed for this paper also captured the issues that implementing these tools raised.

## **5.b Results of Compliance Assessments**

### **Summary of Assessments:**

In this study, compliance assessments were completed with a view of establishing the degree of compliance to cloud environment with two regulatory frameworks, namely the GDPR and the ISO/IEC 27001:2013. These brought out the level of compliance ranging from high to low; this pointed out the parts where security controls where effective, and where more attention was needed. The results highlighted above present a current state of compliance for the cloud environment and reveal best and areas of compromised compliance with these fundamental regulations.

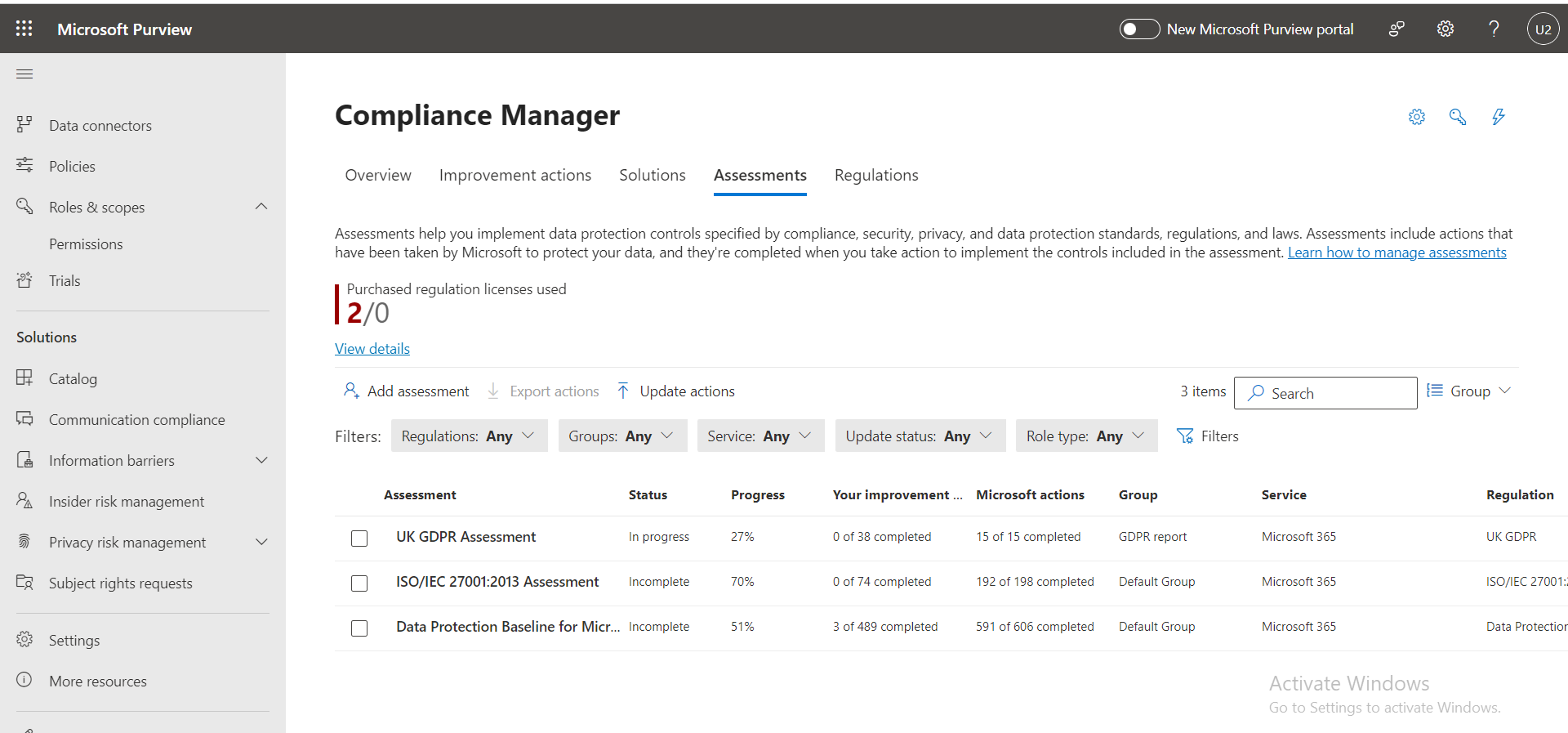


Figure 24 Compliance manager

### **UK GDPR Assessment:** In progress with 27% completion.

The uk gdpr assessment is a crucial evaluation designed to ensure compliance with the general data protection regulation gdpr a significant legal framework governing data protection and privacy for individuals within the united kingdom and the european union this assessment is particularly important for small and medium sized businesses sm bs that process or store the personal data of uk or eu citizens as non compliance can lead to substantial fines and legal repercussions the assessment evaluates various aspects of data protection including how personal data is collected processed stored and shared it also examines the effectiveness of data protection policies and procedures in place within the organization.

With a current completion rate of 27% the uk gdpr assessment indicates that there has been some progress towards achieving full compliance but a considerable portion of the necessary actions remains unaddressed this incomplete status reflects the complexity of gdpr compliance which often requires substantial resources dedicated personnel and a thorough understanding of the legal requirements the assessment progress suggests that while the organization has taken initial steps such as identifying areas of risk and beginning to implement protective measures there are still significant gaps that need to be addressed to fully align with gdpr standards moving forward it will be essential to prioritize the completion of the remaining actions to mitigate potential risks and ensure full compliance with gdpr.

### **ISO/IEC 27001:2013 Assessment:** Incomplete with 70% completion.

The iso 27001 2013 assessment is an essential evaluation process that focuses on the implementation and management of an information security management system isms within the organization iso iec 27001 2013 is a globally recognized standard that provides a systematic approach to managing sensitive company information ensuring its confidentiality integrity and availability the standard covers a wide range of security controls including those related to data protection risk management access control and incident response.

The assessment for iso iec 27001 2013 within the organization is currently at a 70 completion rate indicating that a substantial portion of the required actions has been undertaken this level of completion reflects a strong commitment to establishing a robust security framework that aligns with international best practices the completed actions may include the development of security policies implementation of technical controls and training of personnel on security protocols however the assessment is still incomplete suggesting that there are critical areas that need further attention to achieve full compliance the remaining 30 likely involves more complex or resource intensive tasks such as conducting thorough risk assessments implementing advanced security controls and ensuring continuous monitoring and improvement of the isms achieving full compliance with iso iec 27001 2013 will not only enhance the organization s security posture but also demonstrate its commitment to safeguarding sensitive information which is particularly important for sm bs operating in a competitive and increasingly regulated environment.

These assessments are integral to the organization s overall strategy for achieving and maintaining a high standard of security and regulatory compliance while progress has been made it is crucial to address the remaining gaps to ensure that the organization is fully protected against potential threats and is compliant with relevant regulations.

### **Compliance Score and Progress:**

The current status of the assessments conducted under the compliance manager indicates that while some progress has been made the journey towards full compliance remains ongoing for both the uk gdpr assessment and the iso iec 27001 2013 assessment it is noteworthy that no improvement actions have been completed by the internal team as of yet this lack of completed actions suggests that the organization is still in the early stages of addressing the identified compliance requirements or has encountered challenges in executing the necessary steps to meet these stringent standards.

The absence of completed internal actions highlights the need for a more focused and strategic approach to compliance it is essential to recognize that these assessments are not merely checklists but involve a series of complex tasks including risk assessments policy development implementation of controls and ongoing monitoring the internal team s current progress or lack thereof may be attributed to various factors such as resource constraints limited expertise or the sheer scope of the compliance requirements to move forward the organization may need to allocate additional resources seek external expertise or prioritize specific actions to make measurable progress in these assessments.

Despite the internal challenges the organization has benefited from the actions completed by microsoft which have significantly contributed to advancing compliance efforts in both assessments microsoft has played a pivotal role by addressing a substantial number of compliance controls on behalf of the organization for the uk gdpr assessment microsoft has completed 15 out of 38 required actions while for the iso iec 27001 2013 assessment they have successfully completed 192 out of 198 actions these completed actions by microsoft primarily involve implementing technical controls and providing secure infrastructure that aligns with the requirements of the respective standards.

The actions taken by microsoft are integral to the organization s overall compliance score as they cover critical areas such as data protection encryption access management and incident response by leveraging microsoft s capabilities and secure cloud infrastructure the organization is already closer to achieving compliance than it would be through internal efforts alone however it is important to note that while microsoft s contributions are invaluable they do not absolve the internal team from taking necessary actions specific to their operational processes and data management practices.

Microsoft s completed actions have provided a solid foundation for compliance the internal team must now focus on completing their portion of the assessments this will require a concerted effort to address the remaining gaps implement the necessary controls and ensure continuous monitoring and improvement to achieve and maintain full compliance with the uk gdpr and iso iec 27001 2013 standard.

## **5.c Analysis of Key Findings**

### **UK GDPR Assessment for Microsoft office 365:**

#### **Importance of GDPR Compliance for SMBs:**

For small and medium-sized businesses sm bs gdpr compliance is not just a legal obligation but also a critical component of trust and credibility especially when handling the data of eu citizens the general data protection regulation gdpr is one of the most stringent data protection regulations globally and failure to comply can result in severe financial penalties as well as reputational damage for an smb where resources may already be limited ensuring gdpr compliance is vital to avoid potential fines and to build and maintain trust with customers partners and stakeholders moreover gdpr compliance is often seen as a benchmark for data protection practices globally meaning that achieving compliance can provide a competitive advantage and open doors to new business opportunities.

#### **Analyzing the 27% Progress:**

As of now the uk gdpr assessment for microsoft office 365 shows a 27 completion rate this indicates that a portion of the necessary actions and controls required for compliance have been implemented the progress includes actions that relate primarily to data processing roles controllers and processors and some fundamental principles of gdpr the green segments in the control status breakdown highlight areas where initial steps have been taken possibly involving the establishment of data processing agreements identification of data subjects and initial assessments of data processing activities these are crucial steps as they lay the foundation for the more complex aspects of gdpr compliance such as ensuring lawful processing data minimization and obtaining explicit consent from data subjects

However, the remaining 73% of uncompleted actions suggest that there is still significant work to be done this includes more detailed and challenging aspects of gdpr such as implementing comprehensive data protection by design and by default ensuring the rights of data subjects such as the right to access rectification and erasure and managing data breaches effectively additionally attention must be given to the transfer of personal data to third countries or international organizations ensuring that such transfers comply with gdpr requirements such as implementing standard contractual clauses or binding corporate rules.

#### **Identifying Potential Risks or Non-Compliance Issues:**

The uncompleted actions in the uk gdpr assessment pose several potential risks to the organization one of the most significant risks is the possibility of non compliance with gdpr s core principles which could lead to substantial fines and legal action without completing the remaining actions the organization may also struggle to demonstrate compliance during an audit or investigation by data protection authorities this could result in not only financial penalties but also orders to cease certain data processing activities which could severely disrupt business operations.



Figure 25 UK GDPR Control status

Another critical risk is the potential for data breaches or other security incidents that are not managed according to gdpr requirements the gdpr mandates timely notification of breaches to both the authorities and affected data subjects and failure to comply with these requirements can exacerbate the consequences of a breach moreover if data protection by design and by default has not been fully implemented there is a higher likelihood that personal data could be exposed or misused further compounding the organization s risk profile.

In summary, while progress has been made in the uk gdpr assessment the current status highlights the need for continued focus and effort to address the remaining compliance gaps achieving full gdpr compliance will require a concerted effort to implement all necessary controls particularly those that involve protecting the rights of data subjects and managing international data transfers addressing these areas will be crucial to minimizing risks and ensuring that the organization meets its gdpr obligations.

### **ISO/IEC 27001:2013 Assessment for Microsoft 365**

#### **Progress Analysis and Significance of 70% Completion**

The iso iec 27001 2013 certification is a globally recognized standard for information security management providing a systematic approach to managing sensitive company information to ensure its confidentiality integrity and availability for tech solutions achieving 705 progress in aligning microsoft 365 with the iso iec 27001 2013 requirements represents a significant milestone in strengthening the company s information security management system isms this progress indicates that the organization has successfully implemented most of the required controls and processes to safeguard its cloud based environment.

The 70% completion reflects the organization s commitment to upholding international standards in information security it demonstrates that the company has effectively addressed key areas such as risk assessment access control and incident management which are critical for protecting sensitive data within microsoft 365 this level of progress suggests that the foundational elements of a robust isms are in place providing a strong defense against potential security threats and ensuring compliance with regulatory requirements moreover this progress helps build trust with clients and stakeholders as it indicates a proactive approach to managing information security risks.

However while reaching 70% completion is commendable it is crucial to recognize that the remaining 30% of the assessment holds significant implications for the overall security posture the unaddressed 30% represents critical areas that could expose the organization to vulnerabilities if not promptly and effectively managed

#### **Impact of the Remaining 30% on Security Posture**

The remaining 30% of the iso iec 27001 2013 assessment involves implementing controls and processes that are essential for the comprehensive protection of the organization s information assets if these areas are not addressed in a timely manner they could create security gaps that undermine the effectiveness of the existing controls thereby compromising the overall security posture.

For instance the remaining 30% may include controls related to business continuity management supplier relationships and compliance with legal and regulatory requirements these areas are crucial for ensuring that the organization can continue its operations in the event of a disruption manage third party risks effectively and adhere to applicable laws and regulations failure to implement these controls could lead to data breaches legal penalties and loss of customer trust

#### **Identifying Potential Risks or Non-Compliance Issues:**

The control status breakdown for the iso iec 27001 2013 assessment provides a detailed view of the compliance status across various control families highlighting areas where the organization has successfully implemented security measures and areas that require further attention by analyzing the graph depicting the status of controls grouped by tech solutions can identify potential risks or non compliance issues that may expose the organization to vulnerabilities these gaps in compliance could lead to security breaches data loss or regulatory penalties if not addressed promptly understanding the distribution of compliant and non compliant controls enables the organization to prioritize remediation efforts ensuring that critical areas are fortified and that the overall security posture aligns with industry standards and regulatory requirements.

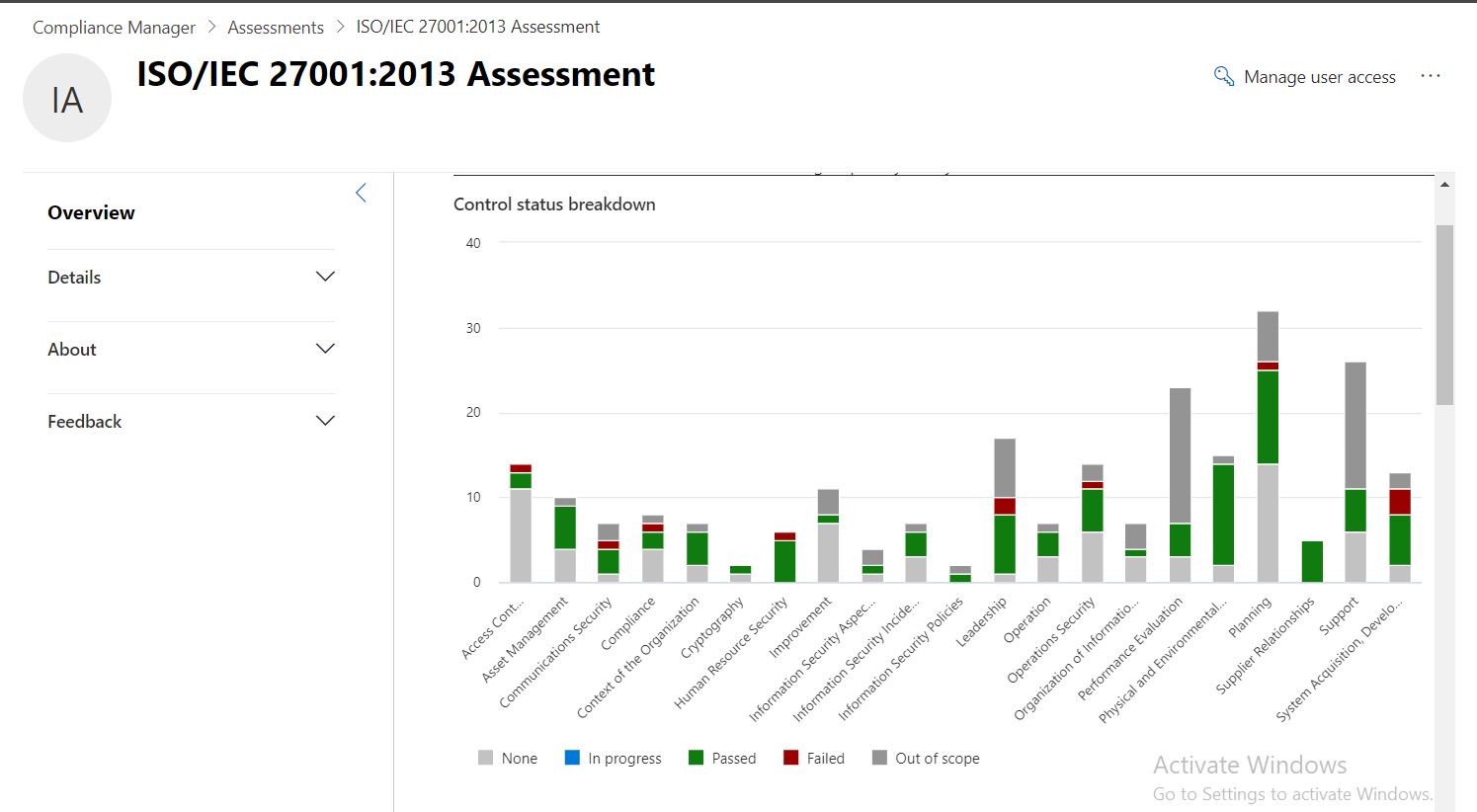


Figure 26 Control status breakdown for ISO/IEC 27001:2013

#### **Analysis of the 192 Actions Completed by Microsoft and Identification of Gaps**

As part of the iso iec 27001 2013 assessment microsoft has completed 192 actions related to the security of microsoft 365 services these actions represent the measures taken by microsoft to comply with the iso iec 27001 2013 standard thereby contributing to the security and compliance of the platform.

The completion of these 192 actions by microsoft significantly enhances the security of microsoft 365 as it ensures that the platform meets stringent security and compliance requirements these actions likely include the implementation of security controls such as encryption multi factor authentication data loss prevention and access controls by addressing these areas microsoft provides a secure foundation for organizations using microsoft 365 helping to protect sensitive information and reduce the risk of data breaches.

However despite microsoft s comprehensive efforts it is important to recognize that the responsibility for information security is shared between microsoft and the customer organization while microsoft provides the necessary infrastructure and tools abc tech solutions must implement additional controls and processes specific to its operational environment to achieve full compliance with iso iec 27001 2013.

## **5.d Impact of Completed Actions:**

The completed actions by microsoft have significantly strengthened the cloud security posture by implementing a robust set of automated and pre configured controls designed to safeguard critical data and resources these actions which include advanced security measures such as encryption multi factor authentication and access controls have created a secure environment that mitigates potential risks and enhances overall compliance with industry standards by leveraging Microsoft s built in security features has benefited from continuous monitoring and real-time threat detection which has reduced the likelihood of security breaches and ensured that the cloud environment remains protected against evolving cyber threats moreover the effectiveness of these automated and pre-configured controls in meeting regulatory requirements cannot be overstated they provide a strong foundation for compliance by ensuring that security policies and procedures are consistently applied across all cloud services thereby reducing the manual effort required for compliance management this systematic approach not only simplifies the organization s compliance journey but also instills confidence in stakeholders that committed to maintaining the highest levels of data protection and regulatory adherence.

## **5.e Challenges in Completing Assessments:**

Completing the improvement actions to strengthen cloud security posture particularly in alignment with iso iec 27001 2013 standards presented several challenges for the team one of the primary challenges was resource constraints as the organization had limited personnel available with the necessary expertise to implement and manage the complex security controls required for full compliance this limitation was exacerbated by the complexity of the tasks which often involved configuring advanced security settings integrating multiple security tools and ensuring that all controls were properly aligned with regulatory requirements additionally the team faced difficulties in interpreting and applying certain security measures due to a lack of specialized knowledge in cloud security best practices and regulatory frameworks these challenges sometimes led to delays in the implementation process and increased the risk of non compliance.

To overcome these challengesx organization scould adopt several strategies first investing in staff training and development would enhance the team s expertise in cloud security and compliance enabling them to more effectively manage and implement complex security controls this could include certifications in cloud security specialized training in regulatory compliance and ongoing education in emerging security threats and best practices additionally the organization could consider leveraging external expertise by partnering with cloud security consultants or managed security service providers mss ps who can provide guidance and support in implementing and maintaining a robust cloud security posture finally improving resource allocation by dedicating more personnel and time to critical security projects would help ensure that the necessary actions are completed efficiently and effectively by addressing these challenges proactively can enhance its ability to maintain a secure and compliant cloud environment even as security demands continue to evolve.

## **5.f Significance for SMBs:**

Cloud security posture management cspm tools like microsoft compliance manager are particularly crucial for small and medium sized businesses sm bs that often face challenges in managing their cloud security and compliance due to limited resources and expertise these tools provide sm bs with a centralized platform to monitor assess and manage their security posture effectively ensuring that they remain compliant with industry regulations and standards the importance of cspm tools lies in their ability to automate complex security tasks such as tracking compliance with regulatory frameworks identifying potential vulnerabilities and providing actionable recommendations for remediation for sm bs this automation is invaluable as it reduces the manual effort required to maintain a secure cloud environment allowing them to focus on their core business activities while ensuring that security is not compromised.

Moreover cspm tools enable continuous monitoring of the cloud environment which is essential for keeping up with the dynamic nature of cybersecurity threats by leveraging tools like microsoft compliance manager sm bs can continuously assess their compliance status receive real time alerts on potential security issues and generate reports that are critical for regulatory audits this ongoing visibility into the security posture allows sm bs to proactively address vulnerabilities before they can be exploited thereby minimizing the risk of data breaches and other security incidents additionally these tools can be tailored to meet the specific needs of sm bs ensuring that the security measures implemented are both effective and scalable as the business grows in summary cspm tools play a vital role in helping sm bs maintain a robust and compliant cloud security posture providing the necessary support to navigate the complexities of cloud security and compliance.

## **5.g Conclusions:**

In conclusion the implementation of CSPM tools such as microsoft defender for cloud azure policy and microsoft compliance manager has significantly enhanced the cloud security posture by automating compliance checks and improving threat detection while the actions completed have strengthened overall security challenges such as resource constraints and complexity must be addressed to ensure continuous improvement the significance of these tools for SMBs lies in their ability to provide ongoing monitoring and compliance management which is critical for maintaining a secure and compliant cloud environment in line with industry standards.

# **Chapter 6 Conclusion and Future work**

## **6.a Conclusions**

This thesis has underscored the importance of Cloud Security Posture Management (CSPM) in securing cloud environments for small and medium-sized businesses (SMBs). Through the implementation of CSPM tools, SMBs can significantly improve their ability to manage cloud security, ensure compliance with industry standards, and protect sensitive information from cyber threats. The research has demonstrated that CSPM tools not only automate the identification and remediation of security vulnerabilities but also provide continuous monitoring and compliance tracking, which are essential for maintaining a strong security posture in dynamic cloud environments. Despite the challenges faced in deploying and optimizing these tools, the benefits they offer in terms of risk reduction and regulatory adherence are substantial. The findings suggest that CSPM is not just an optional add-on but a fundamental component of modern cybersecurity strategy, particularly for SMBs that are increasingly reliant on cloud technologies. Future work should explore the integration of CSPM with other security frameworks and the adaptation of these tools to address emerging threats in a rapidly evolving digital landscape.

The findings demonstrated that cspm tools provide a comprehensive approach to managing cloud security allowing businesses to detect and mitigate threats in real time ensure adherence to regulatory requirements and maintain continuous visibility over their cloud resources the case study revealed that while significant progress has been made in aligning with iso iec 27001 2013 standards there are ongoing challenges related to resource allocation expertise and the complexity of the security environment that must be addressed to achieve full compliance and robust security.

This research underscored the critical role of CSPM tools in supporting SMBs, which often lack the extensive resources and expertise needed to manage cloud security effectively. By automating key security tasks and providing actionable insights, these tools empower SMBs to protect their sensitive data, reduce the risk of cyberattacks, and meet industry regulations with greater efficiency. However, the success of CSPM implementation also depends on continuous improvement and proactive measures to address emerging threats and evolving regulatory landscapes.

## 6.b Future Work

The findings of this thesis open several avenues for future research and practical improvements in the domain of cloud security posture management particularly for sm bs one potential area for future work is the exploration of more advanced machine learning and artificial intelligence ai techniques within cspm tools these technologies could enhance threat detection capabilities provide predictive analytics and offer more tailored recommendations based on the specific security needs and behaviors of an organization.

Another area of future research could involve the integration of cspm tools with other security frameworks and platforms such as security information and event management siem systems or endpoint detection and response edr solutions this integration could provide a more holistic view of an organization s security posture enabling a more comprehensive approach to threat management and incident response.

Moreover future studies could investigate the long term impact of cspm tools on compliance maintenance and cost effectiveness for sm bs understanding how these tools contribute to sustained regulatory compliance and whether they provide a cost efficient solution for smaller businesses could offer valuable insights for organizations considering cloud adoption or cspm implementation in addition to technical advancements future work should also address the human factors involved in cloud security management research could focus on developing more effective training programs and awareness campaigns that equip sm bs with the necessary knowledge and skills to leverage cspm tools fully by enhancing the human element in cloud security businesses can maximize the benefits of their cspm investments.

Finally as cloud technologies and regulatory requirements continue to evolve there will be an ongoing need to update and refine cspm strategies future research should continue to monitor these changes providing updated best practices and guidance for sm bs to ensure that their cloud environments remain secure and compliant in an increasingly complex digital landscape.

In summary while this thesis has laid a strong foundation for understanding the importance of cspm in cloud security for sm bs there remains a wealth of opportunities for future exploration by addressing both technological and human challenges future work can contribute to the development of more effective scalable and sustainable cloud security practices for organizations of all sizes.

# References

1. Bar-Haim, R. E. L. K. Y. A. V. D. M. G. N. K. A. O. M. a. Z. M., 2023. Towards Automated Assessment of Organizational Cybersecurity Posture in Cloud. *In Proceedings of the 6th Joint International Conference on Data Science & Management of Data (10th ACM IKDD CODS and 28th COMAD) (pp. 167-175).`.*
2. Barlette, Y. G. K. &. J. A., 2015. Toward a better understanding of SMB CEOs' information security behavior: Insights from threat or coping appraisal. *Journal of Intelligence Studies in Business, 5(1.*
3. Bhattacharya, D., 2022. Leadership styles and information security in small businesses.. *Information Management & Computer Security, 19(5), 300-312..*
4. Chauhan, M. a. S. S., 2023. An analysis of cloud security frameworks. *problems and proposed solutions. Network, 3(3),,* pp. 422-450.
5. Coppola, G. V. A. a. S. J., 2024. Enhancing Cloud Security Posture for Ubiquitous Data Access with a Cybersecurity Framework Based Management Tool.. *In 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0590-0594). IEEE..*
6. Del Vecchio, J. L. Y. W. L. a. K. A., 2024. Towards Assessing Cybersecurity Posture of Manufacturing Companies: Review and Recommendations.`.
7. Gafni, R. a. L. Y., 2023. Experts’ feedback on the cybersecurity footprint elements: in pursuit of a quantifiable measure of SMBs. *Computer Security, 31(5), pp.601-623..*
8. Johnsen, C. T. A. S. K. a. V. B., 2021. Sme: A high productivity fpga tool for software programmers.. *arXiv preprint arXiv:2104.09768..*
9. Jung, H. a. L. K., 2022. Efficiency Analysis of Security Management System of Affiliates of Conglomerate Using DEA-SBM Model.. *ournal of the Korea Institute of Information Security & Cryptology, 32(2), pp.341-353..*
10. Kunduru, A., 2023. THE PERILS AND DEFENSES OF ENTERPRISE CLOUD COMPUTING: A COMPREHENSIVE REVIEW.. *Central Asian Journal of Mathematical Theory and Computer Sciences, 4(9), pp.29-41..*
11. Loaiza Enriquez, R., 2021. Cloud Security Posture Management/CSPM) in Azure.
12. Manns, G., 2021. The Adoption of Cybersecurity in Small-to Medium-Sized Businesses: A Correlation Study (Doctoral dissertation, Capella University).
13. Mansfield-Devine, S., 2023. Do you have too much security?. Network Security,.
14. Masoud, T., 2024. Distributed Systems and Web-based Inspirations on Cybersecurity and Sustainability: A Review of the Intertwined Challenges and Solutions in Enterprise Systems. *Journal of Information Technology and Informatics, 3(2)..*
15. Moyo, M. &. L. M., 2020. Evaluation of Cloud Business Intelligence Prior to Adoption: The Voice of Small Business Enterprises in a South African Township.. *In Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, November 25–26, 2020, Proceedings 17 (pp. 449-460). Springer International Publishing..*
16. Öhman, M., 2023. IT security: Exploring the Benefits of Cloud Computing for Incident Response..
17. Olaoye, G. a. L. A., 2024. Future trends and emerging technologies in cloud security..
18. Ouma, G. A. M. W. K. a. M. B., 2024. DESIGNING A COMPREHENSIVE FRAMEWORK FOR DATA AND NETWORK SECURITY IN CLOUD COMPUTING: CASE OF KENYAN BANKING INDUSTRY.. *African Journal of Emerging Issues 6, no. 2.*
19. Patel, S. A. R. A. S. a. J. R., 2023. A Modest Approach Toward Cloud Security Hygiene.. *In International Conference on Recent Developments in Cyber Security (pp. 217-227). Singapore: Springer Nature Singapore.*
20. Pawar, S., 2016. BUSINESS DOMAIN-SPECIFIC LEAST CYBERSECURITY CONTROLS IMPLEMENTATION (BDSLCCI) FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES (SMES). *Global journal of Business and Integral Security..*
21. Pawar, S. a. P. H., 2022. A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights, 2(1), p.100080..*
22. Pei, J. S. Y. F. Q. S. R. L. L. Y. S. S. J. a. M. Z., 2023. An efficient confidentiality protection solution for pub/sub system.. *Cybersecurity, 6.*
23. Riley, A. a. L. C., 2017. Magic quadrant for cloud access security brokers. November, Skyhigh Networks, available at: https://info. skyhighnetworks..
24. Rizvi, Z. K. C. a. O. M., 2023. Analytical hierarchy process model for managing cloud security.. *information & Computer Security, (ahead-of-print)..*
25. Saha, B. a. A. Z., 2024. A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework.. *Journal of Information Security, 15(01), pp.24-39..*
26. Suriya, B. A. B. R. A. a. A. C., 2024. Cloud Security: Upgradation in CSPM Configuration Setting. *In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-4). IEEE.*
27. Tam, T. R. A. &. H. J., 2022. he good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security, 109, 102385..*
28. Tam, T. R. A. a. H. J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security, 109, p.102385..*
29. Thamrongthanakit, T., 2023. Impacts of Cybersecurity Practices on Cyberattack Damage and Protection Among Small and Medium Enterprises in Thailand.. *2023.*
30. Tomai, N., 2007. Particularities of security design for wireless networks in small and medium business (SMB).. *Informatica Economica, 44(11), 93-98..*
31. Vo, T. W. C. a. Y. F., 2023. Blockchain Security-Efficiency Analysis based on DEA-SBM Model. *The Eurasia Proceedings of Science Technology Engineering and Mathematics, 23, pp.202-208..*
32. Baviskar, C.R., 2022. *Cloud based automated encryption approach to prevent S3 bucket leakage using AWS Lambda* (Doctoral dissertation, Dublin, National College of Ireland).
33. Apeh, A.J., Hassan, A.O., Oyewole, O.O., Fakeyede, O.G., Okeleke, P.A. and Adaramodu, O.R., 2023. GRC strategies in modern cloud infrastructures: a review of compliance challenges. *Computer Science & IT Research Journal*, *4*(2), pp.111-125.
34. Haber, M.J., Chappell, B. and Hills, C., 2022. Mitigation Strategies. In *Cloud Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Cloud Resources* (pp. 221-296). Berkeley, CA: Apress.
35. Choudhary, A., Tripathi, A., Sharma, A. and Singh, R., 2022, November. Evolution and comparative analysis of different Cloud Access Security Brokers in current era. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 36-43). IEEE.
36. Chugh, S., 2023, November. Bridging the Gap: Industry Perspectives and Trends in Cloud Security, and Opportunities for Collaborative Research. In *2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)* (pp. 400-404). IEEE.
37. Ahir, D. and Shaikh, N., 2023, November. A Systematic Survey on Cloud Security Threats, Impacts and Remediation. In *2023 IEEE Engineering Informatics* (pp. 1-9). IEEE.
38. FATTAKHOVA, M. and AHMADOV, S., THE CLOUD SERVICE SECURITY ISSUE RISK EVALUATION: CASE OF AZURE AND MICROSOFT 365. *Journal of Baku Engineering University*, *7*(1), p.47.