Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA
Published: February 18, 2025
DOI: 10.46254/AN15.20250204

Cloud Security Guidance for Small and Medium-sized Businesses (SMBs)

Pooja Shah, Siddharth Dua and Eslam G. AbdAllah
Information Systems Security and Assurance Management (ISSAM) Department
Concordia University of Edmonton
Edmonton, Alberta, Canada
pshah2,sdua@student.concordia.ab.ca, eslam.abdallah@concordia.ab.ca

Abstract

Small and Medium Businesses (SMBs) play a crucial role in national economies and employment worldwide. As these businesses rapidly adopt technology and cloud services to stay competitive, they become prime targets for cyber criminals. SMBs are particularly more vulnerable to cyber-attacks due to limited awareness and resources for implementing cybersecurity measures. This research aims to address these challenges by providing practical guidance to SMBs on implementing Cloud Security controls. By focusing on understanding the security responsibilities as Cloud Service Consumers and targeting quick wins and easy-to-implement strategies for various aspects of cloud security, SMBs can establish a robust security posture and excel in this dynamic environment. The implementation of these strategies also facilitates the creation of a baseline for potential future compliance with Service and Organization Controls 2 (SOC 2) requirements or adherence to cybersecurity frameworks.

Keywords
Cloud Consumer, Cloud Provider, Cloud Security for SMBs

1. Introduction
Small and Medium Businesses (SMBs) are pivotal in driving economic growth globally, and their adoption of technology, mainly cloud services, is accelerating. Cloud Computing offers numerous benefits, such as easy deployment, flexibility, scalability, and cost savings, making it an attractive option for businesses of all sizes. However, with these benefits come new complexities and security challenges.

According to recent research, the global cloud computing market is projected to reach USD 947.3 billion by 2026, underscoring the widespread adoption of cloud services (ThreatModeler 2023). However, alongside this growth, there has been an increase in cloud security incidents, with 80% of companies experiencing at least one incident last year (Harris 2024). According to the Verizon DBIR report, almost half of all cyberattacks are aimed at small businesses, and a staggering 60 percent of those hit end up shutting down within just six months of the attack. The evolving threat poses additional risks to SMBs, with cyber adversaries ranging from amateurs to sophisticated nation-state actors targeting businesses of all sizes. Recent testimonies before the House Select Committee have highlighted the threat posed by cyber actors, particularly those linked to state-sponsored campaigns targeting critical infrastructure and supply chain vulnerabilities, including small businesses.

SMBs encounter significant challenges in implementing cybersecurity. Limited resources, such as smaller budgets and fewer IT staff, make it hard to allocate sufficient resources. Additionally, there is often a lack of awareness among SMB owners and managers about cybersecurity risks, leading to complacency. The complexity of cyber-security, coupled with technical barriers and cost concerns, and shared responsibility for cloud security further complicates matters. The absence of formal cybersecurity policies and procedures and limited employee training leaves SMBs

vulnerable to cyber threats. Despite these challenges, SMBs must prioritize security and adopt effective cloud security strategies, even with limited resources. Various widely acclaimed cyber-security frameworks are available in the industry that any organization can choose to implement and create cyber resiliency. However, the frameworks available in the market need adequate guidance and support to implement them which do not work in favor of SMBs (Chauhan 2023, Alrasheed 2022, Gapinski 2015).

This paper aims to provide SMBs with the knowledge and resources to secure their cloud environments effectively. It begins by discussing the major risks associated with cloud services and examining existing cloud security frameworks. The fourth section explains the shared security responsibilities between Cloud Service Providers and Consumers, guiding SMBs on areas to focus on securing while using cloud services. Subsequent sections delve into specific aspects of security domains, such as access management, data protection, network security, asset protection, logging and monitoring offering practical guidelines for implementing controls. Moreover, the paper advocates user training as one of the most effective measures for SMBs to safeguard their operations and enhance the resilience of the digital ecosystem. In the concluding section, the paper enumerates security controls and services provided by CSPs, along with available open-source resources at no cost. By adhering to the security practices outlined in this paper, SMBs can shield themselves from anonymous and continually expanding threat actors while also striving for compliance with widely accepted frameworks such as Service and Organization Controls 2 (SOC2) and others.

2. Cloud Security Risks

Cloud security risks pose significant threats to the operations and integrity of SMBs relying on cloud services. One major challenge is the loss of visibility. With cloud services dispersed across multiple devices, departments, and locations, maintaining visibility in who accesses data and how it is utilized becomes increasingly complex. This lack of visibility heightens the risk of data breaches and loss, as sensitive information may be accessed, uploaded, or downloaded without proper oversight (Ahmadi 2024, Chaudhuri 2024, Hassan 2022). Common cloud security risks include:

Unmanaged Attack Surface: The wide adoption of microservices has led to a proliferation of publicly available workloads, adding to the attack surface. SMBs are particularly vulnerable to zero-day exploits and attacks targeting vulnerabilities in software or operating systems that have not been patched. For example, the SolarWinds supply chain attack in 2020 exploited zero-day vulnerabilities, affecting numerous organizations worldwide (Arcserve 2024).

Human Error: Gartner predicts that through 2025, 99% of all cloud security failures will be due to some level of human error (Puzas 2024). Hosting resources on the public cloud magnifies this risk. Users may unknowingly use APIs without proper controls, creating vulnerabilities. According to Proofpoint's 2023 Human Factor report, 94% of monitored cloud tenants faced either precision or brute-force attacks each month. Among these tenants, 62% fell victim to successful attacks (Coker 2023).

Misconfiguration: Misconfiguration of cloud services, particularly insecure APIs, can expose SMBs to data breaches. Default settings or inadequate access management can leave critical data open to exploitation. For example, in June 2023, Toyota reported that approximately 260,000 customers' data was exposed online due to a misconfigured cloud environment (Arcserve 2024).

Data Breach: Unauthorized access to sensitive data can result in financial losses and reputational damage. Facebook's breach before August 2019, which went undisclosed until April 2021, exemplifies this. The breach affected over 530 million users, leading to regulatory penalties and tarnishing the company's reputation (Arcserve 2024).

3. Existing Cloud Security Frameworks

Cloud Security Strategies for Small and Medium Businesses (SMBs) are essential for safeguarding digital assets against cyber threats. While existing frameworks such as MITRE ATT&CK, Center for Internet Security (CIS), CSA STAR, and ISO/IEC 27017:2015 offer comprehensive guidelines, they can be daunting for SMBs due to their complexity resource requirements. This paper aims to provide easy-to-follow steps and guidelines explicitly tailored

for SMBs, addressing their limitations in resources and technical expertise. SMBs can effectively protect their data without undue complexity or financial burden by simplifying cloud security measures.

4. Preparing for secure cloud implementation

Implementing cloud security strategies for small and medium businesses (SMBs) requires thorough planning and proactive measures to mitigate risks effectively. This section outlines key preparations SMBs must undertake to implement cloud security controls.

Leadership Team: The leadership team should prioritize cybersecurity as a strategic component of the business model, communicate security goals clearly, and ensure alignment with budgetary considerations. Promoting security awareness and encouraging secure practices can significantly reduce the risk of human error or negligence. Effective leadership is pivotal in driving the organization's security vision and objectives. Moreover, fostering a culture of security at all levels of the organization is essential, with regular communication and integration of security objectives into business goals.

Risk Management: SMBs must understand and manage various cybersecurity risks, including regulatory compliance, criminal threats, legal liabilities, and reputational damage. Recognizing that security is a collective responsibility is paramount, particularly in smaller organizations where individual actions impact overall security posture. Integration of security controls across the organization is essential to mitigate these risks effectively.

Budget Allocation: Adequate budget allocation for cybersecurity is imperative. SMBs often need to pay more attention to the costs of implementing robust security measures. Hence, allocating sufficient resources to develop and maintain a comprehensive cyber-security plan tailored to the organization's needs is essential.

Cloud Security Lead: Appointing a proficient individual to oversee cloud security initiatives is essential. The Cloud Security Lead should possess a deep understanding of both security and business requirements. They are crucial in designing adequate security controls that balance operational efficiency with risk mitigation. Moreover, they should facilitate or overlook reporting, metrics analysis, and user training to enhance overall security posture.

5. Understanding Cloud Security – Shared responsibility model

When considering public cloud services, it is crucial to understand the shared responsibility model and the division of security tasks between the cloud provider and consumer (Kumar 2018, Ramachandra 2017, Zhang 2013). This model varies depending on whether the workload is on Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or in an on-premises data center.

5.1 Common Cloud Services

Software-as-a-Service (SaaS): SaaS provides ready-to-use applications that are accessible via web browsers or client platforms. The provider manages the infrastructure in this model while consumers utilize the applications. Though consumers have limited control, securing connections to SaaS environments remains a shared responsibility. In small businesses, examples of Software-as-a-Service (SaaS) could include using cloud-based email services such as Gmail or Office 365, which provide ready-to-use email applications accessible via web browsers. While the provider manages the infrastructure, businesses use email applications for communication.

Platform-as-a-Service (PaaS): PaaS empowers consumers to deploy custom applications using provider-supplied tools and services. While the provider manages the underlying infrastructure, consumers control deployed applications and configurations. Security measures, including authentication and access control, are shared between consumers and providers. For Platform-as-a-Service (PaaS), a small business might deploy custom web applications using a platform such as Heroku or Google App Engine. These platforms provide tools and services for application development and deployment while businesses control the deployed applications and configurations.

Infrastructure-as-a-Service (IaaS): IaaS enables consumers to provision computing resources for deploying and managing environments and applications. Cloud providers oversee infrastructure management, while consumers control computing resources and specific networking components. Security responsibilities, such as configuring fire-walls, are shared between consumers and providers (Cybersecurity and Infrastructure Security Agency 2022). In the case of Infrastructure- as-a-Service (IaaS), a small business might use cloud computing resources from providers such

as Amazon Web Services (AWS) or Microsoft Azure to host its website or web application. The business can provision virtual machines and storage while the cloud provider manages the underlying infrastructure. The business is responsible for configuring security measures such as firewalls to protect its hosted environment.

5.2 Shared Responsibility

A common confusion for the SMBs is to understand what the cloud provider protects and what they have to take care of Security responsibilities are shared between the Cloud Service Provider (CSP) and the user. This division of responsibilities is the shared responsibility model for cloud security. Data classification, network controls, and physical security have clear owners in the public cloud. Understanding where these responsibilities lie within different cloud environments is essential. Here is the breakdown for cloud service models (Dotson 2023).

SaaS (Software as a Service):
Access Control: Cloud consumers are responsible for managing user access to the SaaS application, including provisioning and deprovisioning user accounts, assigning appropriate roles and permissions, and enforcing strong authentication mechanisms such as multi-factor authentication (MFA).

Data Protection: Cloud consumers must ensure the security and privacy of data stored within the SaaS application. This includes implementing encryption for sensitive data both in transit and at rest, setting up data loss prevention (DLP) policies to prevent unauthorized data disclosure, and regularly reviewing access logs and audit trails for suspicious activities.

PaaS (Platform as a Service):
Cloud consumers need to take care of SaaS responsibilities along with new ones specific to PaaS.

Secure Configuration: Cloud consumers are responsible for configuring and securing the underlying platform services provided by the PaaS provider. This involves configuring firewall rules, network access controls, and identity and access management (IAM) policies to restrict access to platform resources based on business requirements.

Application Security: Cloud consumers must ensure the security of applications deployed on the PaaS platform. This includes implementing secure coding practices, such as input validation and output encoding, to prevent common web application vulnerabilities such as SQL injection and cross-site scripting (XSS).

IaaS (Infrastructure as a Service):
Cloud consumers must handle responsibilities from SaaS and PaaS, along with new ones specific to IaaS.

Network Security: Cloud consumers are responsible for configuring and securing the virtual networks, subnets, and security groups provided by the IaaS provider. This involves implementing network segmentation to isolate sensitive workloads, configuring firewall rules to control inbound and outbound traffic, and enabling network encryption to protect data in transit.

Vulnerability Management: Cloud consumers must regularly assess and remediate security vulnerabilities within the virtual machines and operating systems deployed on the IaaS infrastructure. This includes applying security patches and updates in a timely manner, conducting vulnerability scans and penetration tests, and implementing intrusion detection and prevention systems (IDPS) to detect and respond to potential security threats.

6. Secure the cloud

Small and Medium Businesses (SMBs) increasingly utilize cloud technology to enhance operations while prioritizing security measures against cyber risks. Understanding the importance of cloud security is vital for SMBs navigating evolving cyber threats. Robust cloud security ensures the confidentiality, integrity, and availability of sensitive data, particularly crucial for SMBs lacking resources compared to larger enterprises. Cloud security solutions, such as those from AWS, offer cost-effective scalability and seamless integration of security features, ensuring compliance with regulations and building customer trust. This section delves into security controls that fall under the responsibility of

cloud consumers and offers clear guidelines for SMBs to secure their cloud environments through easily implementable steps.

6.1 Access Management

Verizon Data Breach Report 2023 states Access Management in the top three security controls recommended for small and medium-sized businesses (Stansfield 2023). Access Management involves appropriate provisioning, modification, and revocation of every user's identity and access across all organizational assets. Here is a list of actionable steps that SMBs can employ.

Enable MFA: MFA enhances security by requiring users to provide multiple forms of verification, such as a password and a code sent to their phone, before accessing cloud resources. This additional layer of protection helps prevent unauthorized access, even if login credentials are compromised. Surprisingly, only 13% of employees at Small and Medium Businesses (SMBs) are required to use MFA, compared to 87% at larger companies with 10,000+ employees. However, MFA is an effective deterrent, blocking 99.9% of modern automated cyberattacks and 96% of bulk phishing attacks (Flynn 2023). Moreover, MFA is typically offered as a free service in most cloud platforms, making it highly advisable to enable it for all users.

Establish Access Requirements: Identify and map the access needs of all individuals to fulfill their business activities. During this phase, distinguish between regular and privileged users to determine the appropriate level of access control. A privileged account is a type of user account with more permissions and access rights than a standard account. Privileged accounts allow users to make significant changes to a system, such as changing system configuration, installing software, accessing sensitive data, or creating new user accounts (Brook 2023).

- Follow least privilege and separation of duties to assign appropriate access to all users
- Utilize RBAC to assign roles and permissions based on job responsibilities and organizational hierarchy. This approach ensures that users have access only to the resources necessary for their roles, reducing the risk of unauthorized access and data breaches. RBAC streamlines access management by defining roles, associating permissions with each role, and assigning roles to users.

Privileged Access Management: Securing privileged accounts is the foremost step in protecting critical assets. Cybercriminals target these accounts to gain access to an organization's sensitive resources. According to an article by One Identity, a leading Identity Security Company, 70% of data breaches are associated with privileged account abuse, and 61% are caused by improper credential management. This situation becomes even more concerning when we realize that nearly 90% of security professionals report that their organization's users have more privileged access than required for their work (Esposito 2023).

- To secure privileged access, one must isolate the accounts from the risk of being exposed to a cyber attacker.
- Cloud services administration permissions for administrative user access must be restricted and limited to only a handful of users.
- Administrator or root accounts should not be used for daily activities.
- A successor should be planned for the administrators to ensure a fallback administrator if the primary user becomes unavailable.
- Privileged Access Management and Password Manager, services offered by Cloud Providers or other third-parties can be considered for additional security.

Access Reviews: User Access Review is a crucial security practice in which organizations periodically assess and validate users' access rights to ensure alignment with their job requirements and overall organizational security policies. The primary objective is to confirm that users have the necessary permissions to perform their roles, following the principle of least privilege. During these reviews, unauthorized or redundant permissions are identified and revoked, reducing the potential risk of data breaches or internal misuse. Regular access reviews assist organizations in complying with regulatory requirements, maintaining a secure IT environment, and ensuring that the right individ-

uals have appropriate access to systems and data. Additionally, proactive management and monitoring of user permissions can enhance the security of critical assets and foster trust among various stakeholders.

6.2 Data Protection

Cloud providers employ robust security measures to safeguard sensitive data, including automatic backups and disaster recovery solutions, ensuring that critical business information remains protected, easily recoverable, and less susceptible to loss. Nevertheless, additional considerations are necessary for SMBs to effectively secure their data. This section explores essential strategies for data protection in the cloud environment tailored for SMBs.

Data Minimization: A fundamental principle of data protection involves minimizing the storage of unnecessary personal information. Despite the scalability and cost-effectiveness offered by cloud storage, SMBs must avoid collecting data indiscriminately. Conducting regular audits to assess the necessity of stored data and securely disposing of non-essential information reduces the attack surface and minimizes the impact of potential breaches (Jillson 2020).

Data Classification: It is crucial for SMBs to categorize data based on sensitivity and importance to organize and protect their information effectively. Engaging in discussions with business unit heads to clarify classification levels and integrating data classification into organizational security training ensures compliance and fosters a culture of data protection.

Encryption: Encrypting data during transmission outside the organization's network is paramount for safeguarding sensitive information. SMBs should encrypt data stored in public cloud services and during transmission to mitigate the risks of interception and unauthorized access. Selecting encryption solutions that seamlessly integrate with existing workflows simplifies implementation and ensures compliance with security policies.

Backup and Recovery: Regular backups of critical data are in-dispensable for SMBs to mitigate the impact of data loss incidents. Identifying and prioritizing critical data, such as customer Personally Identifiable Information (PII) or intellectual property (IP), ensures that essential assets are protected against potential threats. Cloud-based backup solutions offer scalability, redundancy, and accessibility, enabling swift restoration of operations in the event of data loss or system failures.

6.3 Network Security

Network security protects organization's sensitive data travelling through internal or external channels, preventing unauthorized access, and ensuring business continuity in cloud environments.

Network Diagram Maintenance: SMBs should maintain an up-to-date network diagram, updated annually and whenever significant changes occur. This ensures accurate documentation of the private cloud network layout.

- Assign responsibility to a designated team member for regularly updating the network diagram.
- Document any changes promptly and ensure they are reflected in the diagram to maintain accuracy.

Network Segmentation: Segmenting the network helps minimize the impact of breaches by isolating different parts of the network. This enhances security by containing any potential threats.

- Categorize network segments based on sensitivity and business requirements.
- Implement segmentation using VLANs or subnetting to isolate critical assets from less sensitive areas.

Network Firewalls: Deploy network firewalls to protect the private cloud network from external threats.

- Choose reputable firewall solutions that offer robust security features and regular updates.
- Work closely with IT security professionals to configure firewalls based on industry's best practices and specific business requirements.
- Configure network firewalls with secure, encrypted administrative access, and implement outbound filtering to prevent unauthorized access.
- Review firewall rules annually to ensure necessity and compliance, documenting any changes made by the Security Team.
- Regularly test firewall configurations for vulnerabilities and adjust settings accordingly.
- Regularly review firewall logs and alerts to identify and respond to suspicious activities promptly.

6.4 Asset Protection

Securing the infrastructure begins with identifying and prioritizing assets critical to the company. This knowledge allows organizations to tailor security controls effectively. Asset protection is vital for SMBs to safeguard valuable data and resources. For instance, neglecting software updates can expose systems to known vulnerabilities, risking data breaches and financial losses. In cloud environments, SMBs must implement key security controls to safeguard assets effectively (Thompson 2020).

Application Security: Ensuring the security of cloud-based applications is a critical aspect of cloud security for SMBs. Implementing robust application security measures involves various practices and considerations. Firstly, employing a Secure Software Development Lifecycle (SSDLC) helps in integrating security into every phase of the application development process, from initial design to deployment. Additionally, designing and architecting applications with security in mind can greatly enhance their resilience against cyber threats. Moreover, embracing DevOps and Continuous Integration/Continuous Deployment (CI/CD) methodologies can streamline the development and deployment of cloud applications while introducing new security considerations and opportunities. It's important to note that addressing application security can be a substantial undertaking and may require a phased approach, allowing organizations to study and implement security measures gradually to ensure effectiveness and minimize disruptions.

Vulnerability Management: Employ cloud vulnerability scanners to detect and address misconfigurations and vulnerabilities promptly. Proactive vulnerability management enhances the organization's overall security posture by identifying and remediating potential security weaknesses before they can be exploited by malicious actors.

Software and System Updates: Ensure all software and systems are kept up to date with the latest patches and updates to mitigate known vulnerabilities effectively. Regularly applying patches and updates reduces the risk of known vulnerabilities' exploitation, helping maintain a secure and resilient cloud environment.

Endpoint Protection: Deploy endpoint protection platforms (EPP) with anti-malware and anti-phishing capabilities to defend against endpoint threats. Endpoint protection is crucial for securing devices connected to the cloud environment, such as laptops, desktops, and mobile devices, from malware infections and phishing attacks that could compromise sensitive data.

Configuration Management: Utilize the security baseline cloud providers provide and integrate it with security for expedited resolution of misconfigurations and vulnerabilities. Configuration management ensures that cloud resources are correctly configured to meet the best security practices and compliance requirements, reducing the risk of unauthorized access and data breaches. Regular monitoring and auditing of configurations help maintain the integrity and security of the cloud environment over time.

6.5 Logging and Monitoring

Implementing robust logging and monitoring mechanisms within a cloud environment is necessary for compliance and for ensuring the security of small and medium businesses (SMBs). By enabling and monitoring security logs, organizations can effectively detect and respond to potential threats in real-time. Enabling logging functionality within cloud services is a foundational step in cloud security strategy. It allows system administrators and security teams to monitor user activities and identify any unauthorized modifications or suspicious behavior. This level of visibility would be difficult, if not impossible, to achieve manually. Furthermore, logging provides a clear record of actions taken by attackers in the event of a security breach, facilitating swift remediation to mitigate potential damage. As the organization grows, managing and corelating logs becomes challenging. In such cases, incorporating a Security Information and Event Management (SIEM) system further enhances the effectiveness of logging. By ingesting log data into a centralized SIEM platform, SMBs can streamline the monitoring and response process. SIEM tools provide advanced analytics and correlation capabilities, enabling quick identification of security incidents and proactive threat mitigation. Effective logging is crucial for compliance and Incident Response. It offers real- time visibility into system activities and security threats. With comprehensive logging, organizations can quickly detect, investigate, and respond to security incidents, identifying the root cause and implementing necessary remediation measures to mitigate risks and prevent future occurrences.

6.6 Training and Awareness

In safeguarding SMBs against cyber threats in the cloud, employee awareness and action play a crucial role. Human error is a common vulnerability, making comprehensive security training essential. Employees need to be trained to identify potential cyber threats, such as phishing emails or suspicious website links. Strong passwords are vital for protecting cloud accounts, so employees should learn how to create and maintain robust passwords. Social engineering tactics can trick employees into divulging sensitive information, so training should focus on recognizing and thwarting such tactics. Moreover, training in incident identification and reporting is equally important. Employees should be equipped with the skills to recognize unusual activities or potential security breaches and know-how to report them promptly to the designated authorities. This proactive approach ensures that security incidents are addressed promptly, minimizing their impact on the organization. Additionally, employees should grasp the broader implications of cybersecurity risks for the organization and understand their role in mitigating risks. Educating employees about the risks associated with unauthorized tools can help minimize shadow IT threats. Continuous training for security staff ensures they remain up to date on emerging threats and effective defense strategies. By investing in clear and concise security training tailored to SMBs, businesses can empower their employees to effectively protect against cyber threats in the cloud.

7. CSP Services and other free resources

SMBs can utilize the cloud provider services listed in Table 1 along with the open-source resources referenced in this section to deploy the controls outlined in the previous section.

Other Free Resources

SANS Cloud Security Tools: SANS offers over 150 open-source tools curated by instructors, covering a wide range of areas such as threat detection, vulnerability assessment, and incident response. These tools empower SMBs to proactively identify and address security risks in their cloud environments.

CIS Hardened Images: The Center for Internet Security (CIS) provides pre-configured hardened images for major cloud platforms such as AWS, Azure, and GCP. These images come with security configurations and settings that help SMBs strengthen the security of their cloud deployments, reducing the risk of common threats and vulnerabilities.

OWASP Cloud-Native Security Top 10: OWASP's guide outlines the top risks and best practices for securing cloud-native environments. SMBs can use this resource as a roadmap to implement effective security measures that address the unique challenges of cloud environments, ensuring the protection of their data and applications.

CISA Cloud Security Factsheet: The Cybersecurity and Infrastructure Security Agency (CISA) has developed a factsheet specifically tailored for businesses transitioning into the cloud. This resource equips SMBs with essential information about the proper tools and techniques necessary for protecting critical assets and ensuring data security in the cloud.

8. Conclusion

In conclusion, as Small and Medium-sized Businesses (SMBs) increasingly adopt cloud technology, the need for robust cloud security measures is paramount. With the rapid growth of the global cloud computing market, SMBs face significant security challenges, compounded by limited resources and awareness of cybersecurity risks. This paper has provided practical guidance for SMBs to implement effective cloud security controls, recognizing the shared responsibility between Cloud Service Providers and Consumers. By addressing common cloud security risks such as unmanaged attack surfaces, human error, misconfigurations, and data breaches, SMBs can establish a resilient security posture. Recognizing the critical importance of cloud security in maintaining the confidentiality, integrity, and availability of sensitive data is paramount for SMBs. Understanding the shared responsibility model enables SMBs to allocate resources effectively and implement appropriate security controls in collaboration with cloud service providers. Key preparatory measures outlined in this paper, including leadership commitment, risk management, budget allocation, and appointing a dedicated cloud security lead, lay the foundation for a robust security framework. SMBs can benefit from leveraging the knowledge provided in this paper to implement security controls with limited resources and budget. By following the guidance and resources provided for access management, data protection, asset protection, network security, logging and monitoring, and employee training and awareness, SMBs can create a strong shield against attackers, thrive, and contribute to a positive economy (Table 1).

Table 1. CSP Security Services

Security Control	AWS	Microsoft Azure	Google Cloud Platform (GCP)
Identity and Access Management (IAM)	AWS IAM, AWS MFA	Azure Active Directory, role-based access control (Azure RBAC), Azure Active Directory External Identities, Azure AD	BeyondCorp Enterprise, IAM, Identity Platform, Identity-Aware Proxy, Google Authenticator, Titan Security Key
Data Security	Amazon Macie	Data Catalog, Azure Information Protection	Data Catalog, Cloud Data Loss Prevention
Key management	AWS Key Management Service, AWS CloudHSM	Key Vault, Azure Dedicated HSM	Cloud Key Management
Archival storage	S3 Glacier	Deep Archive	Archive Storage
Backup	AWS Backup	Azure Backup	Managed backup and disaster recovery (DR)
Virtual Private Cloud (VPC)	Amazon VPC, VPC Traffic Mirroring	Azure Virtual Network, Network Watcher	Virtual Private Cloud, VPC Flow Logs and Packet Mirroring
Firewall management	AWS Firewall Manager, AWS Network Firewall	Azure Firewall Manager, Web Application Firewall	Cloud Armor, Cloud firewalls
Intrusion Detection Systems (IDS)	AWS GuardDuty	Azure Security Center	Cloud IDS
Vulnerability scanning and Application Security	Amazon Inspector, AWS Web Application Firewall (WAF)	Security Center, Azure WAF	Web Security Scanner
Distributed denial-of-service (DDoS)	AWS Shield	Azure DDoS Protection	Google Cloud Armor
Threat Detection	Amazon GuardDuty	Microsoft Azure Attestation, Azure Defender, Azure	Chronicle, Phishing Protection, Web Risk, Event Threat Detection (preview)
Logging and Monitoring	AWS CloudTrail, Cloud-watch, SNS	Azure sentinel	cloud audit logging, cloud monitoring, cloud security command center (Cloud SCC)
Centralized security management	AWS Security Hub	Security Center	Security Command Center

Acknowledgements

This research is funded by Mitacs Canada (https://www.mitacs.ca/) and Treefort Technologies Incorporated (https://treeforttech.com/).

References

Ahmadi, S., Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies, Journal of Information Security, vol. 15, pp. 148-167, 2024.

Alrasheed, S. H., Aied alhariri, M., Adubaykhi, S. A., & El Khediri, S., Cloud Computing Security and Challenges: Issues, Threats, and Solutions, 5th Conference on Cloud and Internet of Things (CIoT), pp. 166-172, Marrakech, Morocco, 2022, doi: 10.1109/CIoT53061.2022.9766571.

Arcserve, 7 most infamous cloud security breaches, 2023. Available at: https://www.arcserve.com/blog/7-most-infamous-cloud-security-breaches. Accessed 24 November 2024.

Brook, C., What are privileged accounts? Common types security risks, 2023. Available at: https://www.digitalguardian.com/blog/what-are-privileged-accounts-common-types-security-risks. Accessed 24 November 2024.

Chauhan, M., & Shiaeles, S., An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions, Network, vol. 3, no. 3, pp. 422-450, 2023.

Chaudhuri, A., Sarkar, S., & Bala, P. K., Thematic Exploration and Analysis of Cybersecurity Policies of Businesses: An NLP-Based Approach, Journal of Organizational Computing and Electronic Commerce, pp. 1-31, 2024.

Coker, J., Human error the leading cause of cloud data breaches, 2023. Available at: https://www.infosecurity-magazine.com/news/human-error-cloud-data-breaches//. Accessed 24 November 2024.

Cybersecurity and Infrastructure Security Agency, Cloud security technical reference architecture v.2, 2022. Available at: https://www.cisa.gov/sites/default/files/2023-02/cloud_security_technical_reference_architecture_2.pdf. Accessed 24 November 2024.

Dotson, C., Practical cloud security, 2nd edition, O'Reilly Media, Inc., 2023.

Esposito, B., Minimalize privileged access management security risks, 2023. Available at: https://www.oneidentity.com/community/blogs/b/privileged-access-management/posts/staying-ahead-of-privileged-access-management-security-risks-success-strategies. Accessed 24 November 2024.

Flynn, J., 17 essential multi-factor authentication (MFA) statistics [2023], 2023. Available at: https://www.zippia.com/advice/mfa-statistics/. Accessed 24 November 2024.

Gapinski, A., Cloud Computing: Information Security Standards, Compliance and Attestation, The Thirteenth Latin American and Caribbean Conference for Engineering and Technology, pp. 1-1, 2015, Lima, Peru, 2015.

Harris, C., 50 cloud security stats you should know in 2024, 2024. Available at: https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/. Accessed 24 November 2024.

Hassan, J., Shehzad, D., Habib, U., Aftab, M. U., Ahmad, M., Kuleev, R., & Mazzara, M., The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges-A Systematic Literature Review (SLR), Comput Intell Neurosci, vol. 2022, pp. 8303504, 2022.

Jillson, E., Hasty, A., Six steps toward more secure cloud computing, 2020. Available at: https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing. Accessed 24 November 2024.

Kumar, P. R., Raj, P. H., & Jelciana, P., Exploring Data Security Issues and Solutions in Cloud Computing, Procedia Computer Science, vol. 125, pp. 691-697, 2018.

Puzas, D., 12 cloud security issues: Risks, threats, and challenges, 2024. Available at: https://cs-staging-22-www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/ Accessed 24 November 2024.

Ramachandra, G., Iftikhar, M., & Khan, F. A., A Comprehensive Survey on Security in Cloud Computing, Procedia Computer Science, vol. 110, pp. 465-472, 2017.

Stansfield, T., Verizon Data Breach Investigations Report 2023: Our Top Takeaways, 2023. Available at: https://www.vadesecure.com/en/blog/verizon-data-breach-report-2023. Accessed 24 November 2024.

Thompson, G., CCSK Certificate of Cloud Security Knowledge All-in-one exam guide, McGraw-Hill, 2020.

ThreatModeler, Understanding live cloud environment and threat modeling, 2023. Available at: https://threatmodeler.com/how-do-you-threat-model-in-a-live-cloud-environment/. Accessed 24 November 2024.

Zhang, N., Liu, D., & Zhang, Y., A Research on Cloud Computing Security, International Conference on Information Technology and Applications, pp. 370-373, Chengdu, China, 2013.

Biographies

Pooja Shah is a Data Security Analyst at Canadian Western Bank. She got her Master of Information Systems Security Management (MISSM) from Concordia University of Edmonton in Alberta, Canada in April 2024.

Siddharth Dua, CISA, CISM is a Security Governance, Risk and Compliance Analyst at Canadian Western Bank. He got his Master of Information Systems Assurance Management (MISAM) from Concordia University of Edmonton in Alberta, Canada in April 2024.

Eslam G. AbdAllah is an Associate Professor at Concordia University of Edmonton, AB, Canada, where he currently serves as the chair of the Information Systems Security and Assurance Management (ISSAM) Department. He joined Concordia University of Edmonton as an Assistant Professor in July 2020. Prior to his tenure at Concordia, Dr. AbdAllah was a postdoctoral fellow at the Department of Systems and Computer Engineering at Carleton University, ON, Canada. His academic journey also includes working as an Assistant Professor at the Faculty of Computer and Information Sciences in Ain Shams University, Egypt. Dr. AbdAllah earned his PhD from the School of Computing at Queen's University in Kingston, ON, Canada, in 2017. Throughout his career, he has made contributions to the field, reflected in publications in journals, technical papers, and reports. He has been recognized with scholarships and awards from NSERC, MITACS, and industry partners.