CIS Microsoft AzureGoat Build Gap Analysis

CloudStrategik Consulting

Effective Date: September 9, 2024
Version: 1.0

Prepared by: CloudStrategik Consulting
Anderson@cloudstrategik.com

Confidentiality Statement

This document contains proprietary and confidential information of CloudStrategik Consulting. The information contained herein is disclosed to the recipient in confidence for the sole purpose of internal use. No part of this document may be disclosed, reproduced, or distributed without the prior written consent of CloudStrategik Consulting.

Assessment Title:	CIS Microsoft Azure Gap Analysis
Assessment Owner:	Anderson Anthony, Chief Compliance Officer
Effective Date:	September 9, 2024
Revised Date:	-

Contents

1 Introduction

This document presents a detailed gap analysis of the AzureGoat setup in relation to the CIS Microsoft Azure Foundations Benchmark. AzureGoat serves as a purposely misconfigured Azure environment, designed to illustrate common security vulnerabilities. This analysis aims to uncover compliance gaps and recommend necessary remediation measures.

2 Scope of Analysis

The scope of this assessment encompasses all Azure services within the AzureGoat environment, with a focus on security configurations and compliance with CIS benchmarks. The areas evaluated include:

- Identity and Access Management
- Network Security
- Virtual Machines
- Storage Accounts
- Database Services
- Logging and Monitoring
- Data Protection
- Microsoft Defender
- App Services
- Key Vault

Each area will be scrutinized against the relevant CIS Microsoft Azure Foundations Benchmark controls to identify security deficiencies and non-compliant configurations.

3 Detailed Gap Analysis

3.1 Identity and Access Management

Identity and Access Management (IAM) is fundamental to controlling access to Azure resources. The following table highlights the current IAM configurations in AzureGoat and their compliance status:

CIS Control	Description	Current Status	Compliance

1.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID	Not Configured	No
1.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users	Partially Configured	No
1.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users	Configured	Yes
1.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled	Configured	Yes

The analysis shows notable gaps in IAM security. The absence of Security Defaults and inconsistent Multi-Factor Authentication (MFA) for privileged users present considerable risks, potentially allowing unauthorized access and privilege escalation.

3.2 Networking

Network security is critical for safeguarding Azure resources. The AzureGoat environment's network configurations are reviewed as follows:

CIS Control	Description	Current Status	Compliance
2.1.1	Ensure NSGs are used for all virtual networks and subnets	Partially Configured	No
2.1.2	Secure access to subnet resources using NSGs	Configured	No
2.1.3	Disable public access to Azure SQL Database services	Not Configured	No
2.1.4	Ensure encryption for Azure SQL Database and MySQL	Configured	Yes

The network configuration reveals critical vulnerabilities, including inadequate use of Network Security Groups (NSGs) and lack of access control for Azure SQL Database services. These issues could result in unauthorized access and data exposure.

3.3 Virtual Machines

Virtual Machines (VMs) are integral to many Azure setups. The security configurations for VMs in AzureGoat are examined as follows:

CIS Control	Description	Current Status	Compliance
3.1.1	Ensure VM disks are encrypted	Not Configured	No
3.1.2	Secure access to virtual machines	Configured	No

3.1.3	Regular updates and patch management for VMs	Not Configured	No
3.1.4	Enable monitoring and logging for VMs	Partially Configured	No

Significant security gaps are identified in VM configurations, including unencrypted disks, inadequate access controls, and absence of regular updates. These misconfigurations heighten vulnerability to data breaches and system compromises.

3.4 Storage Accounts

Azure Storage Accounts manage various data types and require robust security. The following table presents the security status of storage accounts in AzureGoat:

CIS Control	Description	Current Status	Compliance
4.1.1	Ensure storage account encryption is enabled	Not Configured	No
4.1.2	Restrict access to storage accounts using Network Rules	Partially Configured	No
4.1.3	Enable secure transfer for storage accounts	Configured	Yes
4.1.4	Ensure diagnostic logging is enabled for storage accounts	Configured	Yes

The storage account configurations display gaps such as lack of encryption and partial implementation of access controls. These issues could lead to unauthorized data access and loss of data integrity.

3.5 Database Services

Database services are vital for data management in Azure. The security configurations for database services in AzureGoat are reviewed:

CIS Control	Description	Current Status	Compliance
5.1.1	Ensure database encryption is enabled	Configured	Yes
5.1.2	Disable public access to databases	Not Configured	No
5.1.3	Enable auditing and monitoring for databases	Partially Configured	No
5.1.4	Restrict database access using firewall rules	Partially Configured	No

The database service configurations reveal gaps such as lack of public access restrictions and incomplete auditing. These deficiencies expose databases to potential attacks and unauthorized access.

3.6 Logging and Monitoring

Effective logging and monitoring are essential for security and compliance. The security configurations for logging and monitoring in AzureGoat are assessed:

CIS Control	Description	Current Status	Compliance
6.1.1	Ensure Azure Monitor is configured for all resources	Configured	Yes
6.1.2	Enable diagnostic logging for all Azure services	Partially Configured	No
6.1.3	Store logs in a centralized location	Configured	Yes
6.1.4	Ensure alerts are set for critical security events	Not Configured	No

While Azure Monitor and centralized log storage are in place, gaps in diagnostic logging and alert configurations are present. These issues could hinder timely detection of security incidents.

3.7 Data Protection

Data protection ensures confidentiality and integrity of data. The security settings for data protection in AzureGoat are examined:

CIS Control	Description	Current Status	Compliance
7.1.1	Enable encryption at rest for all data	Configured	Yes
7.1.2	Enable encryption in transit for all data	Configured	Yes
7.1.3	Ensure backup data is encrypted	Partially Configured	No
7.1.4	Implement data retention policies	Not Configured	No

Data protection configurations show encryption is in place for data at rest and in transit, but there are gaps in backup encryption and data retention policies. These gaps could result in data breaches and non-compliance with retention requirements.

3.8 Microsoft Defender

Microsoft Defender provides security for Azure resources. The configuration status of Microsoft Defender in AzureGoat is assessed:

CIS Control	Description	Current Status	Compliance
8.1.1	Ensure Microsoft Defender is enabled for all subscriptions	Configured	Yes
8.1.2	Enable Microsoft Defender for Servers	Not Configured	No

8.1.3	Enable Microsoft Defender for SQL	Partially Configured	No
8.1.4	Configure Microsoft Defender alerts and recommendations	Partially Configured	No

Microsoft Defender configurations show some components enabled, but gaps are present in coverage for servers and SQL databases, and in the configuration of alerts. These gaps could lead to undetected threats and security vulnerabilities.

3.9 App Services

Azure App Services host web applications and APIs. The security configurations for App Services in AzureGoat are reviewed:

CIS Control	Description	Current Status	Compliance
9.1.1	Ensure App Service environments are configured securely	Not Configured	No
9.1.2	Enable Web Application Firewall (WAF) for App Services	Partially Configured	No
9.1.3	Ensure SSL/TLS is enforced for all App Service endpoints	Configured	Yes
9.1.4	Implement app configuration settings securely	Partially Configured	No

App Services configurations indicate gaps in secure environment configurations and Web Application Firewall (WAF) implementation. These gaps could expose applications to web-based attacks and data breaches.

3.10 Key Vault

Azure Key Vault is essential for managing sensitive information. The security settings for Key Vault in AzureGoat are assessed:

CIS Control	Description	Current Status	Compliance
10.1.1	Ensure Key Vault is configured with access policies	Configured	Yes
10.1.2	Enable logging and monitoring for Key Vault	Partially Configured	No
10.1.3	Rotate secrets and keys regularly	Not Configured	No
10.1.4	Ensure Key Vault encryption settings are enabled	Configured	Yes

The Key Vault settings show that while some configurations are in place, there are gaps in logging, monitoring, and secret/key rotation. These issues could impact the security and manageability of sensitive information.

4 Recommendations

To address the identified gaps and enhance security posture, the following recommendations are made:

- Enable Security Defaults and enforce Multi-Factor Authentication (MFA) for all users.
- Improve network security by using NSGs and restricting public access to sensitive services.
- Ensure all VMs have encrypted disks and implement regular patching and updates.
- Configure encryption for all storage accounts and enforce access controls.
- Restrict public access to database services and improve auditing and access controls.
- Enhance logging and monitoring configurations, including setting up alerts for critical events.
- Implement encryption and data retention policies for data protection.
- Enable and properly configure Microsoft Defender for all relevant services.
- Secure App Services environments and implement Web Application Firewall (WAF) protections.
- Improve Key Vault configurations by enabling comprehensive logging and key rotation.

5 Conclusion

The gap analysis highlights significant security vulnerabilities within the AzureGoat environment. Addressing these gaps is essential for achieving compliance with the CIS Microsoft Azure Foundations Benchmark and improving overall security. Implementing the recommended actions will enhance security and reduce risks.

6 Appendices

6.1 Appendix A: CIS Controls V8

1. CIS Control 1: Inventory and Control of Enterprise Assets
2. CIS Control 2: Inventory and Control of Software Assets
3. CIS Control 3: Data Protection
4. CIS Control 4: Secure Configuration of Enterprise Assets and Software

5. CIS Control 5: Account Management
6. CIS Control 6: Access Control Management
7. CIS Control 7: Continuous Vulnerability Management
8. CIS Control 8: Audit Log Management
9. CIS Control 9: Email and Web Browser Protections
10. CIS Control 10: Malware Defenses
11. CIS Control 11: Data Recovery
12. CIS Control 12: Network Security
13. CIS Control 13: Security Awareness and Skills Training
14. CIS Control 14: Application Security
15. CIS Control 15: Incident Response Management
16. CIS Control 16: Penetration Testing

7 Document Revision History

Version	Date	Description of Changes	Author
1.0	08/07/2024	Initial document creation	A. Anthony
1.1	08/07/2024	Updated with Salesforce-specific details	A. Anthony

8 Approval

This document has been reviewed and approved by:

Name:	**Signature:**
Title:	**Date:**
Name:	**Signature:**
Title:	**Date:**

9 Disclaimer

This gap assessment report is based on information available at the time of the assessment and may not reflect all potential vulnerabilities or risks. It is recommended to regularly review and update security measures as new threats emerge and technology evolves.

10 Contact Information

For any questions or clarifications regarding this report, please contact:

Name: Anderson Anthony
Title: Chief Compliance Officer
Email: Anderson@cloudstrategik.com
Phone: +1 (555) 123-4567