NAME: MBA NONNA
CYBER ID: 12533987
PROJECT 4
IT AUDIT TESTING OF CONTROLS

IT AUDIT REPORT FOR GOOGLE WORKSPACE

PREPARED FOR: Management Team, Google.
PREPARED BY: Mba Nonna.

INTRODUCTION

As cloud technologies continue to revolutionize workplace operations, ensuring secure access to cloud-based platforms like Google Workspace are crucial for maintaining confidentiality, integrity, and availability of organizational data. Google Workspace is a widely adopted suite that integrates email, cloud storage, document collaboration, and administrative tools, supporting millions of users across various industries.

Given the platform's broad reach and its critical role in day-to-day operations, maintaining strong access controls is imperative. Unauthorized access can lead to data breaches, operational disruption, or non-compliance with data protection regulations. This audit was initiated to evaluate the effectiveness of the access control mechanisms within Google Workspace, particularly focusing on Two-Factor Authentication (2FA) and Role-Based Access Control (RBAC). These mechanisms are essential in preventing unauthorized access and ensuring users operate within appropriate boundaries based on their roles.

The aim is to identify any weaknesses in current implementations, propose corrective actions, and align security practices with industry standards such as ISO 27001 and NIST SP 800-53. A strong access control framework will not only mitigate security risks but also reinforce trust among stakeholders and ensure operational resilience.

AUDIT PROCESS

The audit process on Google Workspace was conducted using the audit cycle below;

- Planning (Audit Objective and Scope).
- Kick-Off Meeting.
- Field Work.
- Reporting.
- Exit Meeting

PLANNING

Audit Objective

The objective of this audit is to evaluate the effectiveness of access control mechanisms within Google Workspace, focusing on Two-Factor Authentication (2FA) and Role-Based Access Control (RBAC). The audit aims to determine whether these controls are properly implemented to prevent unauthorized access, ensure users have only the permissions necessary for their roles, and support compliance with security best practices and standards such as ISO 27001 and NIST SP 800-53.

Audit Scope

The scope of this audit includes:

- **Review of Two-Factor Authentication (2FA) Enforcement:**
  This assesses whether 2FA is consistently applied across all user accounts to enhance login security and prevent unauthorized access.
- **Assessment of Role-Based Access Control (RBAC) Implementation:**
  This evaluates whether users are granted only the minimum necessary permissions based on their job responsibilities.
- **Policy Documentation Analysis:**
  This involves reviewing formal security policies to ensure they clearly define access control requirements and responsibilities.
- **Logging and Monitoring Setup:**
  This checks if access logs are maintained, reviewed regularly, and capable of detecting suspicious or unauthorized activity.
- **Compliance with Standards (e.g., ISO 27001, NIST SP 800-53):**
  This determines whether the organization’s access controls align with internationally recognized cybersecurity frameworks.

KICK-OFF MEETING

Participants;

- IT Security Manager.
- Google Workspace Administrator.
- Internal Audit Team Lead.
- HR Systems Officer.

Agenda;

- Review Audit Scope and Deliverables.
- Grant Necessary Access to Systems and Logs.
- Establish Communications and Timelines.
- Schedule Final Reporting and Exit Meeting.

FIELD WORK

1. Examination

A detailed review of relevant documents, systems, and logs was conducted to assess the design and implementation of access controls. This included:

- **Policy Review:** Examination of Google Workspace access control policies, including account provisioning, role-based access assignments, and authentication enforcement.
- **Log Analysis:** Analysis of audit logs such as login attempts, device access, and administrative activity to verify compliance with internal policies and detect anomalies.
- **Access Provisioning Procedures:** Review of workflows for onboarding and offboarding users, including HR-IT coordination and policy documentation.

2. Interview

Discussions were held with key stakeholders to understand the practical application of access controls and uncover any implementation gaps. This included:

- **IT Security Team:** To assess the current use and enforcement of 2FA and RBAC within Google Workspace and gather insight into any technical limitations.
- **HR and Admin Personnel:** To review the deprovisioning process and identify delays or inconsistencies in account removals following staff departures.
- **End Users:** To understand user experiences with authentication mechanisms and identify any usability challenges or security workarounds.

3. Testing

Hands-on testing was performed to validate the operational effectiveness of access controls in real-world scenarios. Activities included:

- **Authentication Testing:** Attempted unauthorized logins to confirm the enforcement and functionality of Two-Factor Authentication (2FA).
- **Access Permissions Testing:** Role simulation exercises were conducted to ensure that permissions were appropriately defined and enforced based on user responsibilities.
- **Configuration Review:** Evaluated admin console settings and delegated roles to identify any unnecessary privileges or overlooked security configurations.

REPORTING

Key findings and observations were documented based on evidence collected during the fieldwork phase. A Corrective Action Plan was developed to address the identified issues and provide practical recommendations for improvement.

1. Strengths:

- Enforcement of Two-Factor Authentication (2FA) for administrators and support for security key-based authentication.
- Role-Based Access Control (RBAC) framework allows for flexible, scalable permission assignments.

- Centralized audit logging and visibility into user and administrator activities.

2. Weaknesses:

- 2FA was not consistently enforced across all user accounts, leaving gaps in protection.
- Some users were assigned permissions beyond what was required for their job functions.
- Manual offboarding processes increased the risk of orphaned accounts remaining active after employee departures.

EXIT MEETING

The findings and recommended corrective actions were presented to key stakeholders during the exit meeting. Feedback was incorporated into the final report, and agreement was reached on implementation priorities and timelines. A follow-up review was scheduled for three months after the audit to ensure that the corrective actions are implemented effectively and that compliance with new policies is being maintained.

CORRECTIVE ACTION PLAN

Finding	**Impact**	**Corrective Action**	**Timeline**	**Responsible Party**
Inconsistent 2FA enforcement	Risk of credential theft from phishing or brute-force attacks	Enforce 2FA for all accounts using Admin Console policy enforcement and periodic compliance reviews	1 month	IT Security Team
Over-provisioning of user roles	Increased exposure to unauthorized actions and data leakage	Review and redefine roles with least privilege principles; implement quarterly permission audits	2 months	Workspace Admin
Lack of automated deprovisioning	Former employees retain access beyond termination	Integrate HRIS with Google Workspace for real-time user deactivation	1 month	IT and HR Team

AUDIT REPORT

To: Senior Management
From: IT Audit Team
Subject: Access Control Audit – Google Workspace
Date: April 2025.

EXECUTIVE SUMMARY

This audit assessed access control mechanisms within Google Workspace, focusing on Two-Factor Authentication (2FA) and Role-Based Access Control (RBAC). While Google Workspace offers robust native security tools, enforcement gaps were identified. These include inconsistent application of 2FA and role overprovisioning, which could lead to unauthorized access and potential data breaches.

METHODOLOGY

- **Documentation Review:** Access policies and system configuration guides.
- **Testing:** Simulated login and role assignment tests.
- **Log Analysis:** Reviewed security logs for anomalies and compliance.
- **Interviews:** Gathered feedback from IT and HR stakeholders.

FINDINGS

Strengths

- Built-in audit logging and device management features
- Flexible 2FA methods (Authenticator apps, security keys)
- Transparent admin activity tracking

Weaknesses

- 2FA not enforced for all user groups
- Broad role permissions without documentation
- Manual user deactivation post-termination

RECOMMENDATIONS

1. **Mandatory 2FA Enforcement**
   Apply organization-wide 2FA enforcement policies and send periodic compliance reminders.
2. **Role Review and Access Minimization**
   Redesign custom admin roles following the principle of least privilege.
3. **Automated Offboarding**
   Integrate HR termination workflows with Workspace to automatically suspend or delete accounts.

CONCLUSION

The audit confirms that Google Workspace provides a comprehensive framework for access control, offering administrators a variety of tools to manage users, monitor activities, and enforce security standards. However, as with any system, the effectiveness of these tools depends on consistent and disciplined implementation.

Key areas such as 2FA enforcement, appropriate role assignment, and automated deprovisioning were identified as needing improvement. These gaps, if left unaddressed, could expose the organization to credential theft, data leaks, or regulatory violations.

By implementing the corrective actions outlined in this report—namely enforcing mandatory 2FA, minimizing privilege through refined roles, and integrating HR systems for automated offboarding—the organization will significantly strengthen its cybersecurity posture. Moreover, ongoing training, audits, and policy updates will ensure these controls remain effective as the threat landscape evolves.

Ultimately, this audit serves as a proactive measure to safeguard organizational data, enhance user accountability, and promote a culture of continuous security improvement.

APPENDICES & REFERENCES

Appendix A: Interview Participants

- IT Security Manager – Oversight of Workspace access policies and enforcement.
- Google Workspace Administrator – Configuration and monitoring of user access.
- HR Systems Officer – Coordination of employee onboarding and offboarding processes.
- End-User Representatives – Feedback on practical challenges with access protocols.

Appendix B: Tools and Resources Used

- Google Workspace Admin Console
- Google Audit Log Viewer
- Policy documentation from internal IT governance repository
- NIST Cybersecurity Framework
- ISO/IEC 27001:2022 Implementation Guidelines

Appendix C: Audit Checklist Snapshot

- Is 2FA enforced across all users?
- Are administrative roles appropriately scoped?
- Are access logs actively reviewed?
- Is account deactivation automated through HRIS integration?
- Are audit logs retained per policy requirements?

References

1. **Google Workspace Security Documentation**
   https://support.google.com/a/topic/7582924
2. **ISO/IEC 27001:2022 Standards** – International Organization for Standardization
3. **NIST Special Publication 800-53 (Rev. 5)** – Security and Privacy Controls for Information Systems
4. **Google Admin Help Center** – https://support.google.com/a

5. Internal IT Policy Manual, Google.
6. Employee Onboarding & Offboarding Procedures, HR Department

APPROVAL

Senior IT Auditor

IT AUDIT REPORT FOR CISCO ANYCONNECT VPN

PREPARED FOR: Management Team, Cisco AnyConnect VPN Solution.
PREPARED BY: Mba Nonna.

INTRODUCTION

With the growing adoption of remote work, Virtual Private Network (VPN) solutions have become essential for providing secure access to internal organizational resources. Cisco AnyConnect is a widely used VPN platform offering secure mobility and endpoint control for enterprise users. Given its role in enabling offsite access to sensitive systems, it is crucial to ensure that the access controls associated with AnyConnect are both robust and effectively enforced.

This audit was conducted to assess the access control environment for Cisco AnyConnect VPN, focusing specifically on the implementation and effectiveness of Two-Factor Authentication (2FA) and Role-Based Access Control (RBAC). The goal was to identify any gaps in policy, configuration, or usage that could compromise the confidentiality and integrity of organizational data. In doing so, this audit supports the organization's commitment to a secure digital workplace and compliance with relevant cybersecurity frameworks such as ISO 27001 and NIST SP 800-53.

AUDIT PROCESS

The audit process followed a structured IT audit methodology to ensure thorough evaluation and actionable insights. The key stages included:

- Planning (Audit Objective and Audit Scope)
- Kick-Off Meeting
- Field Work
- Reporting
- Exit Meeting

PLANNING

Audit Objective

The objective of this audit is to evaluate the access controls implemented in the Cisco AnyConnect VPN platform, specifically focusing on Two-Factor Authentication (2FA) and Role-Based Access Control (RBAC). The audit aims to assess whether these controls are configured effectively to prevent unauthorized access, whether they align with cybersecurity best practices, and whether they are consistently applied across all users.

Audit Scope

- **Two-Factor Authentication (2FA):** Assessing enforcement and configuration across different user categories.
- **Role-Based Access Control (RBAC):** Reviewing user profiles and permissions within the VPN.
- **Policy Documentation:** Verifying access control policies are comprehensive and up to date.
- **Logging and Monitoring:** Evaluating VPN access logs for anomaly detection and incident response.
- **Standards Compliance:** Comparing current configurations to ISO 27001 and NIST SP 800-53 guidelines.

KICK-OFF MEETING

Participants;

- IT Security Manager
- Network Administrator
- HR Systems Officer
- Internal Audit Team

Agenda;

- Confirm audit objectives and scope.
- Grant access to VPN logs and configuration interfaces.
- Discuss VPN user groups and existing security challenges.
- Establish timeline and deliverables.

FIELDWORK

The fieldwork phase of the audit involved the following processes to comprehensively evaluate Cisco AnyConnect's access controls.

1. Examination

A detailed review of relevant documents, systems, and logs was conducted to assess the design and implementation of access controls. This included:

- **Policy Review:** Examination of Cisco AnyConnect access control policies, VPN group profiles, and multifactor authentication requirements.

- **Log Analysis:** Analysis of VPN access logs to verify account activity, detect unusual login patterns, and review session behavior.
- **Configuration Inspection:** Review of firewall, authentication, and authorization settings within the VPN management interface.

2. Interview

Discussions were conducted with key stakeholders to gain insight into the practical application of VPN access controls and uncover any process gaps:

- **IT Security Team:** To validate the deployment and management of 2FA, certificate usage, and user group assignments.
- **Network Administrator:** To review segmentation of user access based on operational roles and network zones.
- **HR and Admin Teams:** To evaluate offboarding workflows and coordination between HR and IT.

3. Testing

Hands-on testing was conducted to validate the functional security of VPN access under real-world conditions. Activities included:

- **Authentication Testing:** Attempted logins from unauthorized devices and locations to assess 2FA enforcement and geo-restriction effectiveness.
- **Permissions Testing:** Simulated user sessions with varied group access to ensure network segmentation and privilege restrictions were properly enforced.
- **Session Behavior Testing:** Observed idle session termination and auto-logout settings to evaluate risk of unintended access.

REPORTING

Key findings and observations were documented, and a Corrective Action Plan was developed to address identified issues and recommend best practices.

1. Strengths:

- Mandatory 2FA for administrative VPN users via Duo integration.
- Logging and monitoring mechanisms actively track user sessions and generate alerts.
- VPN access is logically segmented by user groups (e.g., Admin, Staff, Contractors).

2. Weaknesses:

- 2FA not consistently enforced for temporary and contractor accounts.
- Role configurations are not regularly reviewed, resulting in outdated permissions for some users.
- Manual deactivation of VPN access during offboarding introduces delays and potential access risks.

EXIT MEETING

The findings and proposed corrective actions were presented to stakeholders during the exit meeting. Feedback was discussed and incorporated into the final report. A follow-up review was scheduled for three months post-audit to assess the implementation of corrective measures and overall compliance improvements.

CORRECTIVE ACTION PLAN

Finding	**Impact**	**Corrective Action**	**Timeline**	**Responsible Party**
Inconsistent 2FA for contractors	Risk of unauthorized remote access	Extend 2FA enforcement to all user categories, including temporary accounts	2 months	IT Security Team
Outdated RBAC configurations	Excessive privileges increase risk of internal threats	Conduct quarterly access reviews and implement role recertification	2 months	Network Administrator
Manual VPN deactivation	Residual access risk for former staff	Integrate HRIS with VPN provisioning system for automated offboarding	1 month	IT & HR Teams

AUDIT REPORT

To: Senior Management
From: IT Audit Team
Subject: Access Control Audit – Cisco AnyConnect VPN
Date: April 2025.

EXECUTIVE SUMMARY

This audit assessed the effectiveness of access control mechanisms in Cisco AnyConnect VPN, with a focus on Two-Factor Authentication and Role-Based Access Control. While strong security features are available and used effectively for core staff, inconsistent enforcement for certain user groups and manual deprovisioning processes represent key risks. The implementation of the proposed corrective actions will help strengthen the security framework and ensure alignment with cybersecurity best practices.

METHODOLOGY

- Policy Documentation Review
- Configuration Inspection
- Log Analysis and Anomaly Detection
- Simulated User Testing
- Stakeholder Interviews

FINDINGS

Strengths;

- Secure authentication via 2FA
- Comprehensive session monitoring
- Group-based access segmentation

Areas for Improvement;

- 2FA not applied to all user groups
- Stale role configurations
- Manual account termination process

RECOMMENDATIONS

To enhance the effectiveness and consistency of access controls within the Cisco AnyConnect VPN environment, the following actions are recommended:

1. **Enforce Two-Factor Authentication (2FA) for All Users**
   Extend 2FA requirements to include all user categories, including contractors, vendors, and temporary employees. This will reduce the risk of unauthorized access due to compromised credentials.
2. **Conduct Regular Role-Based Access Control (RBAC) Reviews**
   Implement quarterly access reviews to ensure users have only the permissions necessary for their current roles. Deactivate or adjust outdated privileges to reduce the potential for misuse.
3. **Automate VPN Offboarding Procedures**
   Integrate HR systems with the VPN platform to automatically revoke access when employees are terminated or transferred. This will close security gaps caused by delays in manual deprovisioning.

4. **Standardize VPN Configuration Policies Across Departments**
   Develop and enforce uniform VPN access policies that apply consistently across departments to ensure compliance and reduce administrative errors.

CONCLUSION

Cisco AnyConnect VPN serves as a critical entry point to the organization's internal network, and while foundational access controls are in place, there are gaps that must be addressed to maintain a secure and compliant environment. The audit identified several strengths, including effective 2FA implementation for core users and solid access segmentation, but also revealed risks related to inconsistent enforcement, outdated permissions, and manual offboarding procedures.

By implementing the recommended corrective actions—such as enforcing 2FA across all user categories, streamlining role-based permissions, and integrating automation into the offboarding process—the organization will significantly enhance its overall security posture. These steps will not only help mitigate current vulnerabilities but will also lay the groundwork for a more agile and responsive access control system.

In the long term, it is crucial to establish a culture of continuous improvement through periodic audits, user training, and policy reviews. Doing so will ensure that access control practices evolve in step with emerging threats and regulatory expectations, protecting both organizational assets and stakeholder trust.

APPENDICES & REFERENCES

Appendix A: Interview Participants

- IT Security Manager
- Network Administrator
- HR Officer
- Selected VPN Users

Appendix B: Tools and Resources Used

- Cisco AnyConnect Secure Mobility Client
- Duo Admin Panel
- Cisco Secure Firewall Dashboard
- NIST SP 800-53
- ISO/IEC 27001:2022

References

1. Cisco AnyConnect Secure Mobility Documentation
2. Duo Security Integration Guide for VPNs
3. ISO/IEC 27001:2022 – Information Security Management
4. NIST Special Publication 800-53 (Rev. 5)
5. Internal VPN Access Policy – Cisco AnyConnect VPN.

6. HR Offboarding Checklist – Cisco AnyConnect VPN.

APPROVAL

Senior IT Auditor