Philocybers Consulting Firm

YESYOUCAN CYBERSECURE, LLC
GRC/IT AUDIT TRAINING — Dallas, Texas, USA

PROJECT 4 — TESTING OF CONTROLS
IT AUDIT REPORT

Prepared by: Oswald Eyram Toku

Deadline: October 10, 2025

Submit to: noahdarkoadjei@cybersecure.work

Confidential — For internal use only

PROJECT 4 (INDIVIDUAL) - TESTING OF CONTROLS

YESYOUCAN CYBERSECURE, LLC
GRC/IT AUDIT TRAINING — Dallas, Texas, USA

Project	PROJECT 4 (INDIVIDUAL) - TESTING OF CONTROLS
Company	Philocybers Consulting Firm (YESYOUCAN CYBERSECURE, LLC)
Prepared by	Oswald Eyram Toku
Target system	Microsoft Active Directory (on-prem AD DS)
Controls tested	MFA Enforcement for Privileged Logons; Privileged Account Provisioning & Review
Deadline / Submission	October 10, 2025 / noahdarkoadjei@cybersecure.work

Contents

1. Executive Summary

This report documents the results of control testing performed on Microsoft Active Directory. Two access controls were tested: (1) Multi-Factor Authentication enforcement for privileged logons, and (2) Privileged account provisioning and periodic review. Testing used a combination of design reviews and non-intrusive operating effectiveness tests (log and ticket reviews). The findings identified gaps in MFA coverage for a small subset of emergency accounts and weaknesses in the documented provisioning/recertification process. Corrective actions are provided in the Corrective Action Plan (CAP) and prioritized for management attention.

2. Introduction

2.1 Background

Microsoft Active Directory (AD) is the organisation's primary authentication and authorization platform. AD manages domain accounts, group memberships, and privileged roles that control access to servers and critical systems. Securing privileged access is essential to prevent account takeover and limit blast radius from compromised credentials.

2.2 Objectives

The objectives of this audit were to: (a) assess whether MFA is enforced for privileged interactive logins, and (b) verify that privileged account provisioning follows approved procedures and periodic recertification.

2.3 Scope

Scope: Microsoft Active Directory domain 'CORP.LOCAL' (production). The assessment covered Domain Admins, Enterprise Admins, and service accounts used for privileged activities. Testing focused on configuration reviews, authentication log analysis (last 90 days), and a sample of provisioning tickets (last 12 months).

2.4 Methodology

The methodology followed a standard IT audit approach, structured around recognized industry frameworks such as **NIST SP 800-53**, **NIST SP 800-30**, **COBIT**, and **COSO**. The process involved **planning and authorization**, defining the **audit scope**, performing **control design reviews**, and applying **sampling techniques** to select evidence for testing. Non-intrusive **operating effectiveness testing** was carried out through log reviews and ticket analysis to verify control implementation. **Evidence collection** supported the validation of control performance, followed by **risk assessment using a 5×5 matrix** to evaluate the likelihood and impact of any identified control gaps. Finally, the results were documented in a formal **audit report**, including **recommended remediation actions** and a plan for **follow-up** to track the resolution of findings.

3. Audit Process

We performed the audit by planning the audit with an understanding of the objective and scope of the audit, then holding a kickoff meeting with the auditee. Key personnel were identified. Fieldwork followed: walkthroughs to confirm control design and detailed testing to verify operating effectiveness. Findings were documented and discussed in an exit meeting. Follow-up will be scheduled based on criticality.

3.1 Planning

Purpose: Define why the audit is being conducted, what will be audited, and how the work will be performed.

Key planning activities

- Senior leadership engagement and initial walkthrough: convene a meeting with senior management to confirm audit mandate, objectives, constraints and initial expectations.
- Define audit objectives: document measurable objectives (for example: “evaluate the design and operating effectiveness of access controls for privileged and non-privileged users”).
- Determine scope: specify systems, business units, locations, and the time period to be reviewed (for example: “Oracle EBS production environment; January–December 2024; all user accounts with application or administrative privileges”).
- Understand the environment: gather information on business processes, IT architecture, system interfaces, and third-party dependencies that are relevant to the scope.
- Review prior evidence: obtain and review prior audit reports, risk assessments, incident histories, and control self-assessments to identify areas of elevated risk and recurring issues.
- Prepare the audit plan: produce a formal audit plan that documents objectives, scope, methodology, sampling approach, resource requirements, roles and responsibilities, timelines and reporting milestones.
- Engagement documentation: where applicable, issue an Engagement Letter (EL) for external engagements and obtain the client’s acknowledgement. Agree on a PBC (Provided-By-Client) list that identifies the evidence and artifacts the client will supply.

Example (objective & scope statement)

- **Objective:** Assess user access controls for the core banking system to determine whether controls are designed appropriately and operating effectively, and to confirm compliance with applicable regulatory requirements (e.g., SOX).
- **Scope:** Review all user access activity and provisioning for the Oracle E-Business Suite (EBS) production environment for the period **1 January 2024 – 31 December 2024**, including privilege assignments, access provisioning/deprovisioning records, periodic access recertifications, and relevant authentication and authorization configurations.

Deliverables from planning

- Approved audit plan and schedule.
- Agreed PBC list and evidence delivery dates.
- List of subject matter experts and points of contact.
- Risk-based priority areas to be tested during fieldwork

3.2 Kick-off Meeting

Purpose:
The kick-off meeting aligns the audit team and the auditee's management on the audit objectives, scope, methodology, timelines and logistics. It establishes the lines of communication, confirms required evidence (PBC list), and ensures both parties understand responsibilities and expected deliverables.

Key objectives of the kick-off meeting

- Introduce the audit team and primary points of contact.
- Confirm and finalize the audit objective and scope (systems, business units, time period).
- Explain the audit methodology and sampling approach.
- Agree the logistics for evidence delivery, fieldwork scheduling and communication channels.
- Set expectations for milestones, reporting cadence, and the exit meeting.
- Clarify any auditee questions and identify immediate risks or pre-existing remediation activities that may affect scope.

Proposed attendees

- Audit team: lead auditor, senior auditor, junior auditor(s).

- Auditee representatives: IT Manager / AD Team Lead, IT Security Manager, Application Owners, Helpdesk Lead.
- Business stakeholders: Department leads relevant to the scope (e.g., Finance, HR) where applicable.
- Optional: Legal / Compliance representative and Project Coordinator.

Recommended duration and format

- Duration: 45–60 minutes (longer if multiple business units are involved).
- Format: Presentation slide deck followed by Q&A and minutes. Convene via virtual meeting or in person as appropriate.

Kick-off Deck (Recommended slides and talking points)

1. **Title & Introductions**
   - Slide: Project title, date, and attendees.
   - Talking points: Team roles, primary contacts, escalation path.
2. **Purpose of the Meeting**
   - Slide: Why we are meeting; alignment goals.
3. **Engagement Overview**
   - Slide: Audit objectives (e.g., evaluate MFA enforcement and privileged provisioning).
   - Slide: Audit scope (systems, environments, timeframe, inclusions/exclusions).
4. **Timeline & Milestones**
   - Slide: Key phases (Planning, Fieldwork, Reporting, Exit).
   - Slide: Start/end dates and milestone due dates (e.g., evidence due, fieldwork window, draft report delivery).
5. **Approach & Methodology**
   - Slide: High-level methodology (design review, sampling, non-intrusive log/ticket analysis).
   - Slide: Tools/techniques to be used (PowerShell exports, SIEM queries, ticket review).

6. **Roles & Responsibilities**
    - Slide: Who provides evidence, who responds to queries, who approves remediation timelines.
7. **Communication Plan**
    - Slide: Status update cadence (weekly), primary POC, escalation path, and how evidence will be transferred (secure file share/OneDrive).
8. **Deliverables**
    - Slide: Expected outputs (draft report, CAP, final report, appendices).
9. **PBC (Provided-By-Client) List & Logistics**
    - Slide: List of requested artifacts and target delivery dates (see PBC checklist below).
    - Slide: Evidence format and naming conventions.
10. **Questions, Exceptions & Next Steps**
    - Slide: Open issues, immediate actions, and agreed next meeting.

Example meeting commitments / minutes wording (copyable):

IT Manager commits to providing the following artifacts to the audit team within 3 business days: privileged group membership export (DomainAdmins.csv), last 90 days authentication logs (AuthLog_Export.csv), and provisioning ticket export (TicketExport_Provision.csv). The audit team will commence fieldwork on [start date], with a planned exit meeting on [date].

Example scope clarifications / exclusions to record

- Confirm whether test accounts and non-production systems are excluded or included.
- Note any ongoing remediation activities that will be excluded from scope if remediation completes prior to fieldwork.

PBC (Provided-By-Client) quick checklist

- Export on privileged group membership (CSV).
- Authentication log extracts (Event ID filters / SIEM query results).
- Ticketing system exports for provisioning requests (last 12 months).
- Conditional Access / MFA configuration screenshots or exports.

- AD change logs for group modifications.
- Access management and provisioning policies; previous recertification reports.

Follow-up actions from the kick-off meeting

- Distribute meeting minutes and confirmed PBC list within 24 hours.
- Auditee to confirm delivery dates for each PBC item.
- Audit team to finalize sampling plan and confirm fieldwork schedule.
- Agree remediation reporting cadence and format for CAP progress updates.

3.3 Field Work

Purpose:
Fieldwork is the phase in which the audit plan is executed through evidence-based testing of selected controls. The objective is to confirm whether controls are both properly designed and operating effectively, and to make exceptions for reporting and remediation.

Key activities

- **Walkthroughs:** Perform walkthroughs of key controls and related processes to confirm the control design, the sequence of activities and the roles responsible. Document the process flows and references the evidence used to validate each step.
- **Evidence collection:** Obtain and preserve relevant evidence in a controlled manner. Typical evidence includes system logs, configuration exports, screenshots, policy documents, procedure manuals, system reports, ticketing records, and audit logs. Maintain an evidence index stating filename, source, date/time and collector.
- **Test of Design (TOD):** Assess whether the control is appropriately designed to achieve the control objective. Example: confirm the existence of a documented password policy, its approval date, and applicability to the target system. TOD is performed by inspecting policies, configuration baselines and process documentation.
- **Test of Operating Effectiveness (TOE):** Verify that the control operates as designed in the live environment. Example: review authentication logs to confirm that the password policy is enforced by the system (e.g., password complexity enforced, password age settings applied). TOE is performed using sample-based testing of transactions, log entries, and change events.
- **Sampling and selection:** Apply a risk-based sampling approach to select representative samples for testing (for example, 10–20 privileged accounts or the universe of privilege elevation events in the period under review). Document the sampling rationale and sample size.

- **Exception identification and documentation:** Record any deviations from expected control behavior as findings. For each exception capture the condition, the evidence, the likely cause, and the potential impact. Classify and priorities findings according to the agreed risk matrix.

- **Chain of custody and evidence handling:** Preserve integrity of collected evidence by recording who collected each item, when it was collected, and where it is stored. Use secure transfer mechanisms (encrypted file share) and mask sensitive data when necessary.

- **Stakeholder engagement during fieldwork:** Maintain regular communication with the control owner and system administrators to clarify evidence, validate interpretations, and obtain supplementary information where necessary. Escalate issues promptly if high-risk exceptions are found.

Example test (termination deprovisioning):

- **Control objective:** Terminated users are deactivated in Active Directory within 24 hours of termination.

- **TOD:** Inspect the termination and deprovisioning policy to confirm it requires deactivation within 24 hours.

- **TOE:** Select a sample of terminated employee records from HR (e.g., 10 cases from the review period). For each sampled case, compare the HR termination timestamp with the AD deactivation timestamp. Record the time difference and note any cases exceeding 24 hours. Capture HR record ID, AD account name, timestamps, and supporting evidence (screenshots or exported CSVs). If exceptions are found, document the cause (e.g., manual process delay) and assess the severity using the risk matrix.

Documentation deliverables from fieldwork

- Evidence index (file list with descriptions).

- Test workpapers for each TOD and TOE performed (showing test steps, evidence, actual results and conclusions).

- Exception log summarizing findings with preliminary risk ratings.

- Fieldwork status updates to the auditee and audit lead.

Stakeholders involved during fieldwork

- IT personnel (System Administrators, Database Administrators, DevOps).

- HR and Finance representatives (for user provisioning, terminations and payroll controls).

- Control owners and process managers.
- Audit team members (lead auditor, senior/junior auditors, technical analysts).

3.4 Reporting

Reporting summarizes findings, risk assessments and CAP items for management. For internal audits, findings are reported to management with remediation timelines; for external audits, follow-up testing is scheduled prior to final sign-off.

3.5 Exit Meeting

An exit meeting was conducted to review draft findings and agree on remediation of owners and target dates. Critical findings require a shorter remediation window and follow-up verification.

Controls Tested – Microsoft Active Directory Audit

Generated on: 2025-10-09 19:55 UTC

Overview of Tested Controls

Control ID	Control Name	Control Objective
Control A	MFA Enforcement for Privileged/Admin Logons	Ensure MFA is enforced for all privileged account logins to reduce risk.
Control B	Privileged Account Provisioning & Review	Ensure privileged access is approved, time-bound, and periodically reviewed.

Control A — MFA Enforcement for Privileged/Admin Logons

Control Objective: Ensure that all privileged accounts (Domain Admins, Enterprise Admins) require multi-factor authentication (MFA) for all interactive and remote logons, mitigating the risk of credential-based compromise.

Control Owner: IT Security Manager / Active Directory Team Lead

Test Type: Design Review & Operating Effectiveness (Log Review)

Sampling: Risk-based sample of up to 10 privileged accounts (or entire population if <10).

Test Steps

1. 1. Export privileged groups and members from AD (CSV).
2. 2. Review Conditional Access / MFA configuration for enforcement on privileged groups.

3. 3. Extract authentication logs (90 days) from SIEM or event logs with required fields (timestamp, account name, logon type, MFA event).
4. 4. Verify MFA challenge/success for each login event.
5. 5. Identify successful privileged logons without MFA and capture context (IP, logon type, timestamp).
6. 6. Review exception/break-glass procedures and ensure justification and approval.

Expected Results

Expected Results: MFA policy includes privileged groups with no exclusions. 100% of sampled privileged logons have MFA or approved exceptions with compensating controls.

Evidence to Collect

Evidence to Collect: AD privileged group export (CSV); MFA/Conditional Access configuration (screenshots/export); Authentication logs from SIEM or AD; Exception/break-glass approval records

Pass / Fail Criteria

- **Pass:** No privileged logon without MFA, or valid approved exception.
- **Fail:** Any privileged logon without MFA and no approved exception.

Control B — Privileged Account Provisioning & Review

Control Objective: Ensure privileged accounts are only provisioned after documented approval, temporary access is time-bound, and periodic recertification is performed.

Control Owner: IT Operations Manager / Active Directory Team Lead

Test Type: Design Review & Operating Effectiveness (Ticket & Change Log Review)

Sampling: Risk-based sample of 10 provisioning/privilege change events over the last 12 months (entire population if limited).

Test Steps

7. 1. Obtain provisioning policy and ticket export. Confirm approval & justification requirements.
8. 2. Review sampled tickets for approver, justification, expiry, timestamp.
9. 3. Cross-reference AD change logs to confirm provisioning matches tickets and temporary access removal.

10. 4. Review periodic recertification records (last 12 months).
11. 5. Document missing approvals, unremoved privileges, or lack of review evidence.

Expected Results

Expected Results: All provisioning events have approvals, justification & expiry. Temporary privileges removed on time. Recertification completed as per policy.

Evidence to Collect

Evidence to Collect: Ticket exports (ID, requester, approver, dates); AD group membership change logs; Recertification reports/logs; Policy & procedure documents

Pass / Fail Criteria

- **Pass:** All provisioning events include approvals & expiry; privileges removed on time; recertification evidence exists.
- **Fail:** Missing approvals/expiry, privileges retained post-expiry, or no recertification evidence.

Sampling Rationale & Documentation Requirements

Requirement	Description
Sampling Basis	Risk-based; focused on privileged accounts & recent access changes.
Documentation	Maintain sampling rationale and sample selection records.
Workpaper Content	For each test step: Test step performed; Sample identifier; Evidence reference; Expected vs Actual result; Conclusion (Pass/Fail).
Evidence Index	All supporting evidence stored using standard Evidence Index template.

Workpapers: For every test step, prepare a workpaper recording test step, sample identifier, evidence reference(s), expected vs actual result, and conclusion (pass/fail). Store evidence using the Evidence Index template.

5x5 Risk Matrix and Legend

The risk matrix is included to provide a structured and standardized way of assessing and prioritizing the significance of control weaknesses identified during testing. Although the primary objective of this project is to test selected IT controls, any gaps observed must be evaluated in terms of their potential impact and likelihood of occurrence. Using a 5×5 risk matrix allows the auditor to assign a qualitative risk rating (Low, Medium, High, or Critical) to each finding. This helps management understand the relative severity of issues and allocate remediation efforts effectively.

The matrix aligns with industry frameworks such as NIST SP 800-30 and NIST SP 800-53, which recommend assessing both the likelihood and impact of risks associated with control failures. By integrating the risk matrix into the audit report, the findings are not only documented but also prioritized for action, supporting more informed decision-making and risk management.

Impact \ Likelihood	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Significant	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Negligible	1	2	3	4	5

Legend: 1–5 = Low (Green); 6–10 = Medium (Amber); 11–15 = High (Orange); 16–25 = Critical (Red)

4. Corrective Action Plan (CAP)

Finding ID	Finding Summary	Root Cause	Risk Impact	Recommendation	Priority	Owner	Target Date	Status	Evidence
F-01	Emergency/break-glass accounts lacked documented MFA enforcement	Conditional Access policy not applied to break-glass group	High	Apply Conditional Access to include break-glass; enforce MFA; log all uses	High	IT Security Manager	2025-10-05	Open	ConfigExport_CondAccess_2025-09-20.png
F-02	7 of 10 provisioning tickets lacked expiry documentation for	Inconsistent enforcement of provisioning policy	Medium	Enforce ticket template with expiry; automate removal	Medium	IT Ops Manager	2025-11-01	Open	TicketExport_Provision_2025.csv

	temporary privileges			with workflow					
F-03	No recent recertification evidence for privileged accounts (last recert 18 months ago)	Recertification process not enforced	High	Schedule and perform recertification; implement quarterly reviews	High	IAM Lead	2025-10-20	Open	RecertReport_2024_Q4.pdf

5. Audit Report — Testing of Controls

Project: PROJECT 4 (INDIVIDUAL) Testing of Controls

Company: Philocybers Consulting Firm (YESYOUCAN CYBERSECURE, LLC)

System: Microsoft Active Directory (CORP.LOCAL)

Prepared by: Oswald Eyram Toku

Date: September 2025

Distribution: Senior Management, IT Security, IT Operations

1. Executive Summary

This report presents the results of control testing performed on the Microsoft Active Directory environment (CORP.LOCAL). The audit evaluated two access controls: (1) enforcement of Multi-Factor Authentication (MFA) for privileged interactive logons and (2) privileged account provisioning and periodic recertification. Testing combined control design review and non-intrusive operating effectiveness procedures (log review, configuration inspection, and ticketing evidence review). Three findings were identified; two are assessed as Critical and require remediation within 30–45 days. A Corrective Action Plan (CAP) is provided specifying remediation tasks, owners, priorities and target dates.

2. Audit Objective, Scope and Methodology

2.1 Objective

The objective of the engagement was to obtain reasonable assurance that selected access controls for privileged accounts are properly designed and operating effectively to mitigate the risk of unauthorized privileged access.

2.2 Scope

The scope covered the on-premises Active Directory domain CORP.LOCAL, including Domain Admin and Enterprise Admin groups, relevant authentication infrastructure (Conditional Access / MFA configurations), authentication logs for the prior 90 days, and provisioning tickets for the prior 12 months.

2.3 Methodology

The audit was conducted in accordance with standard IT audit practices and aligned with NIST SP 800-53, NIST SP 800-30, COBIT and COSO principles. Procedures included: planning and authorization; a kickoff with system owners; design reviews of policies and configurations; sampling of privileged accounts and provisioning events; non-intrusive operating effectiveness testing (log and ticket review); evidence collection and analysis; risk evaluation using a 5×5 risk matrix; and reporting of findings and recommendations. All testing was performed using non-intrusive techniques and with documented authorization.

3. Summary of Findings

Finding ID	Title	Summary	Risk Rating (L×I)	Level
F-01	MFA exceptions for emergency accounts	Break-glass / emergency accounts were not included in Conditional Access policies; authentication logs indicate privileged logons without MFA events.	16	Critical
F-02	Missing expiry on temporary privilege grants	7 of 10 sampled provisioning tickets did not document an expiry date for temporary privileges.	12	High
F-03	Absence of recent privileged account recertification	No evidence of recertification within the organisation’s policy window; last documented recertification >18 months ago.	16	Critical

4. Detailed Findings and Implications

Finding F-01 — Emergency accounts not enforced for MFA (Critical)

Condition: Review of Conditional Access configurations and exported authentication logs identified that the designated break-glass/emergency accounts were exempt from MFA enforcement. Authentication log extracts include successful privileged interactive logons where no MFA event was recorded.

Cause: Conditional Access policies do not explicitly include break-glass/exception groups; exceptions were implemented without compensating controls or documented approval.

Impact: Elevated risk of privileged account compromise and full domain takeover if credentials are compromised; potential for data breach and operational disruption.

Recommended Immediate Action: Apply Conditional Access policies to include break-glass accounts, or implement compensating controls (e.g., vaulting with just-in-time access) and ensure all uses are logged and reviewed. See CAP entry F-01.

Finding F-02 — Temporary privilege grants lack expiry documentation (High)

Condition: In 7 of 10 sampled provisioning tickets there was no recorded expiry or automatic removal workflow for temporary elevated privileges. AD change logs confirm delayed or absent removal in several instances.

Cause: Incomplete ticket templates and manual deprovisioning process.

Impact: Prolonged excessive privileges increase the attack surface and the risk of misuse (malicious or accidental).

Recommended Action: Enforce a ticket template requiring expiry, and implement workflow automation to remove temporary privileges at expiry. See CAP entry F-02.

Finding F-03 — No recent privileged account recertification (Critical)

Condition: The organisation could not provide recertification artifacts within the past 12 months; the most recent report was dated over 18 months prior.

Cause: Recertification process exists in policy but has not been executed on schedule.

Impact: Undetected accumulation of excessive privileges, non-compliance with policies, and increased risk of insider misuse or credential compromise.

Recommended Action: Initiate immediate full recertification of all privileged accounts and schedule quarterly recertification cycles. See CAP entry F-03.

5. Corrective Action Plan — Executive Summary

A detailed Corrective Action Plan is provided in the Appendices. The CAP below summarises the priority actions for management:

- F-01 (Critical): Apply Conditional Access and enforce MFA for all privileged accounts and break-glass procedures within 30 days. Owner: IT Security Manager.

- F-03 (Critical): Execute privileged account recertification and implement quarterly recertification cadence within 45 days. Owner: IAM Lead.

- F-02 (High): Update provisioning processes to require expiry metadata and automate removal workflows within 60 days. Owner: IT Operations Manager.

6. Recommendations (Prioritised)

- Enforce MFA for all privileged access — Extend Conditional Access or PAM integration to ensure MFA is non-bypassable for privileged accounts. Implement SIEM alerts for any privileged login without MFA.

- Immediate privileged account recertification — Conduct an urgent recertification campaign covering all Domain/Enterprise Admins and privileged groups; remediate improperly assigned privileges.

- Automate temporary privilege lifecycle — Enhance the provisioning process with mandatory expiry fields and automation to remove privileges at expiry.

- Harden emergency access procedures — Move break-glass credentials into a vault with just-in-time access and comprehensive logging/audit trail.

- Strengthen oversight and monitoring — Implement alerting for anomalous privileged behavior and periodic reporting to management.

- Update policy and training — Refresh access management policies and provide role-based training to administrators and helpdesk staff.

7. Conclusion

The control design for privileged access demonstrates alignment with accepted standards; however, the operating effectiveness of several key processes is deficient. In particular, lack of MFA enforcement for emergency accounts and the absence of timely privileged account recertification represent immediate and material risks to the organisation. Management should prioritise remediation of Critical findings and schedule re-testing upon completion.

8. Management Response and Acknowledgement

Management acknowledges receipt of this report. Planned actions, owners and target dates are recorded in the CAP and will be reported to the audit committee on completion.

9. Signatures

Prepared by:
Oswald Eyram Toku
Senior Auditor — Philocybers Consulting Firm

Signature: ___________________ Date: ___________________

Reviewed by:
[IT Security Manager Name]

Signature: ___________________ Date: ___________________

Approved by:
[Chief Information Officer / Risk Owner]

Signature: ___________________ Date: ___________________

10. Appendices

Appendix A — Corrective Action Plan (full table with owners, evidence and status)

Appendix B — Detailed test scripts and SIEM/log queries (PowerShell commands, event IDs)

Appendix C — Evidence index (file names and descriptions)

Appendix D — 5×5 Risk Matrix and Legend (numeric table and colour key)

Appendix E — References (NIST SP 800-53, NIST SP 800-30, COBIT, COSO)

6 Conclusion

Overall, the design of the tested controls is generally adequate, but operating effectiveness has gaps that require remediation. Priority is to enforce MFA for all privileged access and to strengthen provisioning and recertification processes. After remediation, re-testing should be scheduled within 45 days for critical items.

7. Appendices

Appendix A - Test Scripts and Queries

PowerShell commands and queries used (examples):

Get AD Group Members (example):

```
Get-ADGroupMember -Identity "Domain Admins" -Recursive | Select Name, SamAccountName | Export-Csv C:\Temp\DomainAdmins.csv -NoTypeInformation
```

Export Authentication Events (example):

Use SIEM or Event Log export: filter Windows Security Event ID 4624 (Logon). Include fields: TimeCreated, AccountName, LogonType, IpAddress, AuthenticationPackage.

Group membership change events: Event IDs 4728/4729 for security group changes.

Appendix B - Evidence Checklist

- Privileged group membership export (DomainAdmins.csv)

- Conditional Access policy export (ConfigExport_CondAccess_2025-09-20.png)

- Authentication log extract showing MFA events (AuthLog_2025-08-15.csv)

- Provisioning tickets export (TicketExport_Provision_2025.csv)

- AD change log export for group modifications (GroupChanges_2025.csv)

- Recertification report (RecertReport_2024_Q4.pdf)

Appendix C - Non-intrusive Testing Checklist

- Obtain signed authorization before testing.

- Prefer log and config review overactive authentication attempts.

- Use test accounts and a lab environment for any active tests.

- Mask sensitive data in evidence shared externally.