SECURITY AUDIT REPORT

Prepared for PDF Test Org

25%

COMPLIANCE SCORE

Audit ID: ebbca34d-74ff-4e56-879b-240292f02537
Generated: 2026-01-26 11:13

Executive Summary

This report provides a detailed analysis of the security posture of **{{ audit.organization.name }}** based on the audit performed on January 26, 2026.

Metric	Count	Status
Total Checks	4	-
Passed Checks	1	OK
Failed Checks	3	ATTENTION

Detailed Findings

The following section details the compliance checks performed. Prioritize addressing **CRITICAL** and **HIGH** severity issues.

cis_1_1: MFA Enforced   FAIL   {{ CHECK.SEVERITY }}

MFA must be enabled.

Affected Resources:

Resource	Issue / Remediation
N/A	User alice and bob do not have MFA.

Technical Evidence:

System Log / JSON:

```
{
  "org": "my-org",
  "mfa_enabled": false,
  "admins_without_mfa": [
    "alice",
    "bob"
  ]
}
```

cis_4_1: Branch Protection

FAIL   {{ CHECK.SEVERITY }}

Automated check for Branch Protection

Affected Resources:

Resource	Issue / Remediation
repo-A	Repo A is unprotected.

> **Technical Evidence:**
>
> **System Log / JSON:**

```json
{
  "repo_name": "repo-A",
  "protection": false
}
```

repo-B	Repo B is unprotected.

> **Technical Evidence:**
>
> **System Log / JSON:**

```json
{
  "repo_name": "repo-B",
  "protection": false
}
```

cis_5_1: CODEOWNERS File

PASS   {{ CHECK.SEVERITY }}

Automated check for CODEOWNERS File

✓ Compliance met across 1 resource(s).