Audit Report - Access Control Policy

ISO 27001:2022 Internal Audit

Audit ID: 124

Framework: ISO 27001:2022

Policy: Access Control Policy

Auditor: Radha Sharma

Reviewer: admin.grc

Due Date: 27/09/2025

Progress: 40% (Completed)

Audit Type: Internal

Status: Completed

Executive Summary

This internal audit assessed the organization's Access Control Policy implementation and compliance with ISO 27001:2022 requirements. The evaluation covered user access management, privileged access controls, network security, and application access controls across all systems and platforms.

Overall Assessment: **Good** with some areas requiring attention

Compliance Score: 82%

Audit Period: August 10-25, 2025

Report Date: August 24, 2025

Audit Scope and Objectives

Scope

- User access provisioning (A.9.1)
- User access reviews (A.9.2)
- Privileged access rights (A.9.3)
- Secret authentication information (A.9.4)
- Network access control (A.13.1)
- Operating system access control (A.13.2)
- Application and information access (A.14.1)

Objectives

- Evaluate access provisioning and deprovisioning processes
- Assess privileged access management effectiveness
- Review password and authentication policies
- Validate network and system access controls

Key Findings Summary

Finding Level	Count	Percentage
Critical	0	0%
Major	3	25%
Minor	7	58%
Observations	2	17%

Detailed Findings

Major Findings

M-001: Privileged Access Reviews Overdue

Control: A.9.2 - User access reviews

Finding: Privileged access reviews are 6 months overdue for 34 accounts across critical systems. Last comprehensive review was February 2025.

Risk: Excessive privileges may remain active, increasing insider threat risk and compliance violations.

Recommendation: Implement quarterly privileged access reviews with automated workflow and escalation procedures.

Management Response: *Immediate privileged access review initiated. Quarterly schedule established.*

Target Date: September 30, 2025

M-002: Password Policy Non-Compliance

Control: A.9.4 - Secret authentication information

Finding: 156 user accounts (12% of total) do not meet current password complexity requirements. Legacy systems lack multi-factor authentication integration.

Risk: Weak passwords increase account compromise risk and unauthorized access.

Recommendation: Enforce password policy compliance and implement MFA for all systems.

Management Response: *Password policy enforcement project approved. MFA rollout in progress.*

Target Date: October 31, 2025

M-003: Network Segmentation Gaps

Control: A.13.1 - Network access control

Finding: Critical systems network segment allows unnecessary lateral movement. 23 systems have broader network access than required.

Risk: Network compromise could spread to critical systems and sensitive data.

Recommendation: Implement micro-segmentation and zero trust network architecture.

Management Response: *Network segmentation project planned for Q4 2025.*

Target Date: December 31, 2025

Minor Findings

Minor-001: Access Request Documentation

Control: A.9.1 - User access provisioning

Finding: 15% of access requests lack proper business justification documentation.

Recommendation: Enhance access request workflow with mandatory justification fields.

Minor-002: Terminated Employee Access

Control: A.9.1 - User access provisioning

Finding: 3 terminated employees still have active directory accounts after 30+ days post-termination.

Recommendation: Implement automated account disabling upon HR notification.

Minor-003: Service Account Management

Control: A.9.3 - Privileged access rights

Finding: 12 service accounts lack documented ownership and regular review.

Recommendation: Establish service account governance process.

Minor-004: Application Access Controls

Control: A.14.1 - Application and information access

Finding: 2 legacy applications lack role-based access controls.

Recommendation: Implement RBAC or plan application retirement.

Minor-005: Guest Account Management

Control: A.9.1 - User access provisioning

Finding: Guest accounts for contractors lack automatic expiration dates.

Recommendation: Implement time-limited guest access with automatic expiration.

Access Control Analysis

User Account Statistics

- **Total User Accounts**: 1,298
- **Active Accounts**: 1,156 (89%)
- **Inactive Accounts**: 87 (7%)
- **Disabled Accounts**: 55 (4%)
- **Privileged Accounts**: 89 (7%)

Access Control Metrics

Metric	Current Status	Target	Compliance
MFA Coverage	847 accounts (73%)	95%	Needs Improvement
Password Compliance	1,142 accounts (88%)	98%	Good
Access Reviews	6 months overdue	Quarterly	Non-Compliant
Provisioning Time	2.3 days average	<1 day	Good
Deprovisioning Time	4.7 days average	Same day	Needs Improvement

System Access Analysis

System Category	Total Systems	Access Controlled	RBAC Implemented	MFA Required
Critical Business	23	23 (100%)	21 (91%)	18 (78%)
Financial Systems	12	12 (100%)	12 (100%)	12 (100%)
HR Systems	8	8 (100%)	8 (100%)	6 (75%)
Development	15	13 (87%)	10 (67%)	8 (53%)

Legacy Applications	7	5 (71%)	2 (29%)	1 (14%)

Risk Assessment

High Priority Risks

1. **Privileged Access**: Overdue reviews create insider threat exposure
2. **Password Weakness**: Non-compliant passwords increase breach risk
3. **Network Segmentation**: Lateral movement potential in network architecture

Medium Priority Risks

1. **Legacy Systems**: Older applications lack modern access controls
2. **Service Accounts**: Unmanaged service accounts pose security risks
3. **Guest Access**: Uncontrolled contractor access duration

Low Priority Risks

1. **Documentation**: Incomplete access request justifications
2. **Process Delays**: Slow deprovisioning increases exposure window

Compliance Assessment

ISO 27001:2022 Control Assessment

Control	Requirement	Implementation	Compliance	Comments
A.9.1	User access provisioning	Implemented	85%	Good process, minor documentation gaps
A.9.2	User access reviews	Partial	60%	Privileged access reviews overdue
A.9.3	Privileged access rights	Implemented	75%	Service account governance needed
A.9.4	Secret authentication	Implemented	80%	Password compliance improvements needed

A.13.1	Network access control	Implemented	78%	Segmentation enhancements required
A.13.2	Operating system access	Implemented	90%	Strong OS-level controls
A.14.1	Application access	Implemented	82%	Legacy app controls need updating

Recommendations

Immediate Actions (0-30 days)

1. **Privileged Access Review**: Complete overdue privileged access reviews
2. **Account Cleanup**: Disable accounts for terminated employees
3. **Emergency Access**: Review and validate all emergency access accounts
4. **Service Account Audit**: Document ownership for all service accounts

Short-term Actions (30-90 days)

1. **MFA Deployment**: Complete MFA rollout for all critical systems
2. **Password Enforcement**: Deploy automated password compliance tools
3. **Access Workflow**: Enhance access request documentation requirements
4. **Guest Account Controls**: Implement time-limited guest access

Long-term Actions (90+ days)

1. **Network Segmentation**: Implement micro-segmentation strategy
2. **Zero Trust**: Deploy zero trust architecture components
3. **Legacy Modernization**: Upgrade or retire legacy applications
4. **Access Analytics**: Implement user behavior analytics

Management Action Plan

Action Item	Owner	Target Date	Priority	Status
Privileged access review	Security Team	Sep 30, 2025	High	Initiated
MFA implementation	IT Security	Oct 31, 2025	High	In Progress

Network segmentation	Network Team	Dec 31, 2025	Medium	Planned
Password enforcement	IT Operations	Oct 31, 2025	High	Planned
Service account governance	Security Team	Nov 15, 2025	Medium	Planned

Positive Observations

1. **Strong Financial System Controls**: Excellent access controls for financial applications
2. **Effective OS Security**: Well-implemented operating system access controls
3. **Good Provisioning Process**: Efficient user account provisioning workflow

Technology Recommendations

Access Management Tools

- **Privileged Access Management (PAM)**: Deploy enterprise PAM solution
- **Identity Governance**: Implement identity governance and administration platform
- **Network Security**: Deploy zero trust network access solutions
- **Analytics**: Implement user and entity behavior analytics (UEBA)

Follow-up Schedule

1. **30-day Review**: Progress on privileged access reviews and account cleanup
2. **60-day Assessment**: MFA deployment progress and password compliance
3. **Quarterly Review**: Overall access control posture and metrics
4. **Annual Audit**: Comprehensive access control program assessment

Conclusion

The Access Control Policy audit demonstrates a generally well-implemented access control framework with strong foundational controls. The organization has effective provisioning processes, good operating system controls, and strong financial system security.

The identified major findings, while requiring attention, are manageable and primarily relate to maintenance and enhancement activities rather than fundamental control failures. Implementation of the recommended improvements, particularly around privileged access management and network segmentation, will significantly strengthen the overall security posture.

The organization's commitment to MFA deployment and password policy enforcement demonstrates good security awareness and investment in access control improvements.

Auditor: Radha Sharma, Senior Internal Auditor

Review: admin.grc, Audit Manager

Distribution: IT Security, Executive Team, Department Managers

Next Audit: January 2026