# Security risk assessment report

## Part 1: Three hardening tools and methods to implement

| Hardening tool / method | Primary purpose | Key NIST SP 800-53 Rev 5 controls |
|---|---|---|
| **Centralized Identity & Access-Management (IAM) platform that enforces unique accounts, password-manager integration, and automated credential rotation** | • Eliminates shared passwords<br>• Removes default / unchanged credentials<br>• Gives auditable lifecycle for every account | AC-2 (Account Management), AC-2 (7) Privileged User Accounts, AC-2 (9) Restrict Shared Accounts, AC-2, (10) Shared-Credential Change, AC-6 (Least Privilege), IA-5 (1) Password-based Auth. |
| **Enterprise Multi-Factor Authentication (MFA) for all users—SMS / authenticator app for standard users, hardware tokens for admins** | • Stops credential-stuffing & password-reuse attacks<br>• Raises bar for lateral movement after a breach | IA-2 (1)(2) MFA to privileged & non-privileged accounts, AC-7 (4) Alternate factor, AC-17 (10) Authenticate remote commands |
| **Next-Generation Firewall (NGFW) with "deny-all/ allow-by-exception" rules plus automated configuration validation** | • Filters inbound & outbound traffic<br>• Blocks command-and-control and data-exfiltration paths | SC-7 (5) Deny by Default, SC-7 (11) Restrict Incoming Traffic, AC-4 Information-Flow Enforcement, AU-2 Event Logging (firewall logs) |

# Part 2: Recommendations Explained

| Observed vulnerability | How the selected hardening measure resolves it | Why the mapped NIST control is a good fit |
|---|---|---|
| *Employees share passwords* | The IAM platform forces unique identifiers for each user (AC-2) and technically blocks shared accounts; the built-in password manager delivers unique, strong credentials. | AC-2(9) prohibits shared accounts and AC-2(10) forces regular credential changes, satisfying policy and providing auditability. |
| *Database admin password still at default* | Credential-rotation automation built into the IAM tool immediately changes any default or stale password and can schedule periodic rotations. | IA-5(1) mandates strong, unique passwords and AC-2(7) covers privileged-account management. |
| *Firewalls lack rule sets for egress/ ingress* | The NGFW introduces a deny-all / permit-by-exceptionbaseline, then adds least-privilege service allowances; configuration-drift tools keep rules consistent across devices. | SC-7(5) & SC-7(11) require boundary devices to block all traffic that has not been explicitly approved, effectively hardening the perimeter. |
| *No multi-factor authentication* | Deploying MFA ensures stolen or guessed passwords alone are useless; privileged roles can be bound to stricter hardware-token factors. | IA-2(1)(2) demand MFA for privileged and non-privileged accounts; AC-6 complements by limiting privilege elevation without the extra factor. |

# Apendix A: Implementation Plan Aligned with NIST CSF

## Phase 1: Identity & Access Management (IAM) Deployment

**Actions:**

- Import all users into a centralized IAM system.
- Disable shared/group credentials.
- Enforce strong, unique credentials and rotate all default/admin passwords.
- Assign roles based on least privilege and apply just-in-time (JIT) access for sensitive operations.

**Mapped NIST CSF Categories:**

- **PR.AA** — *Identity Management, Authentication, and Access Control*: Centralized control ensures unique identities and principle of least privilege.
- **GV.RR** — *Roles, Responsibilities, and Authorities*: Enforces who can approve, manage, or assign user privileges.
- **GV.PO** — *Policy*: Implements and enforces access-control and password policies.
- **ID.AM** — *Asset Management*: Tracks identity assets such as accounts and credentials.
- **GV.OV** — *Oversight*: Periodic review of account and privilege status.

# Phase 2: Multifactor Authentication (MFA) Rollout

**Actions:**

- Implement MFA for all users, starting with administrators and critical systems.
- Use app-based or hardware-token MFA.
- Configure policies for remote access, privilege escalation, and sensitive data access to require MFA.

**Mapped NIST CSF Categories:**

- **PR.AA** — *Identity Management, Authentication, and Access Control*: MFA strengthens credential-based authentication.
- **PR.AT** — *Awareness and Training*: Users are trained to use MFA methods securely.
- **GV.OC** — *Organizational Context*: Contextualizes access requirements based on sensitivity and user roles.
- **GV.RM** — *Risk Management Strategy*: MFA directly mitigates risks from credential-based attacks.
- **PR.DS** — *Data Security*: Enhances access security for data-handling systems.

# Phase 3: Network Firewall Rules and Monitoring

**Actions:**

- Implement Next-Generation Firewalls (NGFWs) at all ingress and egress points.
- Apply “deny by default, allow by exception” traffic rules.
- Log all network traffic and integrate with SIEM for continuous monitoring.
- Continuously assess traffic anomalies and configuration drift.

**Mapped NIST CSF Categories:**

- **PR.PS** — *Platform Security*: Firewall policies enforce secure communication boundaries.
- **PR.IR** — *Technology Infrastructure Resilience*: NGFWs ensure resilience against unauthorized or malformed traffic.
- **DE.CM** — *Continuous Monitoring*: NGFW and SIEM provide real-time traffic analysis and alerting.
- **DE.AE** — *Adverse Event Analysis*: Detects anomalies in traffic to trigger incident response.
- **GV.SC** — *Cybersecurity Supply Chain Risk Management*: Secures system boundaries where third-party interactions occur.
- **RS.MA** — *Incident Management*: Prepares the team to respond to traffic anomalies or policy violations.
- **ID.RA** — *Risk Assessment*: Evaluates firewall policies and network exposure during assessment cycles.

# Sustainment and Optimization

**Actions:**

- Regular reviews and audits of identity, authentication, firewall, and logging systems.
- Train personnel on security hygiene and phishing defense.
- Continuously improve policies based on lessons learned from events or changes in threat landscape.

**Mapped NIST CSF Categories:**

- **ID.IM** — *Improvement*: Incorporates feedback loops from events and audits.
- **RS.AN** — *Incident Analysis*: Post-incident evaluation feeds policy improvement.
- **RC.RP** — *Recovery Plan Execution*: Aligns with readiness for breach recovery.
- **RC.CO** — *Incident Recovery Communication*: Ensures stakeholders are informed during/after a breach.
- **GV.OV** — *Oversight*: Confirms compliance with organizational and regulatory standards.