Barbican Security Library — Compliance Summary

What is Barbican?

Barbican is a **security compliance library** implementing **56+ NIST SP 800-53 Rev 5 controls** for web applications. It provides pre-built, auditable security implementations at two layers:

Layer	What It Provides
Application (Rust)	Authentication, session management, password policies, input validation, encryption, audit logging
Infrastructure (NixOS)	Firewall, kernel hardening, database security, intrusion detection, encrypted backups, PKI

NIST 800-53 Control Coverage

Family	Key Controls	Implementation
Access Control (AC)	AC-7, AC-11, AC-12	Account lockout, session timeouts
Audit (AU)	AU-2, AU-3, AU-9, AU-12	Tamper-evident logging with HMAC chains
Identification (IA)	IA-2, IA-5, IA-5(1)	MFA, NIST 800-63B password policy
System Protection (SC)	SC-7, SC-8, SC-12, SC-13, SC-28	Firewall, TLS, key management, encryption at rest
System Integrity (SI)	SI-4, SI-7, SI-10, SI-11	AIDE/auditd, input validation, secure errors
Contingency (CP)	CP-9	Automated encrypted backups
Supply Chain (SR)	SR-3, SR-4	Vulnerability scanning, SBOM generation

---

FedRAMP Profile Defaults

Control	Low	Moderate	High
Session timeout	30 min	15 min	10 min
Idle timeout	15 min	10 min	5 min
MFA required	Privileged	All users	All users
Password minimum	8 chars	12 chars	14 chars
Account lockout	5 tries/15 min	3 tries/30 min	3 tries/30 min
Encryption at rest	Optional	Required	Required
FIPS cryptography	Optional	Recommended	Required

Selecting a profile automatically configures all controls to that level.

Audit Support Features

Feature	Benefit
Single source of truth	All security config in one file (`barbican.toml`)
Control-to-code traceability	Every control maps to specific source files
Automated testing	`nix run .#audit` runs full compliance verification

Feature	Benefit
Compliance artifacts	JSON evidence files with HMAC integrity signatures
Reproducible infrastructure	NixOS ensures deployed state matches documented config

---

Key Audit Documents

- `barbican.toml` — Security configuration (single source of truth)
- `NIST_800_53_CONTROL_RESEARCH.md` — Control-to-implementation mapping
- `docs/AUDIT_GUIDE.md` — Step-by-step audit procedures with checklists
- **Compliance artifacts** — Generated evidence files for each control test

---

Coverage Estimate

Framework	Approximate Coverage
FedRAMP Moderate	~80% of applicable controls
SOC 2 Type II	~85% of applicable criteria
NIST 800-63B (Identity)	Full compliance

Barbican handles application and infrastructure controls. Organizational controls (HR, physical security) remain the responsibility of the deploying organization.

Repository: github.com/Sauce65/barbican | **Profile:** FedRAMP Low / Moderate / High