★ IAM Security Assessment

Executive Report - Qriar IAM Security Framework - Assessment 2026 v0.12 - 2026-02-26

Qriar IAM Security Framework

Gerado: 2026-02-26 20:13 | Idioma: EN | Tipo: Executive

DOCUMENTO CONFIDENCIAL

3.08	72.0%	13	$0
SCORE DE MATURIDADE	TAXA DE CONFORMIDADE	TOTAL DE RISCOS (9 CRÍTICOS)	PERDA ANUAL ESPERADA

1. Executive Summary

Assessment 2026 v0.12 of the Qriar IAM Security Framework (version 1.0) was completed on 2026-02-26. The organization’s Identity and Access Management (IAM) posture is assessed at an overall maturity of **3.08/5** with a framework-wide compliance rate of **72.0%** across **25/25** controls assessed. Performance is uneven across domains: Privileged Access Management (PAM) and Authentication show stronger capabilities, while Monitoring (MON) and Lifecycle (Joiner-Mover-Leaver — JML) present the most material deficiencies. Notably, **15** controls are below target (Level < 2 or not meeting the defined target level), and **10** are at or above advanced maturity (Level ≥ 4).

The risk landscape is concentrated and severe: **13** risks were identified, with **9** Critical, **3** High, and **1** Medium, and **12** remain open/active. The most consequential issues are concentrated around administrative credential compromise (RISK-001), lateral movement via local admin (RISK-004), monitoring blind spots (RISK-005), and multi-factor authentication (MFA) bypass via legacy protocols and uncovered flows (RISK-013, RISK-006). The Total

Annual Loss Expectancy (ALE) currently records as **$0.00**, which indicates a lack of quantified loss modeling rather than absence of exposure; given the identified Critical risks and regulatory mapping gaps, the potential financial impact spans operational disruption, data exfiltration, regulatory penalties, and reputational harm.

- Maturity: **3.08/5** overall; strongest in PAM (**3.67/5**), weakest in Monitoring (**2.33/5**).
- Compliance: average **72.0%** across mapped standards; ISO 27001:2022 at **70.5%**, NIST CSF 2.0 at **74.1%**, CIS Controls v8 at **67.9%**.
- Risk: **9** Critical, **3** High; systemic gaps in monitoring and lifecycle controls drive residual Critical exposure.
- Controls below target: **15**; quick-win remediations exist in MON-001/002/003/005, JML-004, AUTH-005.

Board-level priorities over the next 90 days: (1) eradicate legacy/MFA-bypass paths (AUTH-002, AUTH-005; RISK-013, RISK-006), (2) close visibility and response gaps (MON-001/002/003/005/004), and (3) harden privileged tiers and emergency access (PAM-004/005). These actions materially reduce at least six Critical risks and lift compliance across ISO 27001:2022 A.5.16, A.8.2; NIST CSF PR.AA-02, DE.AE-02; CIS 4.7, 8.2; and ISF SGP TS.1.3/SM.1.1.

2. Scope and Methodology

This assessment was conducted against the Qriar IAM Security Framework version 1.0 for the client environment “Assessment 2026 v0.12” and completed on 2026-02-26. The scope included **25** IAM controls across four domains: Monitoring (MON), Lifecycle (Joiner-Mover-Leaver — JML), Authentication (AUTH), and Privileged Access Management (PAM). Each control was evaluated on a 0–5 maturity scale, where Level 1 indicates ad hoc/fragmented practice, Level 2 basic, Level 3 defined and consistently executed, Level 4 measured and automated, and Level 5 optimized with continuous improvement.

Evidence collection included stakeholder interviews, configuration and policy review, control design and operating effectiveness testing, and selective log and event sampling. Findings were mapped to leading standards for multi-framework alignment: ISO 27001:2022, NIST CSF 2.0, CIS Controls v8, LGPD/GDPR, IBGC 6ª Edição, PSI-CORP-001, and ISF SGP 2024. Risk analysis incorporated likelihood and impact scoring (L×I) to derive severity, with treatment

strategies recorded per risk. ALE currently records as **$0.00**, indicating a lack of quantitative loss data; a FAIR-aligned quantification sprint is recommended to establish statistically defensible loss ranges in the next cycle.

3. Maturity by Domain

IAM maturity is heterogeneous. PAM and Authentication exhibit defined and partially automated practices (notably in vaulting, session control, and strong authentication factors), while Monitoring and Lifecycle controls reveal critical execution gaps, particularly around centralized telemetry, risk-based response, guest account governance, and timely termination.

Cross-domain themes include: (a) control intent is defined but operationalized inconsistently in Monitoring and JML; (b) overreliance on manual processes (e.g., access reviews, token revocation, guest renewals) increases residual risk; and (c) legacy protocols and uncovered flows undermine MFA efficacy and accountability.

Domain	Average Score	Controls	Key Strengths (L4+)	Key Gaps (Below Target)
Monitoring (MON)	**2.33/5**	6	—	MON-001, MON-002, MON-003, MON-004, MON-005, MON-006
Lifecycle (JML)	**2.83/5**	6	JML-002 (L4), JML-005 (L4)	JML-001, JML-003, JML-004, JML-006 (L1 Critical)
Authentication (AUTH)	**3.43/5**	7	AUTH-001 (L4), AUTH-006 (L4), AUTH-007 (L4)	AUTH-002, AUTH-004, AUTH-005
Privileged Access Management (PAM)	**3.67/5**	6	PAM-001 (L4), PAM-002 (L4), PAM-003 (L4)	PAM-004, PAM-005

Monitoring (MON)

Monitoring maturity at **2.33/5** indicates foundational capabilities without consistent centralization or automated response. Key control gaps include: central SIEM onboarding and retention (MON-001), automated risk-based blocking (MON-002), OAuth application consent monitoring (MON-003), Tier 0 group change alerting with out-of-band notification (MON-004), service principal anomaly detection (MON-005), and immediate SOC incident creation from negative MFA signals (MON-006).

These deficiencies directly sustain Critical risks including accountability failure (RISK-009) and loss of visibility into suspicious activity (RISK-005), and they depress compliance against

ISO 27001:2022 A.5.16, NIST CSF DE.AE-02/06, CIS 8.2, LGPD Art. 37/46, and ISF SGP SM.1.1/SM.2.2.

Lifecycle (Joiner-Mover-Leaver — JML)

Lifecycle maturity is **2.83/5** with strengths in selected areas (JML-002, JML-005 at L4), but critical shortcomings persist: JML-006 (guest/B2B TTL) is at Level 1, and JML-004 (access certification) remains at Level 2. Automation of birthright provisioning (JML-001) and near-real-time exit “kill switch” (JML-003) are not yet fully realized.

These issues sustain Critical risks of data exfiltration by former employees (RISK-003) and privilege accumulation (RISK-002) and erode compliance with ISO 27001:2022 A.5.18/A.5.19/A.5.21, NIST CSF PR.AA-01/ID.RA-03, CIS 6.7/6.8, LGPD Art. 5/39, and IBGC Cap. 5.5.

Authentication (AUTH)

Authentication maturity at **3.43/5** reflects strong factors and configurations (AUTH-001/006/007 at L4), yet material exposure remains where legacy protocols and gaps in policy enforcement allow MFA bypass (AUTH-005) and increase susceptibility to prompt bombing absent number matching (AUTH-002). Password hygiene remains partly manual, with no real-time banned password screening (AUTH-004).

These shortcomings drive Critical risk (RISK-013) and High risk (RISK-006) and lower compliance with ISO 27001:2022 A.5.16/A.8.2, NIST CSF PR.AA-02, CIS 4.7/6.6, LGPD Art. 32, IBGC Cap. 5.4/5.5, PSI 5.3, and ISF SGP TS.1.3.

Privileged Access Management (PAM)

PAM maturity is the strongest at **3.67/5**, with consistent strength in credential vaulting, session control, and privileged account governance (PAM-001/002/003 at L4). However, the absence of a fully implemented tiering model (PAM-004) and rigorously governed break-glass access (PAM-005) leaves high-value assets exposed to lateral movement and emergency-access misuse.

These gaps directly contribute to Critical risks of administrative credential compromise (RISK-001), lateral movement via local admin (RISK-004), and conflict of interest in privileged access (RISK-010), with downstream standards impact across NIST CSF PR.AA, ISO 27001:2022 A.5.16, CIS 6.x/4.x, and ISF SGP IM/TS domains.

4. Compliance Analysis

Controls were mapped to seven standards. Overall compliance stands at **72.0%**, with strongest alignment to NIST CSF 2.0 and ISF SGP 2024. Gaps cluster around authentication hardening (legacy/MFA bypass), lifecycle rigor (access certification and guest governance), and monitoring and detection (centralized logging, analytics, and high-risk response).

Remediation of a small set of controls would uplift multiple standards simultaneously. For example, closing AUTH-005 and MON-001/002 would improve ISO 27001:2022 A.5.16/A.8.2 and NIST CSF PR.AA-02/DE.AE-02, while JML-004/006 would address LGPD Art. 5/39 and CIS 6.7/6.8.

Standard	Compliance	Compliant/ Total	Key Gaps (Control → Clause/Function)
ISO 27001:2022	**70.5%**	**31/44**	AUTH-005 → A.5.16 (L2), AUTH-005 → A.8.2 (L2), JML-004 → A.5.18 (L2), JML-006 → A.5.19 (L1), JML-006 → A.5.21 (L1)
NIST CSF 2.0	**74.1%**	**20/27**	AUTH-005 → PR.AA-02 (L2), JML-004 → PR.AA-01 (L2), JML-006 → ID.RA-03 (L1), MON-001 → DE.AE-02 (L2), MON-002 → DE.AE-06 (L2)
CIS Controls v8	**67.9%**	**19/28**	AUTH-005 → 4.7 (L2), AUTH-005 → 6.6 (L2), JML-004 → 6.8 (L2), JML-006 → 6.7 (L1), MON-001 → 8.2 (L2)
LGPD/GDPR	**72.0%**	**18/25**	AUTH-005 → Art. 32 (L2), JML-004 → Art. 5 (L2), JML-006 → Art. 39 (L1), MON-001 → Art. 37 (L2), MON-002 → Art. 46 (L2)
IBGC 6ª Edição	**68.4%**	**26/38**	AUTH-005 → Cap. 5.4 (L2), AUTH-005 → Cap. 5.5 (L2), JML-004 → Cap. 5.5 (L2), JML-004 → Cap. 1.6 (L2), JML-006 → Cap. 5.5 (L1)
PSI-CORP-001	**66.7%**	**10/15**	AUTH-005 → 5.3 (L2), JML-004 → 4.3 (L2), MON-001 → 7.1 (L2), MON-003 → 7.2 (L2), MON-005 → 5.3 (L2)
ISF SGP 2024	**72.0%**	**18/25**	AUTH-005 → TS.1.3 (L2), JML-004 → IM.3.1 (L2), JML-006 → IM.2.4 (L1), MON-001 → SM.1.1 (L2), MON-002 → SM.2.2 (L2)

Addressing AUTH-005 (service accounts), JML-004/006 (reviews and guest TTL), and MON-001/002 (logging and response) yields the broadest compliance uplift in the least time. Implementing PAM-004/005 further strengthens governance and accountability expectations across multiple standards.

5. Risk Landscape

Risk severity distribution is skewed to the extreme: **9** Critical, **3** High, **1** Medium, and **0** Low. Residual risk remains Critical for the majority of top items due to incomplete deployment of monitoring, lifecycle rigor, and MFA hardening. Twelve risks are currently open or under mitigation.

Thematically, the portfolio concentrates on credential compromise (administrative and service), privilege accumulation and lateral movement, monitoring blind spots, and MFA bypass via legacy paths. These risks intersect key business-impact scenarios: disruption of Tier 0 services, exfiltration of sensitive data by insiders or ex-employees, and accountability failures with potential regulatory consequences. While ALE is currently **$0.00**, this should be interpreted as a measurement gap; a FAIR-based quantification sprint will translate these severities into probable loss ranges and inform investment prioritization.

Risk ID	Title	Level	Likelihood × Impact	Residual	Treatment	Status
RISK-001	Administrative Credentials Compromise	Critical	4 × 5 = **20**	Critical (20)	Modify	Mitigating
RISK-004	Lateral Movement via Local Admin	Critical	4 × 4 = **16**	Critical (16)	Modify	Open
RISK-005	Lack of Visibility into Suspicious Activity	Critical	4 × 4 = **16**	Critical (16)	Modify	Open
RISK-007	Service Account Compromise	Critical	4 × 4 = **16**	Critical (16)	Modify	Open
RISK-002	Privilege Accumulation (Privilege Creep)	Critical				