AXIS Platform

IAM Maturity Assessment

Meridian Financial Group (Sample)

1.90

Developing Maturity · 48% Control Alignment

WORKFORCE IAM ASSESSMENT

June 30, 2026

Financial Services · na · 12,000 Identities

AXIS Methodology v1.7

Question bank 2026.1 (4d9e8a442e1e…) · Scoring algorithm v2.0 · Benchmarks & financial constants: 2024–25 published research (constants effective Feb 2026)

Peer benchmark basis: research-derived estimate — no peer assessment data yet for this segment

Executive Summary

Meridian Financial Group (Sample), managing approximately 12,000 identities, rates **Developing** at **1.9 / 4.0** (48% control alignment) for Workforce IAM. This sits above the Financial Services peer benchmark of 1.6.

PAM is the strongest domain at 2.3. The largest opportunities are **Cloud** (1.6) and **IGA** (1.7). The failure pattern to address first: Stolen credentials remain valid for long periods. Compromise window is still large. 3 domains fall below the Developing threshold (2.0).

Against **ISO-27001**, the current posture is non-compliant. Modeled identity risk exposure is $965K–$1.2M annually (assumptions in the Financial Analysis section).

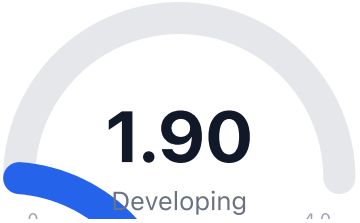
The vendor landscape has 3 domain gaps requiring attention.

1.90 Overall Maturity	**48%** Control Alignment	**$965K – $1.2M** Annualized Loss Exposure
26 Improvement Actions	**3** Vendors in Stack	**$179K – $210K** Potential Annual Savings

Control Alignment indicates the percentage of assessed controls meeting minimum maturity thresholds. It does not constitute compliance certification.

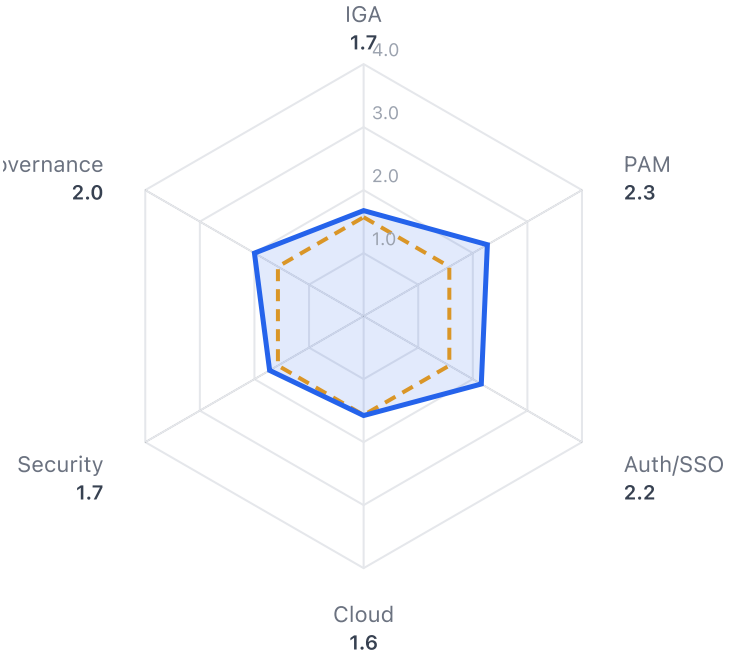
Maturity Overview

Overall Score



Benchmark: 1.57 (Financial Services) — Derived estimate

Domain Radar



Solid: Your Scores Dashed: Industry Benchmark

Domain Breakdown

Domain Deep Dive

Detailed analysis of each assessed domain, including identified strengths, gaps, and foundational control issues.

IGA

1.67

6 questions evaluated

Developing

Gaps & Recommendations

- Access Reviews & Recertification: Level 1 — Integrate access review outcomes with automated deprovisioning workflows.
- Entitlement Discovery and Classification: Level 1 — Connect IGA platform to critical applications to pull entitlement data automatically.

Evidence the next level expects

- **Access Reviews & Recertification:** Automated campaign scheduling; Direct integration with target systems
- **Entitlement Discovery and Classification:** IGA connectors pulling entitlement data from applications; Classification taxonomy applied (e.g., sensitive, standard, privileged)

PAM

2.27

5 questions evaluated

Developing

Strengths

- Admin Credential Protection: Level 3
- Session Management and Recording: Level 3

Gaps & Recommendations

- Just-In-Time (JIT) Cloud & Infrastructure Access: Level 1 — Automate access provisioning and revocation.

Evidence the next level expects

- **Just-In-Time (JIT) Cloud & Infrastructure Access:** JIT tooling integrated with IAM; Time-limited roles

Auth/SSO

2.16

5 questions evaluated

Developing

Strengths

- Adaptive MFA: Level 3
- Phishing-Resistant MFA & Session Integrity: Level 3

Gaps & Recommendations

- Account Recovery & Identity Verification Resistance: Level 1 — Replace KBA with out-of-band verification: callback to a number of record, manager attestation, or a one-time code to a registered secondary channel.

Evidence the next level expects

- **Account Recovery & Identity Verification Resistance:** Callback / manager-attestation workflow enforced in tooling; Privileged resets require dual control

Cloud

1.58

5 questions evaluated

Developing

Gaps & Recommendations

- Non-Human Identity (NHI) Governance: Level 1 — Automate rotation and enforce short TTLs for non-human credentials.
- AI Agent Identity Governance: Level 1 — Implement agent-specific identity policies that distinguish agents by autonomy level, replace static credentials with OIDC/OAuth dynamic tokens, and establish basic behavioral baselines, starting with tool-connection (MCP-style) credentials, which proliferate fastest.

Evidence the next level expects

- **Non-Human Identity (NHI) Governance:** Role-based policies for service accounts; Rotation intervals <30 days
- **AI Agent Identity Governance:** Autonomy-level classification applied to all agents (e.g., read-only, task-scoped, autonomous); Dynamic credential issuance (OIDC, OAuth client credentials) replacing static API keys

Security

1.72

5 questions evaluated

Developing

Gaps & Recommendations

- User Behavioral Analytics (UBA): Level 1 — Incorporate additional context signals (device posture, access history, peer behavior).
- Identity Posture & Attack-Surface Management (ISPM): Level 1 — Deploy posture tooling (IdP-native or ISPM) that scans dormancy, MFA gaps, and risky configurations on a schedule.

Evidence the next level expects

- **User Behavioral Analytics (UBA):** User or peer-group baselines defined; Risk scores generated per session or activity
- **Identity Posture & Attack-Surface Management (ISPM):** Automated posture findings with severity ranking; Trend reporting: exposure counts declining across cycles

Governance

2.00

4 questions evaluated

Developing

Regulatory Compliance

2	1	5
Aligned	At Risk	Non-Compliant

Compliance Heatmap

ISO-27001 0%	SOC2 0%	NIST-800-53-MOD 0%	DORA 57%
NIST-800-63B 33%	SOX 75%	NIST-CSF 82%	NIS2 100%

Framework Detail

FRAMEWORK	THRESHOLD	CONTROLS	PASSING	ALIGNMENT	STATUS
ISO-27001	2.5	20	0 / 20	0%	Non-Compliant
SOC2	2.5	6	0 / 6	0%	Non-Compliant
NIST-800-53-MOD	2.5	6	0 / 6	0%	Non-Compliant
DORA	2.5	7	4 / 7	57%	Non-Compliant
NIST-800-63B	2.5	3	1 / 3	33%	Non-Compliant
SOX	2.0	4	3 / 4	75%	At Risk
NIST-CSF	2.0	11	9 / 11	82%	Aligned
NIS2	2.0	8	8 / 8	100%	Aligned

Financial Risk Analysis

Annualized Loss Expectancy (ALE)

> Based on 12,000 managed identities in the **Financial Services** sector, with a cost per record of **$175** (see Model Assumptions below).

Model Assumptions & Data Sources

- Cost per record: IBM/Ponemon Cost of a Data Breach 2025, industry-specific (constants effective Feb 2026; refreshed with each methodology release).
- Risk factor range: conservative bound anchored to the IBM/Ponemon 2025 finding of 34% cost reduction from mature security controls; optimistic bound models compound multi-domain effects and is pending pilot validation.
- Potential savings assume a +1.0 maturity-level improvement (capped at 4.0) — a target, not a projection.
- Insurance factors: derived from 2024–25 insurer surveys (Delinea, Coalition); no carrier publishes exact discount percentages — treat as directional ranges.
- FTE model: calibrated to published case-study data at a $75/hr fully-loaded North-America rate (2025 vintage).

$965K – $1.2M	46% – 59%	1.00x
Current ALE (Range)	Risk Factor	Scale Factor

Improvement Potential

$179K – $210K	0%
Potential Annual Savings	Insurance Premium Reduction
Score 1.90 → 2.90	

Operational Cost (FTE Model)

> **5.8 FTE** estimated for IAM operations (11,977 hrs/yr at $75/hr = **$898,261**/yr). Maturity gap: 2.10 levels below optimized.

Insurance Premium Factors

CONTROL FACTOR	DOMAIN SCORE	QUALIFICATION	REDUCTION
Privileged Access Management	2.27	Below Threshold	0.0%
Multi-Factor Authentication	2.16	Below Threshold	0.0%
Identity Governance	1.67	Below Threshold	0.0%
Security Automation (ITDR)	1.72	Below Threshold	0.0%

Financial Impact Disclaimer: *Risk exposure is presented as a range. The lower bound reflects published research findings on cost reduction from mature security controls (34% reduction). The upper bound includes estimated compound effects from comprehensive IAM control maturity across multiple domains. Actual risk exposure depends on organization-specific factors not captured in this assessment. These figures are intended for directional planning purposes only and do not constitute financial advice. Organizations should consult qualified financial and risk management professionals before making investment decisions based on these estimates.*

Resource Estimates Disclaimer: *Full-Time Equivalent (FTE) projections are based on industry averages and assessment-derived maturity levels. Actual staffing requirements will vary based on organizational size, complexity, existing capabilities, and strategic priorities.*

Insurance Disclaimer: *Insurance premium estimates and coverage recommendations are generalized projections and do not constitute insurance advice. Consult a licensed insurance broker or risk management professional for coverage decisions specific to your organization.*

Business Value Drivers

Key business outcomes currently being delivered through your IAM maturity. These represent the strategic value your identity program provides to the organization.

Admin Credential Protection

Low

PAM · Level 3

Delivers measurable reduction in breach probability and improves operational resilience.

Session Management and Recording

Low

PAM · Level 3

Detects compromised privileged sessions before damage is done, not after.

Adaptive MFA

Low

Auth/SSO · Level 3

Hardens the workforce perimeter while minimizing interruptions.

Phishing-Resistant MFA & Session Integrity

Low

Auth/SSO · Level 3

Provides strong assurance for critical access without degrading usability.

Lifecycle Management (Joiner / Mover / Leaver)

Medium

IGA · Level 2

Prevents toxic access combinations and reduces audit remediation effort.

Access Requests & Approvals

Medium

IGA · Level 2

Reduces unnecessary access grants and improves decision quality.

Role-Based Access Control (RBAC) & Access Modeling

Medium

IGA · Level 2

Reduces request volume and improves access consistency.

Segregation of Duties (SoD)

Medium

IGA · Level 2

Reduces remediation cost by catching conflicts earlier in the access lifecycle.

First Domino Strategy

Foundational controls that gate overall maturity. The domino effect means that weakness in these controls caps your entire score, regardless of excellence elsewhere.

Foundational Controls

IGA-01: Lifecycle Management (Joiner / Mover / Leaver)

IGA

Level 2

Identity lifecycle failures compound silently. Every manual joiner or delayed leaver creates long-lived access risk that audits only discover after damage is done.

Risk: Access accumulation during role changes. Users retain entitlements from previous roles.

Next move: Implement event-driven access recalculation for movers based on authoritative attributes.

PAM-02: Secrets Management (Non-Human & Application Credentials)

PAM

Level 2

Secrets bypass humans entirely. If they are unmanaged, your strongest human IAM controls are irrelevant.

Risk: Compromised workloads can still reuse valid identities even if secrets rotate.

Next move: Move toward identity-based, short-lived credentials tied to workload identity.

CLOUD-01: Multi-Cloud Permission Management (CIEM)

Cloud

Level 2

Cloud permissions quietly become your biggest breach multiplier. If identity is federated but permissions are wild, you still lose.

Risk: Privilege creep returns between cleanups. The system trends back toward over-privilege.

Next move: Automate right-sizing and require time-bound elevation for sensitive cloud privileges.

SEC-01: Identity Threat Detection & Response (ITDR)

Security

Level 2

Prevention fails. If you can't detect identity abuse quickly, you are donating time to attackers.

Risk: Manual response delays allow attackers to pivot quickly.

Next move: Automate containment (token revocation, user disablement, step-up auth) for high-confidence detections.

GOV-01: Identity Data Ownership

Level 2

Governance

Identity is a business accountability problem disguised as a technical one. Without clear ownership, every control eventually fails.

Risk: Governance inconsistency. Similar access is treated differently across silos.

Next move: Standardize ownership roles, approval criteria, and escalation paths enterprise-wide.

PAM-01: Admin Credential Protection

Level 3

PAM

If admin credentials are weak, everything else is theater. Privileged access bypasses your entire control stack.

Risk: Approval fatigue or rubber-stamping can recreate standing privilege in practice.

Next move: Layer risk scoring into privileged elevation (context-aware approvals) and continuously right-size privileged roles and paths.

AUTH-01: Adaptive MFA

Level 3

Auth/SSO

Static MFA is no longer enough. If attackers can hijack sessions or fatigue users, your 'MFA' becomes a checkbox, not a barrier.

Risk: Risk engine integrity becomes the weak point; poor telemetry leads to blind spots or over-blocking.

Next move: Extend from login-time decisions to session-time decisions (continuous access evaluation).

Vendor Strategy

3	6/9	3	0
Total Vendors	Domain Coverage	Coverage Gaps	Redundancies

Coverage Gaps

Cloud & SaaS IAM	MEDIUM
Customer Identity × Data Security	MEDIUM
Customer Identity × Privileged Access Management	MEDIUM

Strategic Roadmap

Prioritized improvement plan organized into three horizons based on impact, effort, and foundational dependencies.

Quick Wins — start here

High-leverage items with Low–Medium effort. Each also appears in its horizon below.

- **AUTH-05** — Replace KBA with out-of-band verification: callback to a number of record, manager attestation, or a one-time code to a registered secondary channel.
- **PAM-04** — Automate access provisioning and revocation.
- **CLOUD-02** — Automate rotation and enforce short TTLs for non-human credentials.
- **CLOUD-05** — Implement agent-specific identity policies that distinguish agents by autonomy level, replace static credentials with OIDC/OAuth dynamic tokens, and establish basic behavioral baselines, starting with tool-connection (MCP-style) credentials, which proliferate fastest.
- **SEC-03** — Incorporate additional context signals (device posture, access history, peer behavior).

Horizon 1	Horizon 2	Horizon 3
0	6	20
Stabilize — Foundational Fixes	Unlock — High-Impact Gains	Differentiate — Optimization

H1 Stabilize

All foundational (domino) controls below Level 2. These must be addressed first as they cap overall maturity.

No items in this horizon.

H2 Unlock

High and Critical impact controls below Level 2. Addressing these unlocks meaningful maturity improvement.

ID	DOMAIN	LEVEL	IMPACT	EFFORT	NEXT MOVE
AUTH-05	Auth/SSO	L1 → L2	High	Low	Replace KBA with out-of-band verification: callback to a number of record, manager attestation, or a one-time code to a registered secondary channel.
PAM-04	PAM	L1 → L2	High	Medium	Automate access provisioning and revocation.
CLOUD-02	Cloud	L1 → L2	High	Medium	Automate rotation and enforce short TTLs for non-human credentials.

ID	DOMAIN	LEVEL	IMPACT	EFFORT	NEXT MOVE
CLOUD-05	Cloud	L1 → L2	High	Medium	Implement agent-specific identity policies that distinguish agents by autonomy level, replace static credentials with OIDC/OAuth dynamic tokens, and establish basic behavioral baselines, starting with tool-connection (MCP-style) credentials, which proliferate fastest.
SEC-03	Security	L1 → L2	High	Medium	Incorporate additional context signals (device posture, access history, peer behavior).
SEC-05	Security	L1 → L2	High	Medium	Deploy posture tooling (IdP-native or ISPM) that scans dormancy, MFA gaps, and risky configurations on a schedule.

H3 Differentiate

All remaining controls below Level 3. These move the organization toward industry-leading maturity.

ID	DOMAIN	LEVEL	IMPACT	EFFORT	NEXT MOVE
IGA-01 *	IGA	L2 → L3	Medium	Medium	Implement event-driven access recalculation for movers based on authoritative attributes.
PAM-02 *	PAM	L2 → L3	Medium	Medium	Move toward identity-based, short-lived credentials tied to workload identity.
GOV-01 *	Governance	L2 → L3	Medium	Medium	Standardize ownership roles, approval criteria, and escalation paths enterprise-wide.
CLOUD-01 *	Cloud	L2 → L3	Medium	High	Automate right-sizing and require time-bound elevation for sensitive cloud privileges.
SEC-01 *	Security	L2 → L3	Medium	High	Automate containment (token revocation, user disablement, step-up auth) for high-confidence detections.
IGA-02	IGA	L2 → L3	Medium	Medium	Enhance approvals with contextual data (role, peer access, risk level).
IGA-04	IGA	L2 → L3	Medium	Medium	Align roles with business policies and lifecycle attributes rather than historical access.
IGA-05	IGA	L1 → L3	Medium	Medium	Connect IGA platform to critical applications to pull entitlement data automatically.
PAM-03	PAM	L2 → L3	Medium	Medium	Incorporate risk signals (device health, user role, behavior) into elevation decisions.
GOV-02	Governance	L2 → L3	Medium	Medium	Translate IAM KRIs into financial, compliance, or operational risk language consumable by executives.
GOV-03	Governance	L2 → L3	Medium	Medium	Move from periodic detection to continuous enforcement for high-risk IAM policies.

ID	DOMAIN	LEVEL	IMPACT	EFFORT	NEXT MOVE
IGA-03	IGA	L1 → L3	Medium	High	Integrate access review outcomes with automated deprovisioning workflows.
IGA-06	IGA	L2 → L3	Medium	High	Embed SoD checks into provisioning workflows so conflicts are prevented before access is granted.
AUTH-02	Auth/SSO	L2 → L3	Medium	High	Formally prohibit local authentication and implement an exception process with risk acceptance and expiry.
AUTH-03	Auth/SSO	L2 → L3	Medium	High	Integrate EDR and device health signals into conditional access decisions.

+ 5 more items

Technical Backlog

Prioritized user stories for remediation, ready for Jira import. Each item maps to one assessment control with clear acceptance criteria.

1	7	18
High Priority	Medium Priority	Low Priority

ID	DOMAIN	CAPABILITY	LEVEL	PRIORITY	EFFORT	ACCEPTANCE CRITERIA
IGA-01 *	IGA	Lifecycle Management (Joiner / Mover / Leaver)	L2 → L3	Low	High	Near-real-time lifecycle execution
PAM-02 *	PAM	Secrets Management (Non-Human & Application Credentials)	L2 → L3	Low	High	Ephemeral credential model
CLOUD-01 *	Cloud	Multi-Cloud Permission Management (CIEM)	L2 → L3	Low	High	Policy-as-code and automated exception governance
SEC-01 *	Security	Identity Threat Detection & Response (ITDR)	L2 → L3	Low	High	Continuous validation via purple-team exercises and attack simulations
GOV-01 *	Governance	Identity Data Ownership	L2 → L3	Low	High	Governance-enabled automation
CLOUD-05	Cloud	AI Agent Identity Governance	L1 → L2	High	High	Real-time behavioral monitoring with contextual authorization
IGA-03	IGA	Access Reviews & Recertification	L1 → L2	Medium	Medium	Risk-scoped reviews
AUTH-05	Auth/SSO	Account Recovery & Identity Verification Resistance	L1 → L2	Medium	Medium	High-assurance verification for high-risk recovery
SEC-05	Security	Identity Posture & Attack-Surface Management (ISPM)	L1 → L2	Medium	Medium	Attack-path context and ownership

ID	DOMAIN	CAPABILITY	LEVEL	PRIORITY	EFFORT	ACCEPTANCE CRITERIA
IGA-05	IGA	Entitlement Discovery and Classification	L1 → L2	Medium	High	Risk-scored entitlement catalog integrated into governance workflows
PAM-04	PAM	Just-In-Time (JIT) Cloud & Infrastructure Access	L1 → L2	Medium	High	Risk-based JIT
CLOUD-02	Cloud	Non-Human Identity (NHI) Governance	L1 → L2	Medium	High	Keyless workload identity
SEC-03	Security	User Behavioral Analytics (UBA)	L1 → L2	Medium	High	Automated risk scoring with response recommendations
IGA-02	IGA	Access Requests & Approvals	L2 → L3	Low	High	Exception-focused governance
IGA-04	IGA	Role-Based Access Control (RBAC) & Access Modeling	L2 → L3	Low	High	Stable, scalable access model
IGA-06	IGA	Segregation of Duties (SoD)	L2 → L3	Low	High	Continuous SoD monitoring with risk-adaptive enforcement
PAM-03	PAM	Endpoint Privilege & Local Admin Control	L2 → L3	Low	High	Least-privilege endpoint enforcement
AUTH-02	Auth/SSO	Single Sign-On (SSO) Coverage & Enforcement	L2 → L3	Low	High	Passwordless-ready authentication posture
AUTH-03	Auth/SSO	Device Trust & Zero Trust Enforcement	L2 → L3	Low	High	Full Zero Trust access enforcement
CLOUD-03	Cloud	SaaS Application Discovery & Shadow IT Control	L2 → L3	Low	High	Continuous SaaS posture monitoring

+ 6 additional items. Full backlog available via CSV export.

* Denotes foundational (domino) control — address these first.

Disclaimers

Financial Impact Disclaimer

The Annualized Loss Expectancy (ALE) and related financial estimates presented in this report are approximations derived from assessment responses and industry benchmarks. These figures are intended for directional planning purposes only and do not constitute financial advice. Actual financial impact may vary significantly based on organizational context, threat landscape, and market conditions. Organizations should consult qualified financial and risk management professionals before making investment decisions based on these estimates.

Resource Estimates Disclaimer

Full-Time Equivalent (FTE) projections are based on industry averages and assessment-derived maturity levels. Actual staffing requirements will vary based on organizational size, complexity, existing capabilities, and strategic priorities.

Insurance Disclaimer

Insurance premium estimates and coverage recommendations are generalized projections and do not constitute insurance advice. Consult a licensed insurance broker or risk management professional for coverage decisions specific to your organization.

General

This report is generated using the AXIS Methodology and is intended as a professional assessment tool. The scores, recommendations, and analyses contained herein reflect the state of the organization at the time of assessment and should be periodically reviewed and updated. This report does not guarantee compliance with any regulatory framework and should not be used as the sole basis for compliance certification decisions.

Appendix

A. Methodology Summary

This assessment uses the AXIS Methodology, which evaluates IAM maturity across 6 domains using a 5-level maturity model (0 = None through 4 = Optimized).

Scoring Model

Domain scores are calculated as impact-weighted averages of individual question responses. Impact weights (Critical = 6.0, High = 3.5, Medium = 1.5, Low = 0.8) ensure that high-impact controls have proportionally greater influence. The overall score is a domain-weighted average, with PAM (1.3x), IGA (1.2x), and Security (1.2x) weighted more heavily due to their foundational importance.

Domino Controls

Certain questions are designated as "domino" or foundational controls. If any foundational control scores below Level 2, a maturity cap is applied to the overall score, reflecting the reality that advanced maturity is not achievable without foundational hygiene.

Financial Models

The Annualized Loss Expectancy (ALE) model uses industry-specific cost-per-record data from published breach research, combined with a maturity-based risk factor. Insurance premium impact estimates are based on published cyber insurance research. Full source citations are available in Methodology v1.6 Section 6.3.

B. Assessment Scope

Scope: **Workforce IAM (6 domains)**

Industry: **Financial Services**

Region: **na**

Identity Count: **12,000**

C. Maturity Level Definitions

LEVEL	LABEL	DESCRIPTION
0	**Absent**	No capability / Ad-hoc
1	**Initial**	Initial / Reactive
2	**Developing**	Defined / Repeatable
3	**Established**	Managed / Proactive
4	**Optimized**	Optimized / Continuous improvement

D. Glossary

ALE	Annualized Loss Expectancy — estimated annual financial exposure from identity-related incidents
CIAM	Customer Identity and Access Management
FTE	Full-Time Equivalent — standardized measure of workforce effort
IAM	Identity and Access Management
IGA	Identity Governance and Administration
PAM	Privileged Access Management
RLS	Row Level Security — database-level access control
SSO	Single Sign-On

E. Benchmark Confidence Key

Industry benchmark values vary in their empirical backing. The following key indicates the confidence level of each benchmark used in this report:

INDICATOR	LEVEL	MEANING
●	Research-backed	Derived from multiple independent published research sources
◐	Derived estimate	Extrapolated from cross-industry averages and analyst reports
○	Pending validation	Directional estimate pending empirical validation from AXIS assessments

This assessment used: **Financial Services** benchmark (1.57) — Derived estimate: Published industry research (2024–25)

Report generated by AXIS Platform · AXIS Methodology · 2026-07-03