



Product Data Sheet:

Identity Analytics and Compliance Manager (IACM)

In today's fast-paced digital environment, organisations struggle with visibility into identities and access, managing compliance risks, and ensuring governance across human and machine identities. With compliance mandates tightening and AI-powered cyber threats increasing, modern identity governance must go beyond access visibility and certification.

Fálaina IACM provides a single-pane-of-glass visibility into user and non-human access, ensuring continuous monitoring, certification, and governance to maintain security and compliance. With AI-driven identity analytics, enterprises can detect anomalies, automate access reviews, and enforce Zero Trust security models.

Fálaina IACM Key Functionalities:

1. Identity & Access Visibility

- Provides complete insight into identity and access relationships across users, machines, and applications.
- Tracks historical access changes with an identity timeline for auditing and compliance.

2. Access Certification & Continuous Compliance

- Automates periodic access reviews and certifications to ensure compliance with GDPR, HIPAA, SOX, ISO 27001 and any other local and regional regulatory requirements.
- Supports policy-driven recertification and risk-based access approvals to enforce least-privilege access.

Industry Trends & Statistics:

- 80% of security breaches are linked to poor identity management.
- 45% of organisations still rely on manual identity governance processes.
- \$5.3M is the average cost of a compliance failure, making proper governance a necessity.
- Zero Trust adoption is accelerating, with 60% of enterprises implementing Zero Trust security principles.
- AI-driven risk scoring is becoming a standard, reducing identity-related risks by up to 40%.

Source: Gartner

3. Segregation of Duties (SoD) & Sensitive Access Controls

- Prevents conflicts of interest with intelligent, policy-driven SoD enforcement.
- Enforces real-time access policies to prevent toxic access combinations and privilege creep.

4. AI-Powered Role & Policy Management

- AI-driven role mining and automated policy recommendations streamline identity governance.
- Identifies over-provisioned users, suggests optimised roles, and enforces access policies dynamically.

5. Machine Identity & Non-Human Access Governance

- Extends governance to service accounts, bots, APIs, and cloud workloads to enforce security and compliance.
- Applies least-privilege access controls to non-human identities to prevent over-permissioned access.

6. Cloud Infrastructure Entitlement Management (CIEM) Integration

- Integrates with AWS, Azure, and GCP security tools to manage cloud entitlements and detect excessive privileges.
- Prevents privilege escalation risks and ensures governance for multi-cloud workloads.

7. Dynamic Risk Scoring & AI-Driven Access Recommendations

- Uses AI-powered analytics to detect high-risk access patterns, privilege misuse, and anomalous behaviour.
- Automated risk-based access adjustments ensure real-time enforcement of Zero Trust security principles.

8. Security Information and Event Management (SIEM) Integration

- Feeds identity-related security events into SIEM tools such as Splunk, IBM QRadar, and Microsoft Sentinel.
- Enables real-time identity threat detection (i.e. - SoD violations, backdoor access) investigation, and automated response actions.

9. Automated Auditing & Compliance Reporting

- Generates audit-ready reports with AI-enhanced insights for GDPR, NIST, ISO 27001, and financial regulations.
- Provides continuous compliance enforcement and policy validation across all identity transactions.

10. Conversational Identity Assistant

- Automates self-service identity tasks such as access requests, password resets, and role assignments.
- Enhances user experience with AI-driven virtual assistants for identity-related workflows.

Business Benefits:

- Automated Compliance & Audit-Ready Governance – Ensures continuous compliance with GDPR, HIPAA, SOX, ISO 27001, reducing audit failures by 60%.
- AI-Driven Access Risk Analytics – Identifies toxic access combinations, privilege creep, and unauthorised access attempts in real-time.
- Elimination of Manual Access Reviews – Automates access certifications, policy enforcement, and periodic reviews, reducing IT workload by 40%.
- Zero Trust-Based Access Controls – Implements risk-based, dynamic access restrictions, enforcing least-privilege access across all environments.

Case Studies

• Global Bank (Financial Services)

- Challenge: Compliance challenges in managing cross-region identity governance across multiple banking applications.
- Outcome: Reduced compliance audit time by 60%, improved visibility into privileged access and sensitive data handling, and eliminated manual identity certification errors.

• Healthcare Provider (Healthcare & Life Sciences)

- Challenge: Ensuring HIPAA compliance and securing electronic health records (EHRs) against unauthorised access.
- Outcome: Achieved full audit compliance, eliminated manual inefficiencies in access certification, and reduced unauthorised access risks by 40%.

Technical Specifications

- Deployment Models: SaaS, on-premises, and hybrid options with a unified codebase.
- Integrations: Prebuilt connectors for 70+ target systems, including legacy On-premise, cloud and SaaS applications.
- Scalability: Designed for mid-market and large enterprises with dynamic scalability.
- API Support: RESTful APIs for custom integrations.

Pricing and Licensing

- Pricing Model: Subscription
- User Licensing: Flexible plans based on the number of users and connectors.
- Support Packages: Available in Basic, Standard, and Premium tiers, offering various levels of support and response times.

Why Fálaina?

We understand — Managing identity governance and access compliance can be complicated and overwhelming. That's why we've designed a solution that simplifies access control, automates compliance, and gives you full visibility over who has access to what—putting you back in control.

- AI-Powered Identity Risk Scoring – Uses machine learning to detect access anomalies and prevent security breaches before they happen.
- Comprehensive Identity & Access Governance – Governs human, non-human, and cloud identities with real-time risk assessments.
- Automated Role Mining & Policy Enforcement – Identifies over-provisioned users, suggests optimised roles, and prevents access creep.
- Pre-Built Enterprise Integrations – Seamlessly connects across On-premise, SaaS, and cloud platforms for frictionless deployment.
- Zero Trust & Continuous Access Monitoring – Enforces adaptive, risk-based access verification, ensuring compliance with enterprise security frameworks.

Simplify and Secure Your Identity Analytics & Compliance

Managing identity governance and access compliance shouldn't be complicated or overwhelming. With Fálaina Identity Analytics & Compliance Manager (IACM), you gain complete visibility into user access, automate compliance enforcement, and proactively mitigate access risks—ensuring security, governance, and regulatory compliance with ease.

Ready to Strengthen Your Identity Governance and Compliance?

- Visit www.falainacloud.com to learn more.
- Email us at sales@falainacloud.com to schedule a demo or talk to our team.

Turn Identity Governance into Your Strongest Advantage.



About Fálaina

Fálaina is at the forefront of cybersecurity innovation, delivering Converged Identity and Access Management (IAM) solutions that empower organisations to protect and optimise their digital ecosystems with unparalleled precision, scalability, and efficiency. Purpose-built to tackle the complexities of modern cybersecurity, Fálaina's unified platform integrates powerful capabilities, including Identity Governance and Administration (IGA), Privileged Access Management (PAM), Data Access Governance (DAG), Access Management (AM), and Zero Trust Architecture.

With Fálaina, identity security becomes the foundation of progress, helping businesses navigate the future with confidence, resilience, and agility.