SPG Intelligence

G-Cloud 15 Framework

Cloud Support

Identity and Access Management Service

SERVICE DEFINITION DOCUMENT

Newcastle HQ: Platinum Suite 15, Spire, Pilgrim Street, Newcastle Upon Tyne, NE1 2DS
Leeds Office: Orega 3rd floor, St. Paul's House, 23 Park Square S, Leeds LS1 2ND

1. Document Management

1.1. Version History

Document	Date	Version	Status
Identity and Access Management Service	January 2026	1.0	Approved

1.2. Approval Sign-Off

Position	R	A	C	I
CEO		X		
DoO	X			
CFO			X	X

Table of Contents

2. Executive Summary

Robust identity management is no longer a luxury but a critical necessity for safeguarding corporate environments against unauthorised access and cyber threats. SPG, committed to upholding the highest standards of security and compliance, is proud to partner with Saviynt to deliver the Enterprise Identity Cloud (EIC) as a transformative solution designed to meet these challenges head-on.

In the context of rising cyber threats, a significant proportion of application breaches stem from unauthorised access facilitated by default, shared, or stolen credentials. In the complex web of enterprise operations, each application might interact with hundreds of functions and potentially thousands of individuals. This interconnectivity, whilst powerful, presents significant risks. A single misassignment of roles can lead to a hazardous situation where an individual possesses the ability to both generate and approve critical transactions, such as creating and paying invoices.

SPG's Identity and Access Management Service provides a structured journey from initial assessment through rapid deployment to full production operations. Our approach combines the strategic clarity of Lightning Insights assessments, the speed-to-value of Fast Start packages, and the comprehensive capabilities required for enterprise-scale identity governance, all powered by the industry-leading Saviynt Enterprise Identity Cloud platform.

Key Service Differentiators

- Structured Journey: Progressive engagement model from assessment through implementation to production, with clear milestones and decision points
- Rapid Time-to-Value: Fast Start packages deliver production-ready identity governance within 12 weeks using proven methodologies
- Converged Identity Platform: Unified governance across IGA, PAM, CIEM, and third-party access management through Saviynt EIC
- AI-Enhanced Intelligence: Machine learning algorithms continuously analyse access patterns, detect anomalies, and predict potential security risks
- Public Sector Expertise: Deep understanding of NHS, local government, blue-light, and justice sector requirements
- Fixed-Price Packages: Predictable commercial terms with defined outcomes and timelines

3. Service Overview

SPG's Identity and Access Management Service provides comprehensive identity governance, privileged access management, and cloud entitlement intelligence capabilities delivered through a structured, outcome-focused methodology. Powered by Saviynt Enterprise Identity Cloud, our service addresses the full spectrum of identity challenges facing modern organisations.

3.1. Service Scope

The service encompasses three core capability domains delivered through the Saviynt EIC platform:

Identity Governance and Administration (IGA)

Comprehensive management of user identities throughout their lifecycle, from initial onboarding through role transitions to secure offboarding. Saviynt's IGA capabilities include automated provisioning and deprovisioning, role-based access control, access certification campaigns, and continuous compliance monitoring. AI-enhanced analytics identify access anomalies and recommend optimised entitlements based on peer group analysis.

Privileged Access Management (PAM)

Comprehensive protection and monitoring of privileged accounts across on-premises and cloud environments. Saviynt's Cloud PAM capabilities include privileged credential vaulting, just-in-time access provisioning, session recording and monitoring, and privileged access analytics. Risk scoring continuously evaluates privileged access requests, automatically escalating high-risk activities for additional verification.

Cloud Infrastructure Entitlement Management (CIEM)

Specialised governance for cloud-native environments, addressing the unique challenges of managing access across AWS, Azure, and Google Cloud Platform. Saviynt's CIEM capabilities include cloud permission analysis, least-privilege enforcement, cross-cloud visibility, and continuous compliance monitoring. AI-powered analysis identifies excessive permissions and recommends right-sizing based on actual usage patterns.

3.2. Target Organisations

This service is designed for organisations requiring enterprise-grade identity governance capabilities:

- NHS Trusts, Integrated Care Systems, and NHS England arms-length bodies managing complex identity estates

- Universities and higher education institutions balancing open academic collaboration with security requirements
- Blue-light services and justice sector organisations requiring secure access across multi-agency environments
- Local government authorities managing citizen-facing services and internal operations
- Any organisation seeking to modernise identity capabilities with enterprise-grade solutions

4. The Identity Challenge

Modern organisations face an increasingly complex identity landscape. The proliferation of cloud services, remote working, and third-party integrations has exponentially increased the attack surface whilst traditional identity management approaches struggle to keep pace.

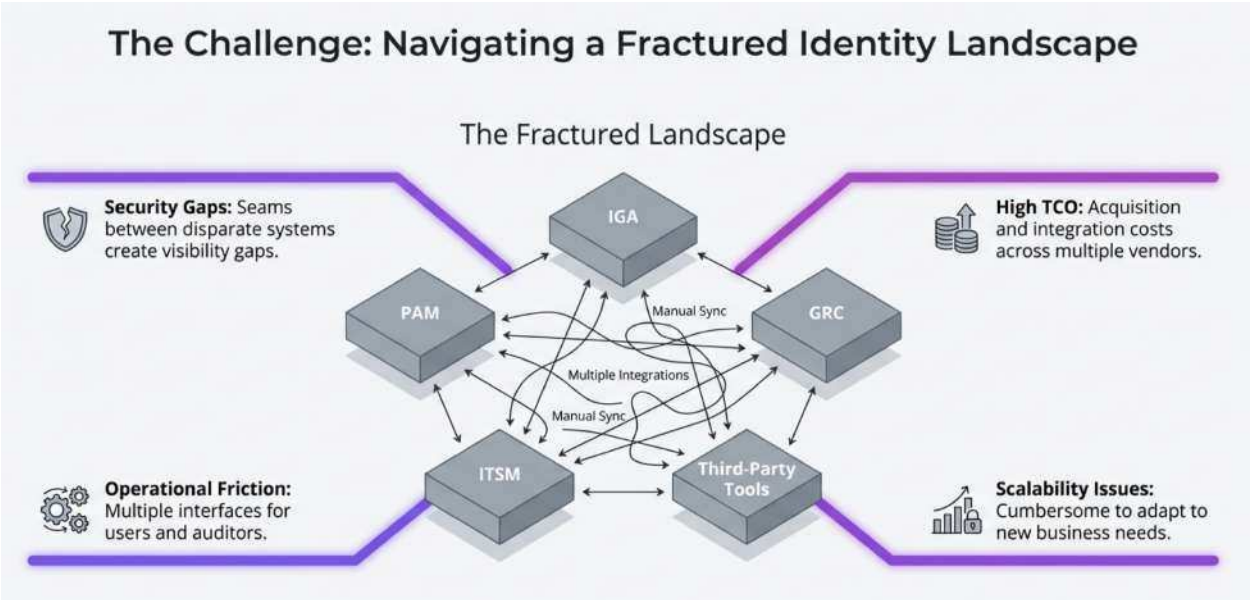
4.1. The Problem: Non-Converged Identity Stacks

In many organisations, particularly those with developing identity programmes, identity management involves a patchwork of disparate technologies. These often include separate solutions for Identity Governance and Administration (IGA), Privileged Access Management (PAM), Governance Risk and Compliance (GRC) tools, third-party management, and IT Service Management (ITSM). This non-converged approach creates significant challenges:

- Multiple Integrations: Organisations must establish and maintain numerous integrations with downstream applications and endpoints. These different identity technologies require interconnections that must be constantly managed and synchronised.
- Multiple Platforms for Users: End users, auditors, and application owners must navigate multiple solutions, complicating training and day-to-day operations whilst increasing the likelihood of security workarounds.
- High Maintenance Requirements: Each solution requires its own deployment, ongoing maintenance, and a team of knowledgeable administrators, increasing operational demands and specialist skills requirements.
- Higher Total Cost of Ownership: The financial burden of multiple systems, including acquisition, integration, and maintenance costs, contributes to significantly higher total cost of ownership.
- Scalability Challenges: As business needs evolve, scaling a non-converged identity stack becomes cumbersome and inefficient, often requiring additional integration or replacement of systems.
- Security Gaps: The seams between disparate systems create visibility gaps that sophisticated attackers can exploit.

4.2. The Imperative for Robust Internal Controls

Without robust identity controls, enterprises expose themselves not only to operational risks but also legal and regulatory repercussions. Inadequate oversight and lack of prompt corrective action can lead to compliance failures, audit findings, and reputational damage. It is imperative for organisations to meticulously manage access rights within their applications, ensuring that no individual has unchecked authority that could lead to both intentional abuses and inadvertent breaches of protocol.



5. Why Saviynt Enterprise Identity Cloud?

SPG assessed many vendors prior to electing to partner with Saviynt. The Enterprise Identity Cloud (EIC) distinguishes itself by offering a comprehensive suite of capabilities that simplify identity governance and streamline access controls. Its innovative approach ensures that only authorised personnel can access sensitive data, thereby reducing the risk of data breaches significantly.

By automating and enhancing identity and access management processes, Saviynt EIC enables organisations to focus on core business objectives. SPG delivers Saviynt EIC to provide the following advantages:

Enhanced Security Posture: SPG clients benefit from an enhanced security model that guards against unauthorised access through stringent yet flexible access controls and identity governance. This system is particularly crucial for organisations in Government, Health, or other regulatory environments.

Streamlined Compliance: Saviynt's solution comes pre-configured with compliance frameworks that significantly ease the burden of adhering to complex regulatory requirements such as GDPR, DSPT, and ISO 27001. This out-of-the-box compliance ensures that clients remain ahead of compliance obligations effortlessly.

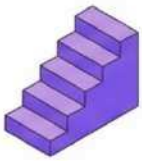
Operational Efficiency: By automating critical IAM functions, Saviynt EIC reduces manual overhead and operational costs. This automation allows for onboarding and offboarding processes, ensuring that user access rights are always aligned with current roles and responsibilities.

Real-Time Risk Management: As part of SPG's CloudOps service, we provide continuous monitoring and real-time risk assessment capabilities, enabling proactive management of potential security threats. This ongoing vigilance helps prevent security incidents and reduces the time and resources spent on resolving access-related issues.

Scalable and Flexible Architecture: Designed to support diverse enterprise environments, whether cloud-based, on-premises, or hybrid, Saviynt EIC adapts to specific organisational needs. Its scalability ensures that as organisations grow, their identity management capabilities can expand without compromising security or performance.

AI-Powered Intelligence: Saviynt's platform incorporates machine learning capabilities for intelligent role mining, anomaly detection, and risk-based access recommendations, transforming identity management from reactive administration to predictive security operations.

Strategic Value: Why SPG & Saviynt?

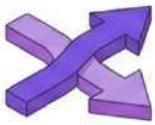


Structured Journey

Progressive engagement from assessment to production.

Rapid Time-to-Value

Production-ready identity governance in 12 weeks.



Converged Platform

Unified IGA, PAM, and CIEM reducing manual overhead.

AI-Enhanced

Machine learning for anomaly detection and risk scoring.

Public Sector Expertise

Deep understanding of NHS, Local Gov, and Blue-Light.

6. Service Delivery Model

SPG's Identity and Access Management Service follows a structured delivery model that guides organisations from initial assessment through to full production operations. This progressive approach ensures appropriate investment at each stage, with clear decision points and measurable outcomes throughout the journey.

Phase	Duration	Outcome	Next Step
Lightning Insights	5 consulting days	Maturity assessment and roadmap	Informed decision on transformation approach
Fast Start	12 weeks	Production-ready IGA foundation	Operational identity governance
Extended Implementation	Variable	Full capability deployment	Comprehensive identity platform
Production Operations	Ongoing	Managed service delivery	Continuous improvement

6.1. Phase 1: Lightning Insights Assessment

The Lightning Insights Assessment provides a structured, time-bound evaluation of your current Identity and Access Management environment, focusing on Identity Governance and Administration (IGA) and Privileged Access Management (PAM). Designed for IT and security leaders seeking strategic clarity, this assessment drives informed decision-making for IAM transformation.

Assessment Framework

Phase 1 - Strategic Foundation: Stakeholder alignment and current state discovery, including tooling inventory, policy review, and identity source mapping. This phase establishes the baseline understanding necessary for meaningful analysis.

Phase 2 - Operational Analysis: Evaluation of existing processes, data flows, and Joiner/Mover/Leaver procedures, identifying operational pain points and risk exposure. This phase examines how identity management functions in practice.

Phase 3 - Maturity Assessment: Structured workshops with key stakeholders across HR, IT, Security, and Application Owner communities. This collaborative approach ensures comprehensive coverage and organisational buy-in.

Phase 4 - Strategic Development: Conceptual architecture and prioritised roadmap development, aligning technical capabilities with business objectives and regulatory requirements.

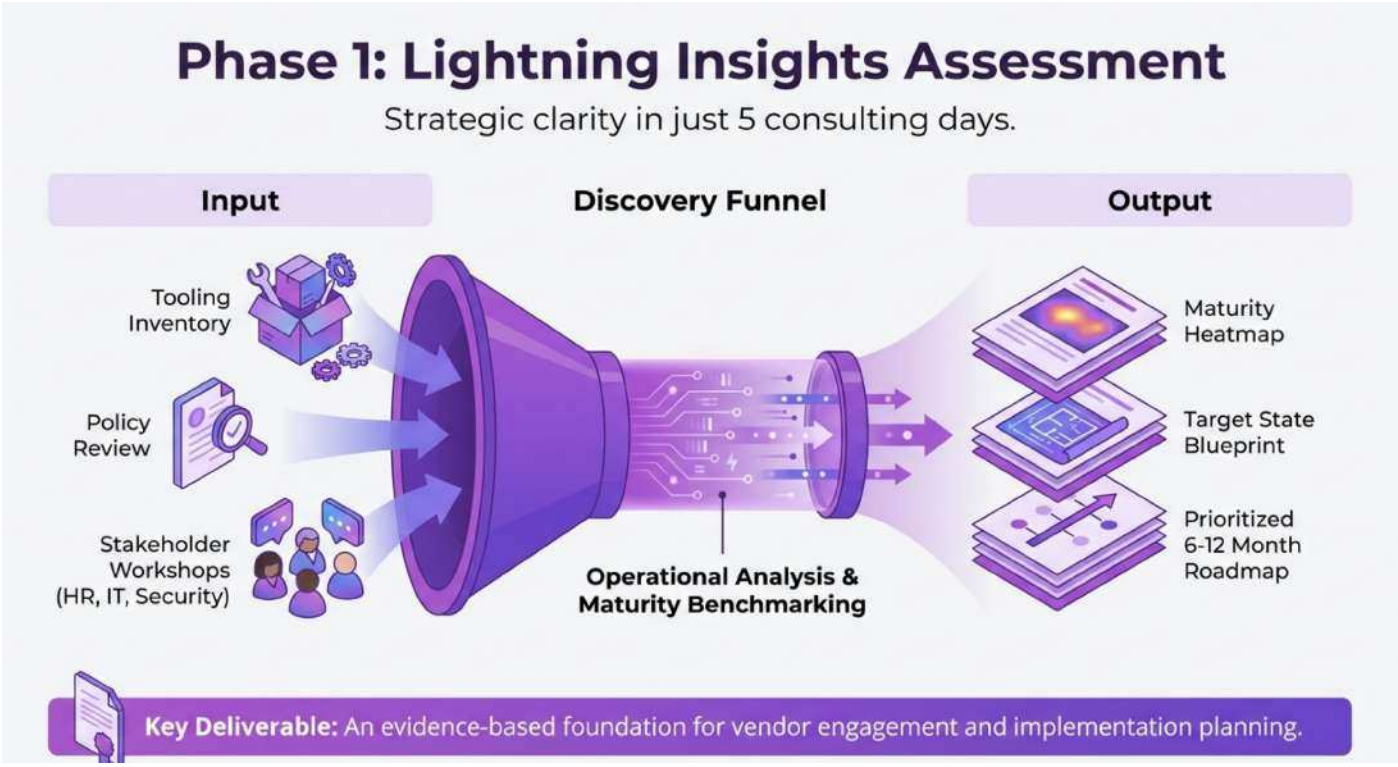
Phase 5 - Executive Reporting: Comprehensive findings and strategic recommendations presented in actionable format for executive decision-making and board-level governance.

Core Deliverables

- Executive Summary Report with maturity heatmap and priority actions
- Target State Blueprint featuring conceptual architecture and role model structure
- Prioritised 6–12-month roadmap with effort and value mapping
- Optional RFP Use Case Pack with vendor-neutral requirements

Strategic Benefits

- Clear visibility of current IAM maturity positioning against industry benchmarks
- Confidence for vendor engagement and procurement activities
- Evidence-based prioritisation of transformation investments
- Structured foundation for implementation planning



6.2. Phase 2: Fast Start Implementation

SPG delivers a time-boxed, low-risk identity governance foundation using Saviynt EIC, enhanced by SPG's readiness validation, risk transparency, and adoption support. The Fast Start package represents the perfect balance between speed-to-value and robust implementation, designed for organisations seeking immediate identity governance improvements without compromising on quality or security posture.

Scope Overview

Authoritative Source Integration: Validate HR data feed for completeness and anomalies. Integrate single HR source into Saviynt Identity Warehouse using predefined connector protocols. Comprehensive readiness documentation summarising data quality risks and mitigation steps.

Application Integrations: Selection and integration of 5 critical target systems from Saviynt's extensive library of predefined connectors. Comprehensive reconciliation of user accounts and rights across all integrated systems with pre- and post-integration snapshots demonstrating measurable risk reduction.

Identity Lifecycle Management: Configuration of up to 10 comprehensive Joiner/Mover/Leaver rules automating identity lifecycle processes. Implementation of sophisticated approval workflow supporting up to 4 levels of authorisation. Workshop facilitation to validate workflow designs and comprehensive documentation.

Access Governance: Deployment of User Manager Certification campaign utilising Saviynt's out-of-the-box functionality. Small-scale pilot campaign to validate processes before full-scale deployment. Detailed summary of revocations achieved and residual risk analysis.

Provisioning Automation: Comprehensive automation for provisioning and deprovisioning across all in-scope applications. Initial simulate-only observation period for validation before production deployment. Break-glass procedures and administrator troubleshooting guides.

Reporting and Dashboards: Deployment of Saviynt's comprehensive suite of out-of-the-box reports and dashboards. Compliance mapping linking reports to GDPR Article 5(1)(f), ISO 27001 Annex A.9, and NCSC Good Practice guidelines.

Branding and Adoption: Professional application of customer branding throughout the Saviynt interface. Comprehensive end-user quick start guides for the access request process.

Implementation Timeline

Week 0 - Readiness Sprint: Validation period to verify data quality, integration requirements, and connectivity before formal engagement commencement.

Weeks 1-12 - Core Implementation: Structured 12-week implementation programme aligned with Saviynt TTV methodology, ensuring production readiness within defined timeframe.

Week 13 - Hypercare: Intensive 1-week post-go-live support period with option to extend under separate agreement for additional stability assurance.

6.2.1. Fast Start Exclusions

Clear scope boundaries ensure predictable delivery and protect the fixed-timeline nature of the Fast Start package. The following items are excluded but can be delivered through Extended Implementation:

- Role-based access control (RBAC) modelling
- Segregation of Duties (SoD) policy definition
- Privileged Access Management (PAM) integration
- Custom report development beyond out-of-the-box capabilities
- Custom connector development
- Data cleansing and transformation
- Historical entitlement remediation

Customer Responsibilities

- Provide clean, validated user, account, and entitlement data in agreed formats and timeframes
- Provision and configure Dev/Test/Prod environments with required connectivity
- Nominate qualified business stakeholders for JML design validation and certification testing
- Execute comprehensive UAT using provided templates and frameworks
- Establish L1-L3 support model and operational procedures prior to handover

6.3. Phase 3: Extended Implementation

Following successful Fast Start deployment, organisations can extend their identity governance capabilities through targeted accelerator packages. These follow-on implementations build upon the established foundation to deliver comprehensive identity management across all domains.

Available Accelerator Packages

Compliance and Audit Enhancement: Establishes advanced compliance controls to govern user access to key enterprise applications. Includes automated certification campaigns, enhanced audit trail capture, and compliance reporting dashboards. Pre-configured for GDPR, DSPT, and Cyber Essentials requirements.

Application Access Governance (AAG): Provides visibility into toxic access combinations in business-critical applications. Prevents Separation of Duties conflicts by proactively applying mitigating controls. AI-driven analysis identifies hidden risks across application portfolios.

Cloud Privileged Access Management (CPAM): Secures cloud-based assets across AWS, Azure, and Google Cloud Platform. Includes privileged credential vaulting, just-in-time access provisioning, and session recording. AI-enhanced risk scoring for privileged access requests.

On-Premises PAM: Secures on-premises workloads including servers, databases, and network infrastructure. Options for password vaulting, session management, and privileged access analytics. Integration with existing SIEM and security operations tools.

Third-Party Access Governance (TPAG): Establishes governance framework for vendors, contractors, and third-party workforce. Includes sponsored identity management, time-bound access, and automated deprovisioning. Enhanced due diligence workflows for high-risk third parties.

Cloud Infrastructure Entitlement Management (CIEM): Prevents excessive cloud permissions across multi-cloud environments. AI-driven analysis of actual permission usage versus granted entitlements. Automated right-sizing recommendations with implementation workflows.

Extended Implementation Benefits

- Flexibility to add modules as building blocks based on organisational priorities
- Enhances existing IGA implementations without complete overhaul
- Focused on increasing security and governance over expanded areas of the business
- Leverages existing Saviynt investment and configurations

6.4. Phase 4: Production Operations

Following implementation, SPG offers comprehensive managed service options through our CloudOps service. This provides continuous monitoring, real-time risk assessment, and proactive management of identity infrastructure, ensuring sustained security posture and compliance.

Managed Service Capabilities

24/7 Platform Monitoring: Continuous monitoring of Saviynt EIC platform health, performance, and security. Proactive alerting and incident response for identity infrastructure issues.

Continuous Compliance Monitoring: Ongoing assessment of identity governance compliance against regulatory requirements. Automated reporting for audit cycles and compliance demonstrations.

Risk Analytics and Reporting: Regular analysis of identity risk posture with executive-level reporting. Trend analysis and recommendations for continuous improvement.

Platform Maintenance and Updates: Management of Saviynt platform updates, patches, and configuration changes. Change management processes ensuring minimal operational disruption.

Support Desk Services: Tiered support model for identity governance queries and issues. Escalation procedures for complex identity scenarios requiring specialist intervention.

Service Tiers

Tier	Scope
Essential	Core platform monitoring, quarterly reviews, standard support hours
Advanced	Enhanced monitoring, monthly reviews, extended support, proactive optimisation
Enterprise	24/7 support, dedicated account management, continuous improvement programme

7. Technical Capabilities

Saviynt Enterprise Identity Cloud provides a comprehensive suite of technical capabilities that address the full spectrum of identity governance requirements. The following capabilities are available through SPG's implementation and managed service offerings.

7.1. Identity Governance and Administration

- Automated identity lifecycle management with intelligent Joiner/Mover/Leaver processing
- Role-based access control with AI-driven role mining and optimisation
- Access request and approval workflows with configurable multi-level authorisation
- Access certification campaigns with intelligent recommendations
- Separation of Duties policy enforcement with real-time conflict detection

- Comprehensive audit trail and compliance reporting

7.2. Privileged Access Management

- Privileged credential vaulting with automatic rotation
- Just-in-time privileged access provisioning
- Session recording and monitoring for privileged activities
- Risk-based authentication for privileged access requests
- Emergency break-glass procedures with full audit capabilities

7.3. Cloud Infrastructure Entitlement Management

- Multi-cloud visibility across AWS, Azure, and Google Cloud Platform
- Permission analysis and least-privilege recommendations
- Cross-cloud policy enforcement and compliance monitoring
- Automated remediation of excessive permissions

7.4. Integration Capabilities

- Extensive library of pre-built connectors for enterprise applications
- Support for cloud, on-premises, and hybrid environments
- REST API for custom integrations and automation
- SCIM support for modern SaaS application integration

8. Features and Benefits

8.1. Out of the Box Ruleset

Feature: Saviynt EIC offers pre-configured rulesets that simplify the implementation of access controls across multiple ERP systems, providing a robust foundation for compliance and governance.

Benefit: Reduces the time and effort required to establish identity governance frameworks, ensuring rapid deployment and integration with existing systems without extensive customisation.

8.2. Fine Grained Separation of Duties

Feature: Enables detailed control over user actions at the page, function, TCode, Auth Object, or privilege level within applications, ensuring that sensitive tasks are appropriately segregated.

Benefit: Minimises the risk of fraud and enhances compliance by preventing conflicts of interest and ensuring that no single individual has control over all aspects of a critical function.

8.3. Automated Certification

Feature: Streamlines the access review process by automatically certifying user rights and permissions, significantly speeding up what is traditionally a manual and time-consuming process.

Benefit: Ensures consistent enforcement of access policies, reduces administrative burden, and helps maintain continuous compliance with fewer errors and less oversight.

8.4. Seamless Risk Reporting

Feature: Provides comprehensive risk assessment capabilities that aggregate and visualise risks across applications, using a predictive model to anticipate potential security issues.

Benefit: Offers actionable insights into security posture, enabling proactive risk management and informed decision-making to address vulnerabilities before they are exploited.

8.5. Our of the Box Compliance Management

Feature: Comes equipped with built-in compliance frameworks that are ready to deploy for a variety of regulatory standards including GDPR, SOX, HIPAA, and ISO 27001.

Benefit: Reduces the complexity and resources required to meet diverse regulatory requirements, ensuring compliance through automated checks and reports that are easy to generate and interpret.

9. Compliance and Security Frameworks

SPG's Identity and Access Management Service aligns with major security and compliance frameworks, ensuring that implementations meet regulatory requirements and industry best practices.

9.1. Supported Frameworks

- NIST Cybersecurity Framework: Full alignment with identity and access management controls across Identify, Protect, Detect, Respond, and Recover functions
- ISO 27001: Support for Annex A controls related to access management, user access provisioning, and privileged access management

- NHS Data Security and Protection Toolkit: Pre-configured controls and evidence collection for DSPT assertion requirements
- Cyber Essentials and Cyber Essentials Plus: Implementation of access control requirements for certification
- UK GDPR: Privacy by design principles embedded throughout, with automated data subject access request support
- SOX Compliance: Separation of duties controls and audit trail capabilities for financial services
- HIPAA: Access controls and audit capabilities for healthcare data protection

9.2. SPG Certifications

- ISO 9001:2015 Quality Management System
- ISO/IEC 27001:2022 Information Security Management System
- Cyber Essentials Plus Certification
- HM Government G-Cloud Supplier
- Microsoft Partner Network
- AWS Partner Network

10. Pricing

All rates associated with our Identity and Access Management Service can be found in the accompanying pricing and SFIA rate card documents on the Digital Marketplace.

Our pricing structure offers:

- Fixed-price packages for Lightning Insights assessments (5 consulting days)
- Fixed-price Fast Start implementation packages (12-week programme)
- Day-rate consultancy for Extended Implementation accelerator packages
- Tiered managed service subscriptions for ongoing Production Operations
- Volume discounts for multi-package implementations

Saviynt Enterprise Identity Cloud licensing is provided separately through SPG's partnership arrangement, with options for annual subscription or multi-year agreements. All pricing is exclusive of VAT and subject to the terms and conditions outlined in our G-Cloud framework agreement.

11. About SPG Intelligence

SPG helps organisations by building technology-enabled solutions based not only on today's ubiquitous platforms but also through established strategic partnerships with innovative vendors and technology providers. Our consultancy services span a wide-ranging portfolio, providing clients with a trusted partner to help with end-to-end technology, business enablement, and transformation services.

Our multi-disciplined teams deliver throughout the project lifecycle from design to development, deployment, and end-state management. We bridge the gap between Big-4 strategic consulting and tactical body-shopping, delivering accountable, hands-on transformation for enterprise organisations.

11.1. Our Service Portfolio

Our service portfolio is built on four foundational intelligence layers:

- Data Intelligence: Data shaped for insight, action, and AI, powered by Microsoft Fabric
- Cloud Intelligence: Cloud-native infrastructure, cost control, and optimisation
- Cyber Intelligence: Secure access, real-time threat detection and response
- Software Intelligence: Bespoke software development, delivery, and deployment

11.2. Why Choose SPG?

- Holistic Data Intelligence: Unlike niche firms, we deliver end-to-end solutions integrating data engineering, analytics, and AI
- AI-Enhanced Delivery: We leverage AI internally to accelerate and deepen insights delivery
- Rapid Insights, Lasting Impact: Our Lightning Insights framework delivers value in weeks, not months
- Microsoft Fabric Specialisation: Deep expertise in Microsoft's comprehensive data stack
- Sector Expertise: Proven experience in NHS, Higher Education, Blue-light, Central and Local Government

11.3. Certifications & Partnerships

SPG maintains the following certifications and partnerships that underpin our service delivery:

- ISO 9001:2015 Quality Management
- ISO/IEC 27001:2022 Information Security Management
- Microsoft Partner
- AWS Partner Network
- HM Government G-Cloud Supplier
- PRINCE2, ITIL, Scaled Agile, and TOGAF methodologies

11.4. Contact Us

Newcastle Headquarters
Platinum Suite 15, Spire, Pilgrim Street, Newcastle Upon Tyne, NE1 2DS

Leeds Office
Orega 3rd floor, St. Paul's House, 23 Park Square, Leeds LS1 2ND

Website: www.spgintelligence.com
Email: info@spgintelligence.com