G-Cloud 14 Framework

Cloud Support

Identity and Access Management

Lightning Insights

SERVICE DEFINITION DOCUMENT

APRIL 2024

Newcastle HQ: The Core, Newcastle Helix, NE4 5TF
Leeds Office: Cubo, 3rd Floor, 6 Wellington Place, Leeds, LS1 4AP

Table of Contents

1. Document Management

1.1. Revision History

Document	Date	Version	Status
Identity and Access Management Service	April 2024	1.0	Approved

1.2. Approval and Sign Off

Role	R	A	C	I
Head of Enterprise Architecture		X		
Enterprise Architecture	X		X	
Solution Architecture			X	X
Technical Design Authority				X
Sales & Marketing Director		X		

2. Overview

Robust identity management is no longer a luxury but a critical necessity for safeguarding corporate environments against unauthorised access and cyber threats.

In the context of rising cyber attacks, a concerning statistic emerged: one-third of all application hacks stemmed 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, while powerful, also presents significant risks. A single misassignment of roles can lead to a hazardous mix, where an individual might possess the ability to both generate and approve critical transactions, such as creating and paying invoices.

This scenario underscores the critical importance of implementing robust internal controls. Without these controls, enterprises not only expose themselves to operational risks but also legal and regulatory repercussions. Furthermore, inadequate oversight and the lack of prompt corrective action in the face of lax controls can lead to whistleblower lawsuits, compounding the financial and reputational damages for companies.

It is therefore imperative for organisations to meticulously manage access rights within their applications, ensuring that no individual has the unchecked authority that could lead to both intentional abuses and inadvertent breaches of protocol. This approach not only aligns with best practices in cybersecurity but also fortifies the company's compliance posture in the face of evolving regulatory landscapes.

The Problem? Ambiguous Identity and Access Management

In many organisations, particularly those with developing identity programs, identity management may involve a patchwork of disparate technologies. These often include Identity Governance and Administration (IGA), Privileged Access Management (PAM), Governance, Risk and Compliance (GRC) tools, third-party management, and IT Service Management (ITSM) tools. This non-converged approach is characterised by several complexities:

- **Multiple Integrations**: Organisations must establish and maintain numerous integrations with downstream applications and endpoints. Additionally, these different identity technologies themselves require interconnections that must be constantly managed.
- **Multiple Platforms for Users**: End users, auditors, and application owners must navigate and be familiar with multiple solutions, complicating training and day-to-day operations.
- **High Maintenance Requirements**: Each solution in a non-converged stack requires its own deployment, ongoing maintenance, and a team of knowledgeable administrators, increasing operational demands.
- **Higher Total Cost of Ownership (TCO)**: The financial burden of multiple systems, including acquisition, integration, and maintenance costs, contributes to a significantly higher TCO.

- **Scalability Challenges**: As business needs evolve, scaling a non-converged identity stack can be cumbersome and inefficient, often requiring additional integration or replacement of systems.

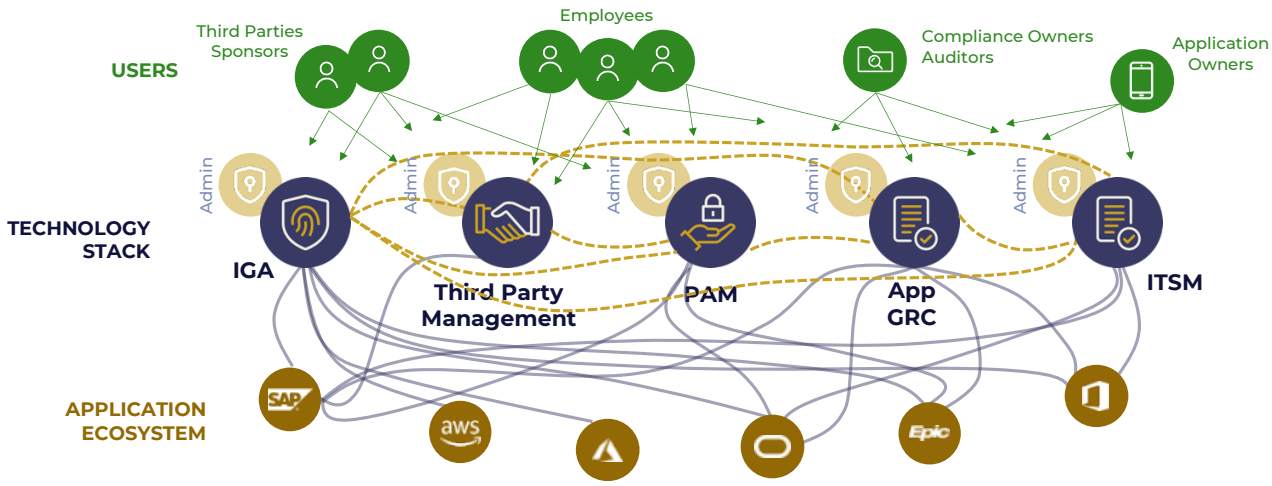

Figure 1 - The Complexity Challenge

Reducing the Time to Value With "SPG Lightning Insights"

SPG provides a structured suite of identity acceleration packages – called Identity Lightning Insights - designed to offer an increase in identity maturity at a compelling price. These packages are crafted around common business problems using best practice designs, ensuring efficient and effective solutions tailored for various business needs.

SPG Identity Lightning Insights are designed to quickly launch initial Phase 1 projects such as IGA (Identity Governance and Administration) and CPAM (Cloud Privileged Access Management), establishing a strong foundation that facilitates future solution expansion.

Packages include:

- **IGA Quick Start**: Automates identity lifecycle events and provisions for key enterprise applications to enable access requests and certifications.
- **Compliance & Audit**: Facilitates compliance controls to govern user access to key enterprise apps.
- **App Access Governance**: Provides visibility into toxic combinations in business-critical applications and prevents Separation of Duty conflicts by proactively applying mitigating controls.
- **CPAM for Cloud Assets**: Secures cloud-based assets, focusing on AWS or Azure accounts.
- **CPAM for On-Prem Assets**: Secures on-prem workloads with options for vaulting passwords.

- **3rd Party Access Governance**: Establishes a governance framework for vendors and third-party workforce.

In addition to technology-enabled IAM accelerators, SPG also provides an Identity and Access Policy & Design engagement, supporting organisations that wish to establish a Role-Based Access Control (RBAC) framework prior to solution selection or implementation.

This service enables clients - such as national bodies, healthcare providers and government departments - to define, document and validate an enterprise-wide access control model covering both systems and data platforms. The engagement delivers the analysis, policy creation and governance framework required to standardise how access is authorised, audited, and maintained across a complex organisation or multi-agency environment.

Typical outcomes include:

- A national or organisation-wide RBAC model defining how roles, permissions and entitlements are structured.
- An access control policy that specifies how users and systems are authorised to access sensitive data or connected records.
- A catalogue of standardised roles, aligned to business and regulatory requirements (e.g. NHS, GDPR, DSPT).
- A governance and lifecycle model for maintaining policy compliance and reviewing access as organisational roles evolve.

The engagement is vendor-agnostic, ensuring the resulting RBAC model can later be implemented on any Identity Governance or Access Management platform, including Saviynt, Azure AD, SailPoint, ForgeRock or bespoke solutions. It provides the essential groundwork for subsequent deployment phases, ensuring that when technology is introduced, it aligns to an agreed policy, data-access framework, and role catalogue.

Approach to Implementation

Each package follows a structured approach ensuring that the deployment aligns with predefined best practices and is tailored to address specific business problems. These are not bespoke projects but are standardised solutions that require minimal customisation, allowing for faster implementation and integration.

SPG offers these Lightning Insights packages while maintaining a consistent and high-quality implementation standard. This service model not only accelerates the deployment process but also reduces the total cost of ownership and enhances the scalability of the solutions provided.

3. Features and Benefits

Feature	Benefit
RBAC Model Design and Role Definition	Establishes a unified role hierarchy across departments or agencies. SPG defines national or enterprise roles, mapping responsibilities to data entitlements and system permissions.
Access Control Policy Authoring	Develops clear, auditable policies describing who can access what data, under what conditions, and through which identity systems, ensuring consistent authorisation across the organisation.
Data Authorisation Framework	Creates a structured model that links data classifications to roles and entitlements, ensuring access is proportionate, justified, and compliant with data-protection requirements.
Federated Identity Governance	Defines how access control operates across multiple establishments, supporting national-level consistency while allowing for local policy variation.
Connected Records Governance	Designs policy controls for linked or shared data records across the data ecosystem through defined role permissions.
Role Mining and Rationalisation	Analyses existing access rights to eliminate duplication and excessive privilege, producing a rationalised and easily governed role catalogue.
Policy Governance Framework	Defines ownership, change control and audit processes to manage ongoing RBAC policy updates, ensuring continuous compliance and accountability.
Technology-Agnostic Blueprint	Delivers a future-ready framework that can be implemented across any chosen identity or access management platform without dependency on a specific vendor.

4. Pricing

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

5. Terms & Conditions

Please see our separate Terms and Conditions document for this service.

6. About SPG

SPG helps by building technology enabled solutions for your business based not only on today's ubiquitous platforms but also through established strategic partnerships with a number of innovative and unique vendors and organisations. 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. Performance is our differentiator.