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 Lightning Insights 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. SPG, committed to upholding the highest standards of security and compliance, is proud to partner with Saviynt to introduce Saviynt Enterprise Identity Cloud (EIC) as a transformative solution designed to meet these challenges head-on.

In the context of rising cyber threats in 2023, 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? Non-Converged Identity Stacks

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.

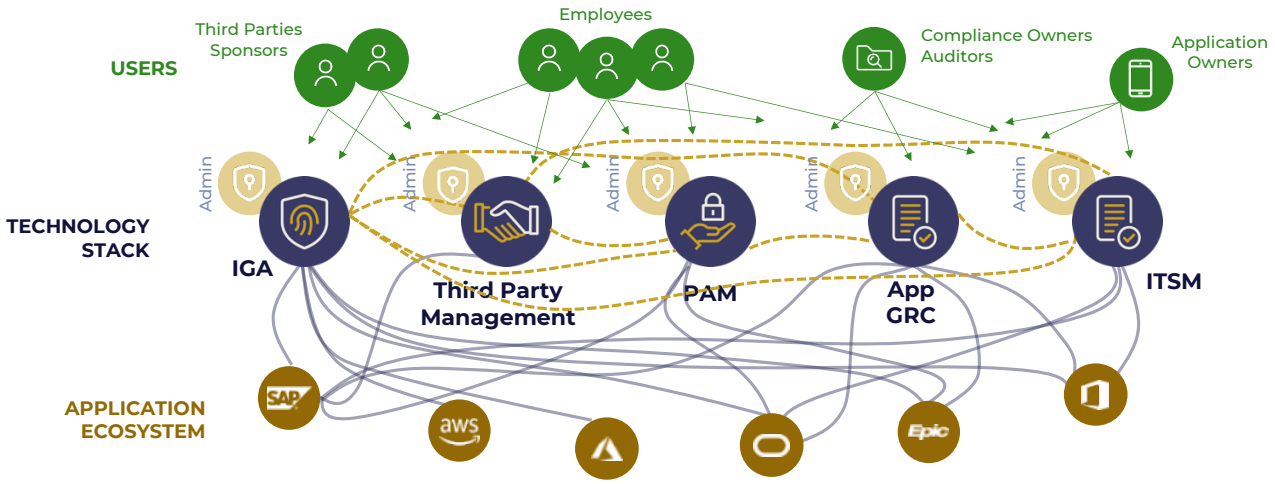

Figure 1 - The Complexity Challenge

Why Saviynt EIC?

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 (IAM) processes, Saviynt EIC enables organisations to focus on core business objectives, knowing their security posture is robust and resilient.

SPG will deliver Saviynt EIC to provide the following advantages.

Enhanced Security Posture: With Saviynt EIC, 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. This out-of-the-box compliance ensures that SPG clients remain ahead of compliance obligations effortlessly.

Operational Efficiency: By automating critical IAM functions such as provisioning, certification, and compliance management, Saviynt EIC reduces manual overhead and operational costs. This automation allows for rapid 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 the specific needs of SPG clients. Its scalability ensures that as SPG clients grow, their identity management capabilities can expand seamlessly without compromising security or performance.

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 fixed-price and fixed duration. 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.

Advantages:

- Rapid deployment and operational efficiency
- Streamlined integration with key enterprise applications
- Enhanced security and compliance adherence
- Fixed-cost model ensures predictable budgeting

Follow-on Accelerator Packages

A variety of complimenting "follow-on" packages are available to move maturity quickly to the next level. Designed to take place following a live Saviynt IGA implementation, these packages facilitate the quick launch of additional Saviynt modules, enhancing the existing identity solutions and supporting continuous improvement.

Key Features:

- **AAG Follow-on**: Builds on existing IGA solutions to prevent toxic combinations and reduce internal fraud.
- **TPAG Follow-on**: Enhances governance of third-party identities through centralized access policies.
- **CPAM Follow-on**: Expands visibility into high-risk assets for both cloud and on-prem workloads.

Advantages:

- Flexibility to add modules like building blocks
- Enhances existing IGA implementations without complete overhaul
- Focused on increasing security and governance over expanded areas of the business

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

a. Out-of-the-Box Rulesets

- 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 the need for extensive customization.

b. Fine-Grained SoD (Separation of Duties) Controls

- 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: Minimizes 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.

c. 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.

d. Seamless Risk Reporting

- Feature: Provides comprehensive risk assessment capabilities that aggregate and visualize 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.

e. Out-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 SOX, GDPR, HIPAA, and more.

- 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.

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.

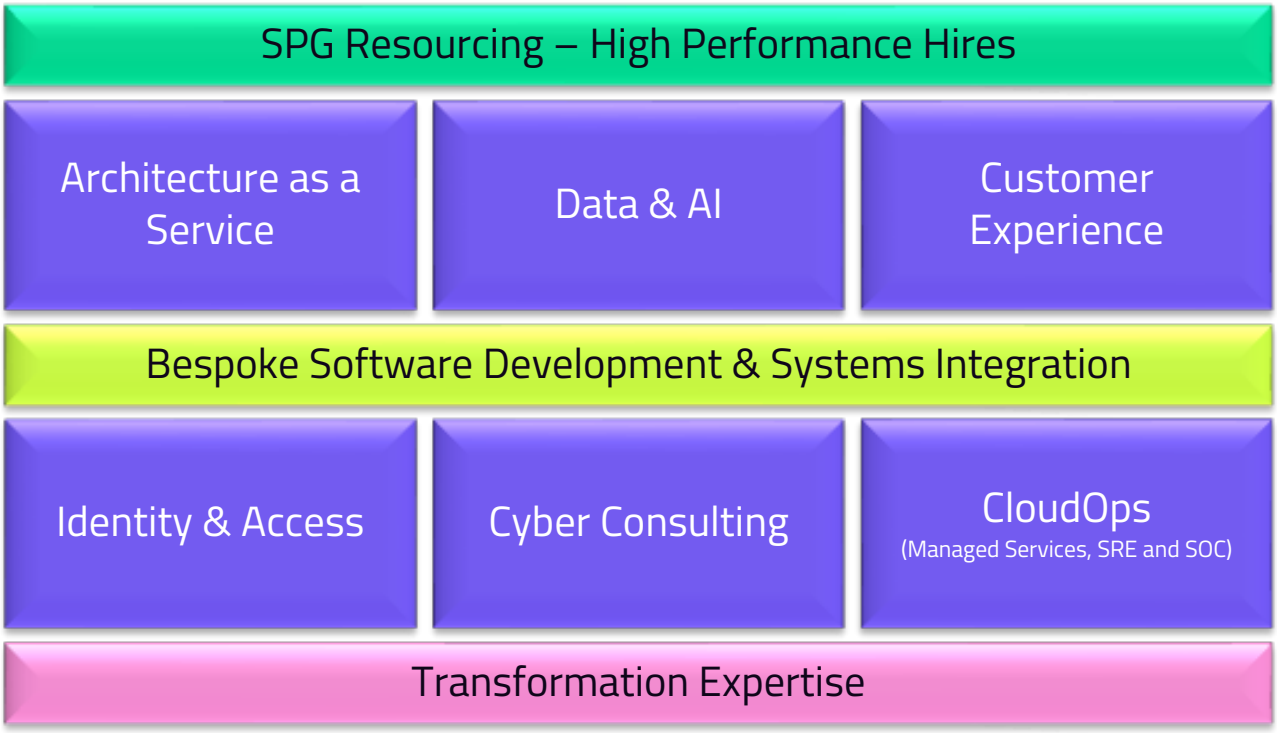

Figure 2- The SPG Ecosystem

At the top of our ecosystem sits **SPG Resourcing**, a cornerstone subsidiary of our Group companies focused on the acquisition and mobilisation of top-tier talent. The individuals acquired through this channel are critical, as they carry the expertise and innovative drive needed to manage and implement all other technological services with a high degree of efficacy, both for SPG internally, and for our clients.

Adjacent to this is our **Architecture as a Service**, which offers clients adaptable and scalable technology architecture solutions, tailor-made to accommodate evolving business demands. This service provides the essential underpinnings for all technological functions, ensuring that foundational structures support future innovations and integrations within the organisation.

Data & AI, a pivotal block within the framework, leverages cutting-edge analytics, machine learning, and comprehensive data processing to distil actionable insights and propel business intelligence forward. This component is instrumental in sharpening decision-making processes,

optimising operational efficiencies, and personalising customer interactions – all while harnessing the latest developments in Artificial Intelligence.

Equally crucial is the **Customer Experience** module, which concentrates on sculpting and refining the customer journey across various interaction points. By harnessing technology to enrich customer engagements, this segment works to elevate satisfaction, foster loyalty, and customise the user experience.

Central to the framework is **Bespoke Software Development & Systems Integration**. This involves crafting custom software solutions that are specifically designed to meet the unique requirements of the business, coupled with the integration of disparate systems and technologies to ensure cohesive operation across diverse platforms and environments – a key part of any technology enabled transformation.

Our **Identity & Access** management function safeguards user identities and governs access to critical resources throughout the organisation. This capability is vital for maintaining robust security protocols and adherence to regulatory compliance, employing Identity Governance and Administration (IGA), Cloud Privileged Access Management (CPAM) and Goverenance, Risk and Controls (GRC) tools to secure and streamline access control.

Cyber Consulting offers specialised guidance on securing digital assets, safeguarding network infrastructures, and maintaining compliance with stringent cybersecurity standards. This expertise is essential for identifying potential vulnerabilities, deploying defensive measures, and managing ongoing security operations effectively.

CloudOps includes 24x7 managed services, site reliability engineering (SRE), and security operations centre (SOC) functions, focusing on the management, optimisation, and security monitoring of cloud-based resources. This ensures that cloud infrastructures are not only performant but also resilient and secure under various operational demands.

Lastly but not least, our **Transformation Expertise** embodies the capacity to drive and implement profound change across both technological and business environments. This block capitalises on digital innovations to revolutionise business operations, enhance efficiencies, and forge new value propositions, ensuring the organisation remains at the cutting edge of technological advancement.

ISO 9001:2015
RH10230Q88

ISO/IEC 27001:2013
RH10230I88