Reliance HIGH-TECH

HM Government G-Cloud

Serious about technology, passionate about people

G-Cloud 15

Service Definition Document

Genesys by ISM CAPSS and NPSA approved PSIM *provided by Reliance*

Protecting your people, assets and reputation

www.reliancehightech.co.uk

Version: 1

Contents

VERSION CONTROL

Date	Version	Changes
26/1/26	1	G-Cloud 15 submission

RELIANCE HIGH-TECH CONTACT

James Smith

Sales and Marketing Director

E: james.smith@reliancehightech.co.uk

T: 0845 121 0802

1.0 About Reliance

Reliance is an independent UK security systems integrator, trusted by organisations operating in high-compliance, high-risk and mission-critical environments - where quality cannot be compromised. With decades of experience, we deliver high-performing, IT-aligned security solutions that reduce risk, strengthen resilience and provide long-term value.

For clients, this means more than system uptime. It means creating safer, better-managed environments through reliable core security, clear operational visibility and, where appropriate, analytics and alerting that help teams identify issues earlier and respond with confidence. By improving situational awareness and reducing avoidable incidents, we help organisations protect people, assets and reputations - while enabling day-to-day operations to run smoothly.

Quality, reliability and integrity sit at the heart of how we design, deliver and support every solution.

1.1 Partnership Ethos and Customer-Centric Delivery

Our mission is to protect people, assets, and reputations - but how we do it is just as important. We believe great partnerships are built on trust, shared goals, and strong personal relationships. That's why we take the time to understand what matters most to you - not just in terms of technical requirements, but the wider priorities, pressures, and aspirations that shape your environment. This approach allows us to deliver solutions that are truly aligned with your objectives. We also invest heavily in our own people - from structured training and mentoring to wellbeing and professional development - ensuring they bring not only expertise, but empathy and care to every engagement. Our clients know us not just for what we deliver, but for how we work - consistently collaborative, dependable, and easy to do business with. We grow with our clients, adapting as their needs evolve and working as an extension of their team.

1.2 A Technology-Led Business with Strategic Depth

While our roots are in security, our capabilities span much further. We are a technology-led business that blends physical security with IT, cloud, analytics, and IoT. This enables us to bring a strategic, joined-up perspective to system design and service delivery, helping clients navigate legacy challenges, embrace cutting-edge platforms, and plan confidently for the future. We work closely

across stakeholder groups - from IT and cyber teams to estates, compliance, and health and safety - taking time to understand their individual needs and turning them into actionable, aligned solutions that deliver meaningful outcomes across the wider organisation.

1.3 From Systems to Outcomes

We deliver more than systems - we deliver outcomes. Through data integration, asset lifecycle management, and remote monitoring, we help clients make smarter decisions, reduce total cost of ownership, and unlock operational efficiencies. Our managed services offering ensures performance is not just achieved, but sustained. These principles of continuous improvement, value creation, and operational excellence are embedded in our culture and backed by rigorous, externally verified standards.

1.4 Commitment to Quality and Assurance

We hold key certifications that reflect the breadth and depth of our commitment to quality, resilience, and cybersecurity - including ISO 27001 (Information Security), ISO 27017 (Cloud Security), ISO 22301 (Business Continuity), and ISO 9001 (Quality Management). We are also certified to Cyber Essentials Plus and are proud to be recognised as being in the top 6% of suppliers to the NHS Data Security and Protection Toolkit, with the rating of “Expectations Exceeded” - an accolade we have held for four consecutive years.

As part of our work with NHS organisations, we are delivering significant volumes of custom development at API and Webhook level - providing tight integration with third-party systems as part of a highly tailored security solution. This is a direct testament to the strength of our in-house development team and our proven ability to deliver secure, scalable, and standards-compliant integrations. Our broader experience spans multiple platforms, and our deep familiarity with Genetec and other enterprise-grade technologies means we can support complex development and testing requirements at an unrivalled level - bringing together security, IT, and application integration in a seamless and robust way.

SSAIB CERTIFICATED UKAS PRODUCT CERTIFICATION 131 Verify at ssaib.org	SSAIB CERTIFICATED UKAS MANAGEMENT SYSTEMS 131 Verify at ssaib.org	CHAS®
ecovadis	JOSCAR REGISTERED	FSQS REGISTERED

1.5 Trusted in High-Governance and High-Compliance Environments

Reliance supports organisations where security, resilience and accountability are non-negotiable. We work across high-governance, highly regulated environments - delivering and maintaining integrated security solutions for complex estates, critical operations and busy public settings. Our experience spans Central Government, CNI and defence-aligned supply chains; energy and utilities (power distribution and generation, water and gas); police and custodial environments; research organisations, governing bodies, large trusts and healthcare; financial and FTSE environments; bio/pharma; data centres and communications; transport and logistics; and higher education, including multi-building campus and university estates.

Across these markets, clients rely on us to operate safely, securely and with minimal disruption - combining strong technical capability with disciplined delivery, clear reporting and a long-term service mindset.

1.6 Organisational Capability and Service Structure

Our c.180-strong team includes expert engineers, project managers, developers, and cybersecurity professionals - backed by robust internal systems, including our centralised Service Management Platform and in-house pre-staging capability. These aren't just people with skills; they are people who care - committed to doing the right thing, taking pride in their work, and delivering consistent quality across every touchpoint. This investment in our people, combined with rigorous internal standards and industry-leading certifications, translates directly into the experience we offer and the outcomes we deliver.

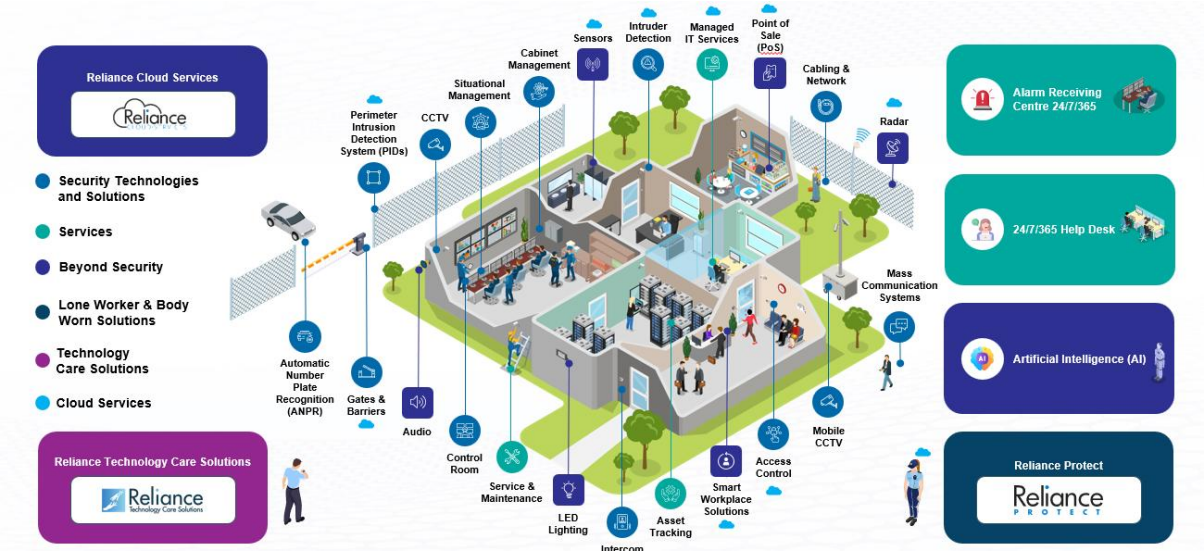
1.7 Serious About Technology. Passionate About People.

Technology is at the core of our approach, but it's the quality of our people that truly sets us apart. All of our engineers are security cleared, and all are trained to operate to the highest technical and ethical standards. We invest heavily in training, development, and wellbeing to ensure our teams not only stay ahead of technology - but consistently deliver with care, professionalism, and integrity. These are people who take pride in what they do and represent our values in every interaction - helping you protect what matters most.

At Reliance, we're Serious about Technology, Passionate about People. That ethos is at the heart of everything we do - driving innovation, building trust, and ensuring that the solutions we deliver truly make a difference.

1.7 Resilient end-to-end solutions

Reliance delivers resilient, end-to-end security solutions that cover the full lifecycle - from design and systems integration through IT enablement, ongoing maintenance, and specialist services such as lone worker protection and monitoring. Clients benefit from one accountable partner who can supply, install, integrate, host, support and continually optimise their solution, ensuring it remains secure, available and fit for purpose as requirements evolve. Whether you need a single capability or a fully integrated estate-wide approach, we bring the people, processes and infrastructure to deliver it reliably at scale.



Systems Integration

- Access Control
- Closed Circuit Television
- Perimeter Security
- Network
- Information Management & Situational Awareness

IT Capability

- In-house Expertise
- Fully Accredited – ISO27001 & Cyber Essentials Plus
- Support for all Security related IT Requirements
- High-availability Hosting and DR Solutions

Maintenance

- 24/7/365 Help Desk
- Nationwide Cover & LSP's in Europe
- Flexible & Tailored Plans
- Advance Call Handling and Tracking Software
- Web-based Service Report Module

Lone Worker Solutions

- ID Cards & Fobs with GPS and Audio
- Body Worn Cameras
- Slip/Trip/Fall and 'Man Down'
- Check-ins and Safety Timers
- Two-way Audio with Trained Operators

Monitoring Services

- Dedicated Monitoring Centre
- 24/7/365 Security & Surveillance
- Systems Monitoring and Remote Diagnostics
- Reliance Protect – Lone Worker Monitoring

2.0 Service Definition

This section describes the proposed solution and the benefits it will realise for G-Cloud 15 Framework users.

2.1 Overview

Reliance offer a number of cloud and hybrid security software solutions backed by tried and tested systems manufacturers. Reliance have extensive experience of designing, installing, maintaining and supporting these solutions across complex, multi-site estates and high-governance environments.

This Service Definition document provides details of **Genesys by ISM** (Genesys), a Physical Security Information Management (PSIM) platform designed to unify alarms, events and operational workflows across multiple security systems. Genesys enables control rooms and security teams to manage incidents consistently, reduce response time, improve situational awareness and strengthen governance through auditability and reporting.

Key characteristics of the Genesys service include:

- Unified alarm and incident management across multiple systems (for example CCTV/VMS, access control, intruder, intercoms and other safety/security sources)
- SOP-driven workflows to guide operators through consistent, policy-aligned responses
- Situational awareness tools such as maps, site plans, zones and linked device context
- Automation and rules (cause-and-effect) to standardise escalation, notifications and tasking
- Role-based user management, permissions and audit logging to support governance and compliance
- Multi-site operations support, enabling central oversight with local operational capability
- Flexible deployment models including on-premise, hybrid and SaaS options (deployment dependent)

2.2 Infrastructure & Architecture

A typical Genesys deployment is based on a central PSIM platform that integrates with the buyer's existing security systems and presents a single operational view to authorised users.

Core architectural elements include:

- Genesys platform services - the PSIM application layer hosting workflows, rules, user access, audit and reporting. This is deployed in line with the chosen model (on-premise, hosted or hybrid).
- Integration layer - connectivity to supported third-party systems using approved integration drivers/connectors, allowing Genesys to ingest alarms/events and link to associated devices and actions.
- Data services - a database layer to support state management, incident records, audit trails and reporting (architecture dependent on deployment).
- Operator clients - authorised operator workstations and/or web clients used within the control room environment to manage alarms, run SOPs, view maps and launch linked system functions.

- Secure network connectivity - controlled connectivity between Genesys and integrated systems within the buyer environment. Where remote or multi-site connectivity is required, this is implemented using secure channels aligned to buyer security policies.
- Resilience - resilience can be designed to meet operational requirements (for example redundancy of core services and data services). Where connectivity between sites is interrupted, local systems continue operating, and Genesys visibility is restored when connectivity returns (architecture dependent).

2.3 Technical Solution

The following section details the platform, its key components, functionality, features and benefits.

2.3.1 Unified Alarm and Incident Management

Genesys provides a unified operational view of alarms and events across connected systems. Operators can receive, prioritise, acknowledge, escalate and close incidents within a single interface. This supports faster decision-making, reduces manual handoffs, and improves control room efficiency - particularly across estates where multiple systems and standards exist.

2.3.2 SOP-Driven Operator Workflows

Genesys enables SOP-led incident handling so responses are consistent and aligned to your policies. Typical capabilities include:

- Step-by-step operator prompts and checklists
- Dynamic workflows based on event type, location, time or risk level
- Controlled escalation paths and call-out rules
- Structured incident notes and evidence capture
  This approach reduces operator variability, supports training and improves defensibility in post-incident review.

2.3.3 Situational Awareness - Maps, Site Plans and Context

Genesys supports situational awareness by presenting incidents with relevant context. This can include:

- Geospatial views, site plans and zoning
- Linked assets and device relationships (for example cameras, doors, intercom points, intrusion zones)
- Quick navigation to the right location and associated devices
  This helps operators move from alarm to understanding quickly, particularly on large, complex or multi-site estates.

2.3.4 Automation, Rules and Cause-and-Effect

Genesys supports configurable rules (cause-and-effect) to automate repeatable actions and reduce response time. Examples include:

- Automatically notifying defined roles/teams for specific event types
- Triggering defined tasks or escalation steps after timers expire

- Driving consistent workflows across sites and shifts
  Automation is configured to match the buyer operating model and governance requirements, with appropriate controls and audit.

2.3.5 Integrations and Extensibility

Genesys can be deployed as part of a wider security and operational ecosystem. Integration options may include supported CCTV/VMS platforms, access control, intruder detection, intercoms and other safety/security systems, enabling customers to align incident handling with wider processes, reporting requirements and estate-wide operating standards. Where appropriate, integration can also support structured data exchange with other tools used by the buyer (deployment and scope dependent).

2.3.6 Cybersecurity

Genesys deployments are designed to support secure operation, aligned to common best practice for security management platforms. Controls typically include:

- Encrypted communications where applicable between platform components and connected services
- Role-based access control to restrict functions and data access
- Support for multi-factor authentication options (deployment dependent)
- Comprehensive audit logging to support accountability and investigations
- A security-led approach to updates and patching, delivered under agreed change control
  Deployment is designed in collaboration with the buyer's IT/security teams to align with their policies for network segmentation, identity management, endpoint protection and monitoring.

2.3.7 Reporting, Audit and Governance

Genesys supports governance and continuous improvement through reporting and auditability. This can include incident histories, operator actions, response performance metrics, and configurable dashboards/reports to support operational oversight, management review and compliance requirements.

2.3.8 Scalability and Service Continuity

Genesys is well suited to growth and change across an estate. Additional sites, systems and workflows can be onboarded in a controlled manner, with central configuration supporting consistent operating standards as deployments scale. Service continuity is supported through resilient design and the ability to restore central visibility following connectivity interruptions, while local security systems continue operating independently (architecture dependent).

2.4 Pricing Structure

Current guide pricing has been provided in the separate Pricing Schedule provided. However, please contact Reliance to discuss your specific requirements and to obtain specific pricing.