



HM Government
G-Cloud

G-Cloud 15

Service Definition Document

Suprema Biostar Air - Cloud-based Access Control Solution ***provided by Reliance***

*Serious about
technology,
passionate
about people*

Contents

1.0	About Reliance.....	3
1.1	Partnership Ethos and Customer-Centric Delivery	3
1.2	A Technology-Led Business with Strategic Depth.....	3
1.3	From Systems to Outcomes	4
1.4	Commitment to Quality and Assurance.....	4
1.5	Trusted in High-Governance and High-Compliance Environments	5
1.6	Organisational Capability and Service Structure	5
1.7	Serious About Technology. Passionate About People.	5
1.7	Resilient end-to-end solutions	6
2.0	Service Definition	7
2.1	Overview	7
2.2	Infrastructure and Architecture	7
2.3	Technical Solution	7
2.3.1	Configuration and Customisation	8
2.3.2	Integrations and API.....	8
2.3.3	Data Ownership, Export and Offboarding.....	8
2.3.4	Metrics and Service Oversight	8
2.4	Pricing Structure.....	8

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.

 Verify at ssaib.org	 Verify at ssaib.org	
		

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.

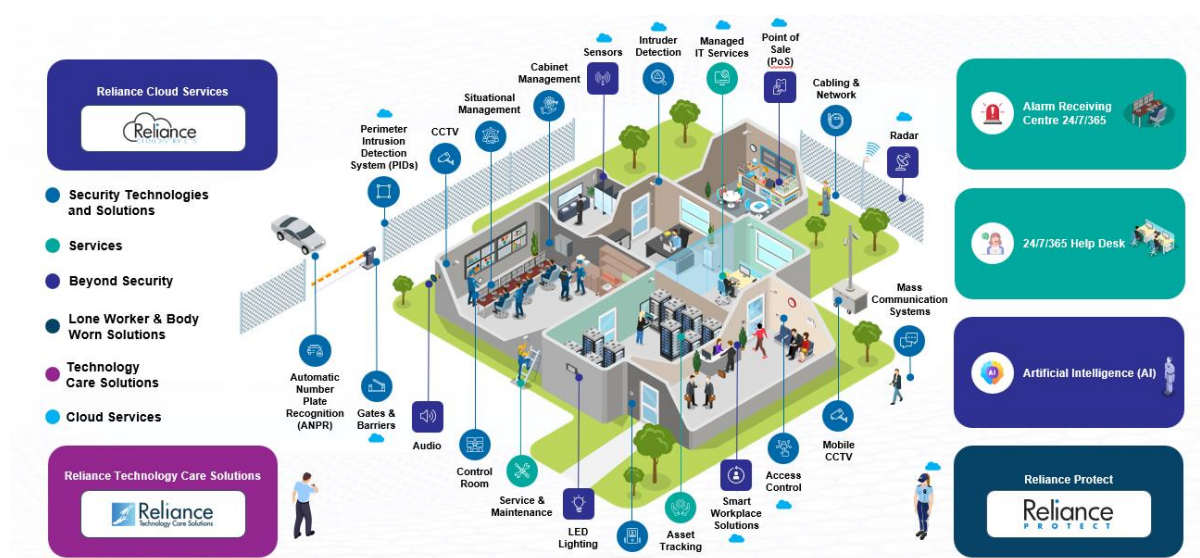
Technology is at the core of our approach, but it's the quality of our people that truly sets us apart. All of our engineers are security cleared, and all are trained to operate to the highest technical and ethical standards. We invest heavily in training, development, and wellbeing to ensure our teams 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

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

Monitoring Services

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

IT Capability

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

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

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 CCTV as a Service” solutions backed by tried and tested systems software manufacturers. Reliance have extensive experience of designing, installing, maintaining and supporting these systems with multiple clients.

The service definition is for **BioStar Air**, Suprema’s cloud-native access control platform, designed to remove the need for on-site servers and simplify multi-site administration through a single cloud portal. It supports biometric and mobile credentials, centralised user and door management, real-time monitoring and reporting, and optional entry-centric video integration to support operational oversight.

2.2 Infrastructure and Architecture

BioStar Air is delivered as SaaS and accessed via a secure web portal and mobile applications. It uses an edge architecture in which compatible smart readers connect directly to the cloud, reducing local infrastructure requirements (no separate controller layer, and no on-prem server for the access control application).

A typical deployment includes:

- Cloud management portal for sites, doors, users, permissions, schedules, alerts and reporting
- Network-connected smart readers/terminals with built-in control functions and direct cloud connectivity
- Mobile credential options, including the Suprema Pass app and app-free LinkPass credentials (use-case dependent)
- Optional ONVIF CCTV integration for live/entry-centric video association with access events
- Cloud APIs to support integration and automation

All components are designed to operate under controlled access and auditability appropriate for access control governance.

2.3 Technical Solution

The service provides structured workflows and controls to support secure access management across one or multiple sites.

Key capabilities include:

- Centralised management of users, doors, sites, schedules, permissions and event monitoring
- Support for biometric authentication using compatible Suprema devices (deployment dependent)
- Mobile credentials, including Suprema Pass (digital wallet) and LinkPass (app-free credentials via secure link)
- Real-time alerts and reporting to support operational oversight
- Basic time and attendance reporting (hours on site) based on event logs, with export/integration options
- Optional CCTV visibility via ONVIF camera support, aligned to entry-point monitoring

- Security controls for credential handling, including AES-256 protection for mobile credential data (as described in Suprema's BioStar Air security overview)

2.3.1 Configuration and Customisation

The solution can be configured to align with the buyer's operational workflows and governance requirements, including:

- Roles, permissions, organisational structure (sites/doors/groups) and access policies
- Schedules, access levels, door rules and alerting thresholds
- Credential policies (biometric, mobile, QR/LinkPass) aligned to use-case and risk profile
- Reporting views (including basic time and attendance outputs where used)

Administrative configuration is completed through the management interface under role-based controls.

2.3.2 Integrations and API

BioStar Air supports integration using cloud APIs to connect with buyer operational systems and automate workflows. Typical capabilities include:

- Creating and updating users, credentials and access permissions
- Retrieving events and status information for operational oversight
- Supporting automation via integration patterns (for example event-driven workflows)
- Enabling controlled data exchange for reporting and downstream processes

API access is protected through authenticated, authorised access and governed through configured permissions.

2.3.3 Data Ownership, Export and Offboarding

Data stored in the service is owned by the buyer organisation. Export and administrative actions are controlled through permissions and logged to support auditability. The service supports export of relevant records and reports required for governance and downstream processes (scope aligned to configuration). Bulk extraction can be supported as part of end-of-contract offboarding to ensure an orderly handover.

2.3.4 Metrics and Service Oversight

Operational and governance metrics are available via the management portal and can be exported for reporting. Typical metrics include access events, alarms/alerts, user activity, door status, reporting outputs, and (where enabled) basic time and attendance reporting and entry-centric video association status.

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.