



HM Government
G-Cloud

G-Cloud 15

Service Definition Document

Brivo 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 & Architecture	7
2.3	Technical Solution	7
2.3.1	Unified Access Control Management	7
2.3.2	Centralised Administration and Configuration	8
2.3.3	Credentials and User Experience	8
2.3.4	Reporting, Audit and Governance.....	8
2.3.5	Integrations and Extensibility	8
2.3.6	Cybersecurity	8
2.3.7	Scalability and Service Continuity	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.

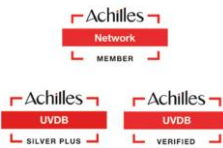
1.3 From Systems to Outcomes

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.

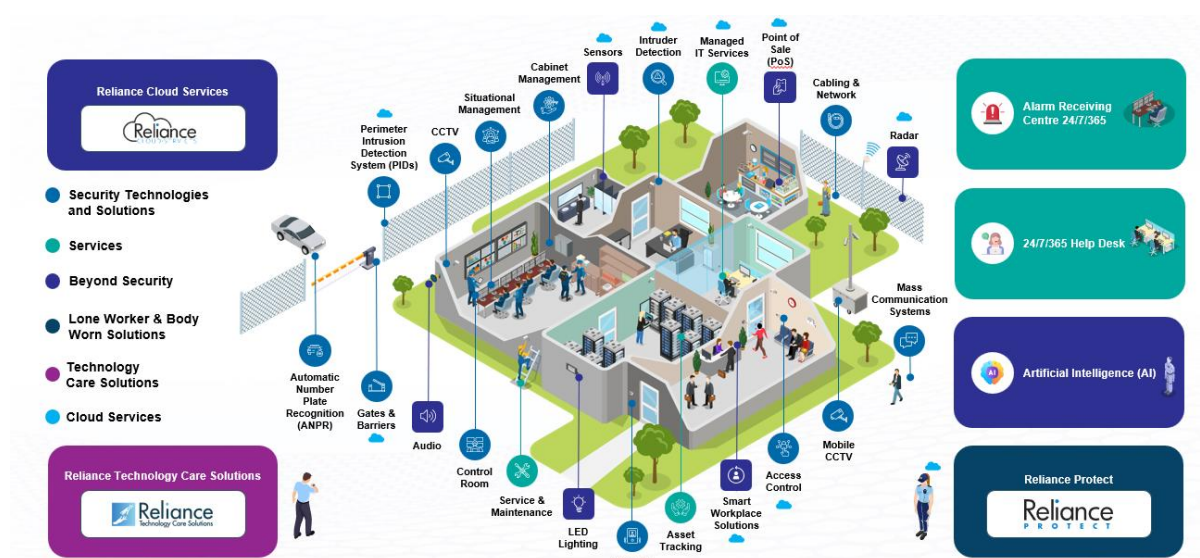
Technology is at the core of our approach, but it's the quality of our people that truly sets us apart. All of our engineers are security cleared, and all are trained to operate to the highest technical and ethical standards. We invest heavily in training, development, and wellbeing to ensure our teams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

This Service Definition document provides details of **Brivo**, a cloud-based access control platform designed to simplify how organisations manage doors, users and permissions. Brivo provides secure, centralised administration through a web portal, with on-site controllers/panels and door hardware delivering access control at the edge.

Key characteristics of the Brivo service include:

- Cloud-based administration and user access via a secure web portal
- Centralised management of doors, schedules, access groups, users and credentials
- Support for mobile credentials as well as traditional cards/fobs (deployment dependent)
- Multi-site visibility and control to support distributed estates and shared operations teams
- Reporting and audit trails to support governance, investigations and compliance
- Integrations and extensibility via supported connectors and APIs (scope dependent)
- Simplified lifecycle management through cloud-delivered updates and remote configuration

2.2 Infrastructure & Architecture

A typical Brivo deployment combines on-site access control hardware with the Brivo cloud service.

- Core architectural elements include:
 - Door hardware: readers, locks, request-to-exit devices and door contacts, installed on site.
 - Controllers/panels: on-site control hardware that connects to door hardware and the local network.
 - Secure cloud connectivity: controllers communicate with the Brivo cloud service using secure, outbound connectivity (architecture dependent).
 - Client access: authorised users manage the system through the Brivo web portal, subject to role-based permissions.
 - Identity and user data: users and credentials are administered centrally; integration with identity systems can be implemented where required (scope dependent).
 - Resilience: access control can be designed to maintain local operation if internet connectivity is interrupted, using controller capabilities and configuration appropriate to the environment (hardware and configuration dependent).

2.3 Technical Solution

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

2.3.1 Unified Access Control Management

Brivo provides a unified operational view of access control, enabling users to manage doors, permissions and schedules across an estate from one interface. This reduces fragmented administration and supports consistent standards across sites.

2.3.2 Centralised Administration and Configuration

Brivo supports central administration to standardise configuration across sites. Typical capabilities include:

- User and role management with granular permissions
- Central configuration of doors, schedules and access groups
- Rapid updates to permissions and time profiles without site visits
- Central visibility of activity and exceptions through event tracking and audit history

2.3.3 Credentials and User Experience

Brivo supports modern credential options to improve usability and reduce operational overhead. This can include mobile credentials and/or physical cards/fobs (deployment dependent), with controlled enrolment, credential lifecycle management and role-based assignment.

2.3.4 Reporting, Audit and Governance

Brivo supports governance through event logs and reporting. Administrators can generate and export reports to support operational oversight, investigations, compliance and internal assurance.

2.3.5 Integrations and Extensibility

Brivo can be deployed as part of a wider security and IT ecosystem. Integration options may include identity platforms, HR systems, visitor workflows, video platforms and other operational systems. Where appropriate, APIs can be used to automate provisioning, event export and cross-platform workflows (scope dependent).

2.3.6 Cybersecurity

Brivo is designed to support secure operation and buyer governance requirements. Typical controls include:

- Role-based access control and strong user permissioning
- Audit logging for accountability and investigations
- Secure communications between on-site components and cloud services (architecture dependent)
- Recognised security assurance and compliance standards, including SOC 2 Type II and ISO/IEC 27001 certification (evidence available on request)

2.3.7 Scalability and Service Continuity

Brivo is well suited to growth and change across an estate. Doors, sites and users can be added in a controlled manner, while central administration supports consistent standards as deployments scale. Local access control capability can be maintained during connectivity interruptions, subject to controller capability and agreed design (hardware and configuration 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.