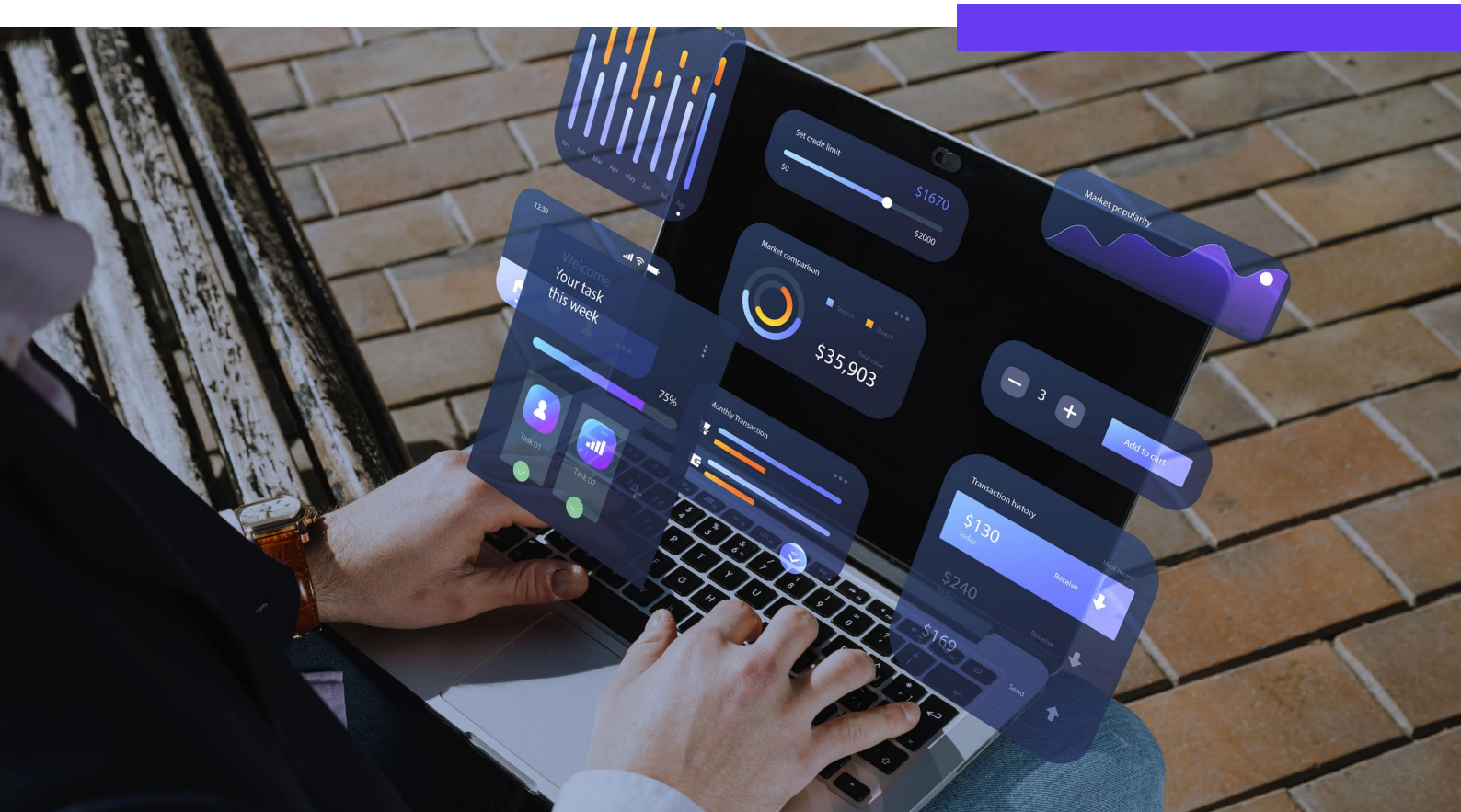
3ROC.
TECHNOLOGY

Service Definition Document

3ROC Ltd.

Table of Contents



Service Offering

Overview

3ROC Ltd provides specialist network, cloud, and infrastructure support services to public sector organisations operating in highly regulated environments. We deliver secure, resilient, and well-governed solutions across network refresh, cloud transformation, and legacy modernisation programmes, using a low-risk, security-led delivery approach.

3ROC Ltd is currently delivering a secure network infrastructure replacement programme involving the planned removal of legacy infrastructure and deployment of a modern enterprise network.

Our scope includes enterprise networking across multiple business departments, structured network cabling upgrades, deployment of fibre connectivity across secure zones, and implementation of enhanced network security services and tooling. This includes network segmentation, access control, traffic management, monitoring, and secure service delivery using industry-standard security platforms such as F5 Networks. Services are delivered under formal design authority, change control, and assurance processes.

We also provide cloud support services across Microsoft Azure and Amazon Web Services (AWS), including hybrid environments. Services include exiting legacy data centres, migrating and stabilising workloads, improving security and resilience, optimising cost and performance, and building internal capability through structured knowledge transfer.

3ROC Ltd's delivery model is built around senior engineers and enterprise architects drawn from Tier 1 providers and major public sector programmes. Many consultants are SC-cleared or SC-clearable, enabling delivery into sensitive environments with strong governance, specialist resourcing, and regulatory assurance.

What Our Service Includes

3ROC Ltd's cloud support service is modular, allowing buyers to procure discrete work packages (for example, migration planning, security uplift, performance testing, or operational support) or combine them into an end-to-end engagement.

Common service components include:

Service Component	What 3ROC Ltd Delivers in Practice
Managed Cloud Support	Monitoring and alerting, incident and request management, triage and escalation, runbooks, service reporting, continual improvement, and integration with network and security operations. Out-of-hours support can be provided where agreed.
Cloud Financial Management (FinOps /cost optimisation)	Spend analysis, cost allocation and tagging approaches, waste reduction and rightsizing, forecasting, reporting, and optimisation recommendations, including cost impacts of network connectivity and security services.
Cloud Migration Planning	Readiness and gap assessment, options analysis, risk and dependency mapping (including network and security dependencies), migration roadmaps with staged waves, and governance checkpoints.
Set Up and Migration Delivery	Target environment build and configuration, secure network connectivity setup, migration runbooks and cutover planning, pilot and phased migrations, validation, hypercare, and handover.
Security Services	Security architecture and risk assessment, network security design, logging and monitoring controls, vulnerability assessment, penetration testing support, incident response readiness, and audit evidence aligned to public sector requirements.
Network and Connectivity Services	Enterprise network design and implementation, secure connectivity between business departments, network segmentation, access control, routing and switching configuration, fibre and structured cabling coordination, and integration with cloud networking services.
Quality Assurance and Performance Testing	Test planning, performance and soak testing across applications and networks, operational readiness testing, resilience validation, and evidence packs for assurance and governance.
Training and Knowledge Transfer	Role-based training and practical handover covering cloud, networking, and security services; troubleshooting guidance; runbooks and documentation; and train-the-trainer sessions.
Ongoing Support	Operational support and optimisation across cloud, network, and security services; incident and problem management; reporting; and knowledge base maintenance.

Public Sector Delivery Approach

3ROC Ltd delivers cloud support services in a way that is suited to government and regulated environments: structured, evidence-led, security-aware, and outcome-driven. We place early emphasis on strategy, operating model, network architecture, and security design, before executing delivery against an agreed and governed plan.

Throughout an engagement, we maintain a comprehensive and auditable set of delivery artefacts, including:

Decision logs and design authority records.	Architecture and network options analysis.	Security risk assessments and risk registers.
Network, security, and performance testing evidence.	Implementation, migration, and cutover runbooks.	Operational readiness, security acceptance, and service transition checklists.

This approach supports accountable governance and provides stakeholders with confidence that network, security, and cloud decisions are based on validated technical and risk information. 3ROC Ltd supports organisations through discovery, design assurance, and readiness activities, aligning outputs to established service management, enterprise architecture, security, accessibility, and operational good practice.

Delivery Strength: People, Capability, and Assurance

3ROC Ltd services are delivered by senior practitioners with direct responsibility for complex, business-critical environments.

Our capability is underpinned by:

- Deep engineering expertise across Amazon Web Services (AWS), Microsoft Azure, enterprise networking, routing and switching, secure connectivity, storage, databases, backup, and cloud security.
- Network security capability including segmentation, access control, traffic inspection, load balancing, monitoring, and zero trust architecture, using industry-standard tooling such as F5 Networks.
- Legacy modernisation expertise across AIX, Solaris, HP-UX, and legacy x86, with proven rehost and replatform approaches where direct modernisation is not feasible
- Repeatable migration and network transition patterns developed through prior data centre exit, infrastructure refresh, and transformation programmes.
- Security-aware delivery, with SC-cleared or SC-clearable resources available subject to client requirements.

Service Scope and Service Options

Scope of Service

3ROC Ltd delivers modular cloud and network support services that help organisations plan, transition, stabilise, secure, and operate cloud-hosted and hybrid services. This includes cloud platforms, on-premise infrastructure, and the networks and security controls that connect and protect them.

Clients may procure:

- A single defined outcome (such as a network security assessment, cloud migration plan, connectivity design, performance testing, or training package), or;
- An end-to-end engagement covering mobilisation, network and cloud build, migration execution, assurance, operational readiness, and ongoing support.

The service supports environments hosted on AWS and Microsoft Azure, including hybrid scenarios combining cloud and on-premise platforms. 3ROC Ltd also supports data centre exit, network refresh, and legacy transformation programmes, including workloads running on AIX, Solaris, HP-UX, and legacy x86 systems.

Service Options Available

The options below can be delivered independently or combined into a single engagement. Each option is delivered using an agreed statement of work that defines scope, deliverables, roles, timelines, governance, and acceptance criteria.

Cloud Migration Planning and Readiness

For clients needing a clear, evidence-led plan before committing to execution. Outputs include:

- Assessment and planning workshops with technical and service stakeholders.
- Workload and dependency assessment (applications, data, integrations, identity, networking, operational processes).
- Target state architecture options (including constraints and trade-offs).
- Migration strategy and wave plan (pilot → scaled migration approach).
- Risk, assumption, issue and dependency management (RAID).
- Operational readiness requirements (monitoring, backup/restore, DR approach, support model).
- An implementation roadmap with indicative sequencing and governance checkpoints.

Cloud Set-up and Migration Delivery

For clients ready to implement, needing controlled cutover and validation. Outputs include:

- Cloud environment set-up aligned to buyer needs (identity, access controls, networking, logging, monitoring, and backup patterns).
- Migration runbooks and cutover plans (including rollback approach where required).
- Pilot migrations to validate approach and refine migration factory processes.
- Controlled migration execution with verification, service validation and stakeholder sign-off.
- Post-migration stabilisation ("hypercare") and service handover to agreed BAU teams.

Legacy Platform Transition and Modernisation Support

For clients exiting legacy estates where direct replatforming is constrained. Outputs include:

- Current state assessment of legacy platforms and operational dependencies.
- Rehost / replatform decision support (including risk-based recommendations).
- Legacy application transition support, including use of emulation patterns where appropriate.
- Testing and validation approach to ensure functional equivalence and controlled risk.
- Operational readiness and handover artefacts tailored to legacy constraints.

Security Services and Cyber Resilience Uplift

For clients strengthening confidentiality, integrity, and availability in cloud services, or needing independent assurance. Outputs include:

- Security posture review and risk assessment, including proactive monitoring and vulnerability assessment where required.
- Threat modelling for critical services and data flows.
- Security architecture and design recommendations (including identity, privileged access, segmentation, logging/monitoring, encryption patterns).
- Incident response readiness: roles, escalation paths, communications approach, recovery planning.
- Security testing and assurance activities (for example, vulnerability assessment, penetration testing support, and remediation planning).
- Security operating model inputs to support BAU delivery.

Quality Assurance and Performance Testing

For clients needing confidence that services will meet non-functional requirements. Outputs include:

- Test approach design (functional and non-functional) with clear entry/exit criteria.
- Performance testing strategy and execution (load/stress/soak as appropriate).
- Operational readiness testing (monitoring, alerting, backup/restore, access controls, failure scenarios).
- Evidence packs suitable for governance and assurance.
- Recommendations for remediation and repeatable testing patterns.

Cloud Financial Management and Cost Optimisation

For clients improving cost control, visibility, and forecasting. Outputs include:

- Baseline cloud spend and usage analysis, including identification of key cost drivers.
- Tagging and cost attribution approaches where appropriate.
- Identification of waste and rightsizing opportunities.
- Recommendations for budgets/alerts and guardrails.
- Licensing and consumption optimisation support (where applicable).
- Reporting approach to track benefits and monitor cost drivers over time.

Training and Knowledge Transfer

For clients building capability to operate cloud services day-to-day. Outputs include:
Typical activities and outputs include:

- Training needs assessment (roles, starting capability, target operating approach).
- Role-based training sessions (basic through to super-user).
- Troubleshooting and operational training aligned to the buyer environment.
- “Train-the-trainer” knowledge transfer so capability is retained internally.
- Runbooks, operational checklists and practical handover sessions.

Ongoing Operational Support

For clients requiring ongoing operational support to maintain stability and performance. Outputs include:

- Incident triage and support aligned to the client’s ITSM processes, including incident management and request fulfilment pathways where agreed.
- Monitoring and alerting refinement and proactive service improvement.
- Problem management support (trend analysis and recommendations for permanent fixes).
- Support documentation upkeep (runbooks, known errors, service knowledge base).
- Regular service reporting and operational governance.

Network Architecture, Security and Connectivity Services

For clients requiring secure, scalable, and well-governed networking to support cloud, hybrid, and on-premise services across multiple business functions. This option supports both transformation programmes and steady-state optimisation.

Outputs include:

- Current state network assessment covering connectivity, segmentation, resilience, performance, and security controls across business departments and service zones.
- Network and connectivity planning, including target state architecture, capacity planning, dependency mapping, and alignment to cloud and hybrid operating models.
- Secure network design incorporating segmentation, access control, traffic management, monitoring, and resilience patterns aligned to public sector security standards.
- Network security services, including design and configuration of controls such as firewalls, load balancing, application delivery, traffic inspection, and monitoring using industry-standard tooling (for example, F5 Networks where appropriate).
- Network migration and transition planning, including cutover sequencing, rollback considerations, and integration with wider cloud or data centre exit programmes.
- Operational readiness for network services, including monitoring and alerting, fault and performance management, security logging, runbooks, and support integration.
- Governance and assurance artefacts, including design decisions, risk assessments, test evidence, and operational handover documentation.

Engagement Models and Delivery Configuration

3ROC Ltd can deliver through one or a blend of the following models depending on client need:

- **Outcome-Based Work Package:** Fixed scope deliverables with agreed acceptance criteria (commonly used for planning, assurance, testing, or security reviews).
- **Embedded Delivery Team:** Named specialists embedded into the client's programme structure to lead or support delivery (commonly used for migration execution and complex transformation).
- **Hybrid Delivery:** A core 3ROC Ltd delivery lead with specialist "surge" support for defined phases (for example, cutover, performance testing, security validation).

Delivery can be provided remote-first, with on-site delivery included where it improves outcomes (for example, stakeholder workshops, critical cutover support, or secure environment requirements). Where required, 3ROC Ltd can propose appropriately vetted personnel, including SC-cleared or SC-clearable consultants.

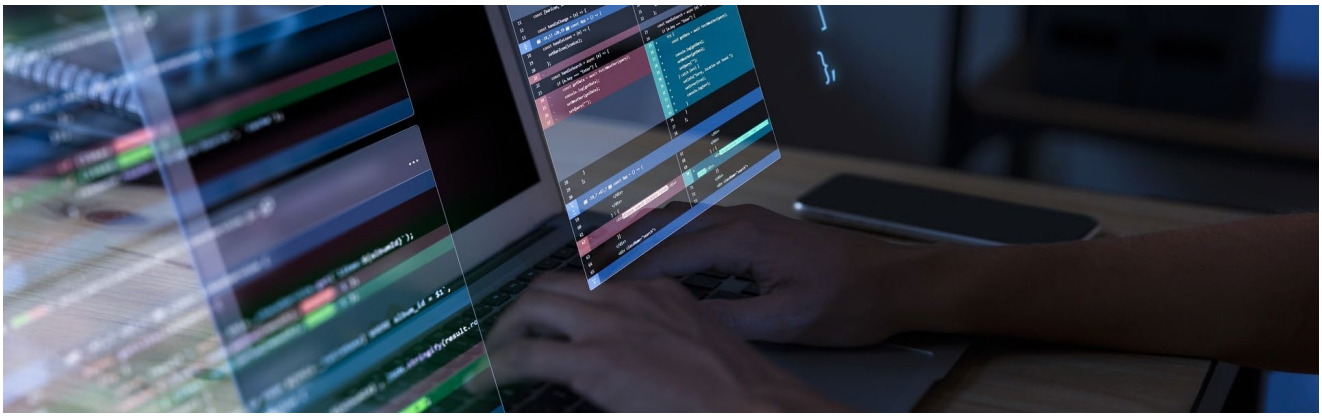
Delivery Control

Across all options, 3ROC Ltd operates with a consistent control framework to keep delivery predictable and auditable:

- Defined deliverables and acceptance criteria agreed up-front.
- Clear governance cadence, typically including delivery stand-ups, weekly checkpoints, and steering governance aligned to buyer requirements.
- RAID management maintained and reviewed throughout delivery.
- Evidence-led assurance, including documented decisions, test results, validation outcomes, and handover artefacts.
- Handover and transition tailored to the client's operating model (including knowledge transfer and operational readiness activities).

Out of Scope

3ROC Ltd's cloud support services focus on enabling, migrating, assuring and supporting cloud services. Bespoke software design and bespoke software development are not included within this service definition.



Delivery Approach and Methodology

How 3ROC Ltd Delivers

3ROC Ltd delivers cloud support services using a controlled, evidence-led approach designed for public sector environments. Our delivery is based on the following principles:

- **Safety and Continuity First:** Minimise risk to live services through staged delivery, controlled change, and clear rollback planning where appropriate.
- **Evidence at Every Step:** Decisions, designs, tests and outcomes are documented so progress can be reviewed and assured.
- **Security by Design:** Security controls are designed in from the outset, not retrofitted at the end.
- **Repeatable Patterns, Tailored Execution:** Proven delivery patterns are applied and adapted to the client's constraints, legacy estate, and operating model.
- **Knowledge Transfer Built-in:** We transfer capability through structured handover, runbooks and training, not just technical delivery.

Delivery Lifecycle

3ROC Ltd typically delivers through three practical stages. The exact shape is confirmed during mobilisation based on scope, complexity, and service criticality.

Stage 1: Mobilise and Discover

Purpose:
Confirm scope, understand the current state, and establish delivery controls.

Activities typically include:

- Kick-off and stakeholder alignment (objectives, constraints, success measures)
- Access and tooling set-up (environments, repositories, comms and reporting cadence)
- Discovery workshops and service/service-map walkthroughs
- Dependency and risk identification (including third parties and legacy constraints)
- Initial plan and schedule confirmation

Outputs typically include:

- Mobilisation plan and governance cadence
- RAID log (risks, assumptions, issues, dependencies)
- High-level migration/support approach and priorities
- Initial operational considerations (monitoring, backup, DR expectations, support boundaries)

Stage 2: Design, Implement and Validate

Purpose: Execute the agreed work package(s) with clear controls and verification.

Activities typically include:

- Target-state design and options analysis (where applicable)
- Cloud landing configuration and environment readiness (where in scope)
- Migration execution (pilot → wave-based delivery), including legacy rehost/ replatform pathways where required
- Security uplift activities (design changes, control implementation, validation)
- Quality assurance and performance testing (as required), with clear entry/exit criteria
- Service validation with client SMEs and service owners

Outputs typically include:

- Low-level designs and implementation records (where applicable)
- Migration runbooks and cutover plans (including rollback approach where appropriate)
- Test evidence (functional verification and non-functional outcomes where required)
- Updated RAID and decision log, reflecting actual delivery outcomes

Stage 3: Stabilise, Handover and Improve

Purpose:
Stabilise the service, embed operational capability, and complete a controlled handover.

Activities typically include:

- Post-change / post-migration stabilisation (“hypercare”) where required
- Operational readiness checks (monitoring, alerting, backup/restore, access controls, support routes)
- Knowledge transfer sessions and “train-the-trainer” enablement
- Handover into BAU (client team, incumbent supplier, or blended model)
- Service improvement backlog and prioritised recommendations (cost, performance, resilience)

Outputs typically include:

- Runbooks and operational checklists
- Handover pack (known issues, support routes, documentation index)
- Training artefacts and recorded sessions where appropriate
- Improvement recommendations with practical next steps

Delivery Controls and Assurance

To keep delivery predictable and governable, 3ROC Ltd applies lightweight but consistent controls:

- **Clear Acceptance Criteria:** Deliverables are agreed upon up front and signed off against objective criteria.
- **Change Control:** Scope changes are managed through documented impact assessment (time, cost, risk).
- **Testing and Validation:** Verification is planned early and executed as part of delivery, not left to the end.
- **Traceability:** Decisions, risks and mitigations are recorded so clients can evidence why choices were made.
- **Escalation Paths:** Issues are escalated quickly to prevent delivery stall and reduce operational risk.

Working with Buyers

3ROC Ltd delivery is most effective when the buyer provides:

- A named service owner and technical lead (for decisions and prioritisation).
- Timely access to environments, documentation and relevant third parties.
- Clarity on constraints (change windows, availability needs, data handling expectations).
- Availability for structured checkpoints and sign-off.

Data Backup, Restore, And Disaster Recovery Support

3ROC Ltd supports clients to design, implement, test, and operate backup and recovery approaches suitable for cloud services and critical workloads.

Typical support includes:

- **Backup and Restore Design:** Define retention, recovery objectives, and restore testing aligned to service criticality.
- **Disaster Recovery Planning:** Establish recovery procedures, roles, and escalation routes; validate feasibility through testing.
- **Operational Readiness Testing:** Validate monitoring, alerting, restore processes, and recovery steps before BAU handover.
- **Continuous Improvement:** Review outcomes from tests or incidents and implement improvements to reduce recovery time.

Where cloud providers deliver native backup/DR capabilities, 3ROC Ltd supports configuration, validation, and operational process embedding so the buyer can operate the service confidently.

Onboarding And Offboarding Support

Onboarding (Mobilisation)

We provide structured onboarding to enable delivery quickly and safely:

- Statement of Work Confirmation: Scope, deliverables, timelines, roles, and acceptance criteria.
- Access and Tooling Onboarding: Secure access to environments and documentation, using client-approved tools.
- Governance Cadence: Stand-ups/checkpoints/steering cadence agreed to match programme complexity.
- RAID and Decision Logs: Established from day one to ensure transparency and control.

Offboarding (Exit And Handover)

Where an engagement ends or transitions to BAU/another supplier, 3ROC Ltd supports a controlled handover:

- **Handover Pack:** Runbooks, documentation index, known issues, and operational guidance.
- **Knowledge Transfer:** Train-the-trainer sessions and walkthroughs of operational processes.
- **Exit Planning:** Where requested, a documented exit approach with timetable, responsibilities, and transfer activities.
- **Secure Close:** Confirmation of returned artefacts and closure of access in line with agreed security procedures.

Service Constraints And Customisation

- **No Bespoke Software Development:** 3ROC Ltd does not provide bespoke application design or bespoke application development within this service definition.
- **Buyer Environment Dependent:** Delivery typically takes place within buyer-provided or client-procured cloud environments (AWS/Azure/hybrid).
- **Security and Change Constraints Apply:** Delivery timelines may be influenced by client change windows, approval processes, and third-party dependencies.
- **Tailored Delivery Approach:** While we avoid bespoke application build, we tailor delivery plans, runbooks, and governance to client operating models and constraints.

Service Levels: Performance, Availability, And Support Hours

Service levels are agreed per engagement and documented in the Statement of Work.

Typical support models include:

- **Core Support Hours:** Monday to Friday, 09:00–18:00 (UK Time), Excluding Bank Holidays.
- **Out-of-Hours Support:** Available for critical incidents or cutover activities where agreed.
- **Response and Escalation:** Severity definitions, acknowledgement targets, and escalation routes agreed during mobilisation.
- **Reporting:** Regular delivery reporting during active phases, and operational reporting where ongoing support is in scope.

Where 24/7 support is required for mission-critical services, 3ROC Ltd can provide an on-call model subject to the client's requirements and the agreed support scope.

After Sales Support and Account Management

3ROC Ltd provides a named point of contact and structured service governance to keep delivery controlled and responsive

- **Dedicated Service Lead:** Primary escalation point for delivery, quality, and governance.
- **Regular Service Checkpoints:** Operational or programme check-ins aligned to the engagement.
- **Issue and Complaint Handling:** Acknowledgement and investigation managed through documented escalation and resolution steps.
- **Invoicing Query Support:** Defined route for invoice queries, with agreed acknowledgement and resolution approach.

Technical Requirements

As a cloud support service, 3ROC Ltd does not require buyers to install proprietary software. Typical requirements include:

- **Secure Connectivity:** Buyer-approved connectivity to relevant cloud environments and tooling.
- **Collaboration Tools:** Access to client-approved collaboration and documentation platforms (e.g., Teams, email, ticketing/ITSM).
- **Stakeholder Availability:** Named technical leads and service owners for decisions, approvals, and validation.
- **Environment Access:** Appropriate access permissions aligned to least privilege and segregation of duties.

Any additional technical prerequisites are confirmed during mobilisation and documented before delivery begins.

Access To Data (Upon Exit)

3ROC Ltd does not retain ownership of client data. Any delivery artefacts produced during the engagement (e.g., runbooks, plans, designs, test results, risk logs) are provided as part of handover.

- **Artefact Transfer:** Documentation and deliverables are transferred using buyer-approved secure methods.
- **Data Minimisation:** We only access and process information required to deliver the agreed scope.
- **Retention and Deletion:** Where 3ROC Ltd holds copies of artefacts (e.g., working documents), retention and secure deletion are handled in line with the agreed engagement terms and buyer requirements.

Security

3ROC Ltd applies security controls appropriate to supporting regulated public sector environments. Our approach includes:

- **Access Controls and Least Privilege:** Role-based access, controlled elevation, and time-bound access where required.
- **Multi-Factor Authentication:** Applied to accounts and tooling where supported by the buyer environment.
- **Secure Handling of Information:** Use of client-approved secure channels, encrypted storage where applicable, and controlled sharing.
- **Vulnerability and Risk Management:** Security risk assessment, prioritised remediation planning, and validation support.
- **Auditability:** Evidence-led delivery artefacts (decisions, testing outcomes, and operational readiness checks) to support assurance.

Where required, 3ROC Ltd provides appropriately vetted personnel (including SC-cleared/SC-clearable consultants) subject to client requirements and role suitability.

3ROC.
TECHNOLOGY

3Roc, Office F8, The Esplanade,
Rochdale OL16 1AE
support@3roc.co.uk
+44 7896-774344