
CLOUD AND DEVOPS SERVICES

Service Definition



19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTIONS

**Regus Atterbury Lakes Fairbourne Drive, Atterbury, Milton Keynes, Buckinghamshire,
England, MK10 9RG**

Contents

Service overview	2
Scope of services	2
Onboarding and engagement initiation	4
Service constraints	4
Service levels	4
After-sales support	5
Technical and client-side requirements	5
Outage and maintenance management.....	6
Hosting options and locations.....	6
Data access on exit	6
Security and governance	6

Service overview

The Cloud and DevOps Services provide end-to-end advisory, design, implementation, and operational support for modern cloud platforms and DevOps practices. The service enables organisations to deploy scalable, secure, resilient, and automated infrastructure and application environments, including those required to support AI, generative AI, and agentic AI workloads, analytics, BI solutions, and enterprise applications.

Capabilities include:

- Cloud adoption strategy, architecture, and platform selection (public, private, hybrid, or multi-cloud)
- Design and implementation of DevOps pipelines, CI/CD workflows, and automated deployments
- Infrastructure-as-Code (IaC) development and management
- Configuration, release, and environment management
- Platform monitoring, alerting, and optimisation
- Security, compliance, and governance integration into DevOps processes
- Automation of repetitive operational tasks and scaling of AI/analytics workloads
- Integration with data platforms, BI, and AI/agentic AI solutions

The service is delivered via project-based or ongoing engagements, combining advisory, implementation, and operational support to ensure rapid, reliable, and auditable deployments.

Scope of services

Cloud strategy and advisory

- Cloud readiness assessments and migration strategy development
- Cloud platform selection and design, including scalability, resilience, and cost optimisation
- Hybrid and multi-cloud architecture guidance
- Recommendations for supporting AI, agentic AI, analytics, and BI workloads

- Governance and risk alignment, including regulatory, compliance, and shared responsibility considerations

DevOps and automation

- CI/CD pipeline design and implementation for applications, analytics models, and AI/agent AI systems
- Automated testing, integration, and deployment workflows
- Infrastructure-as-Code (IaC) frameworks using Terraform, Ansible, or equivalent tools
- Environment provisioning and lifecycle management
- Automated monitoring, alerting, and incident response integration

Security, compliance, and governance

- Integration of security into CI/CD pipelines and cloud infrastructure (DevSecOps)
- Access control, role-based permissions, and least-privilege enforcement
- Compliance alignment with ISO/IEC 27001, ISO/IEC 42001, GDPR, and relevant industry regulations
- Audit trails for deployments, changes, and environment configurations
- Governance and risk advisory for AI and agent AI workloads deployed in cloud or DevOps pipelines

Cloud operations and optimisation

- Monitoring and logging of cloud services, platforms, and applications
- Performance optimisation for compute, storage, and network resources
- Backup, restore, and disaster recovery planning for cloud environments
- Cost management and usage optimisation guidance
- Scalability recommendations for high-demand analytics or AI workloads

Onboarding and engagement initiation

Following contract agreement, a Delivery Manager and cloud/DevOps team are assigned. A kick-off session is conducted to confirm objectives, scope, stakeholders, governance arrangements, and engagement logistics.

A Statement of Work or Engagement Definition document is agreed, defining scope, assumptions, deliverables, timelines, dependencies, and client responsibilities. Access to relevant cloud accounts, environments, and infrastructure documentation is provisioned to enable effective delivery.

Service constraints

Service delivery depends on access to client-managed environments, datasets, and platform credentials. Cloud infrastructure costs are service and client-dependent. CI/CD pipeline effectiveness relies on defined source control, testing, and deployment standards. Scheduled maintenance, platform upgrades, or optimisation activities may temporarily affect availability. Security and compliance alignment requires active client participation and defined governance.

Service levels

Unless otherwise agreed in writing, the service and ongoing support shall be provided during standard business hours (9-5), Monday to Friday. Support outside of these hours, including 24/7 support, may be provided subject to a separately agreed arrangement.

Support levels are defined per engagement:

Standard Support: Remote assistance during business hours for cloud or DevOps issues, guidance on CI/CD, and deployment troubleshooting.

Enhanced Support: Extended business-hours coverage, proactive monitoring of pipelines and cloud resources, optimisation support, and named technical contact.

Premium Support: Designed for mission-critical cloud or DevOps environments, offering priority response, 24/7 coverage, proactive monitoring, incident escalation, and dedicated Cloud/DevOps Lead.

Severity Classifications:

- **Severity 1 (Critical):** Production environment outage or deployment failure; immediate response



- **Severity 2 (High):** Major issue affecting CI/CD pipelines or cloud availability; rapid resolution required
- **Severity 3 (Medium):** Partial functionality limitation; addressed within standard response times
- **Severity 4 (Low):** Minor queries, optimisations, or configuration adjustments; handled during business hours

Support is primarily delivered remotely, with onsite assistance available by arrangement.

After-sales support

Following implementation, a formal handover is conducted including documentation covering CI/CD pipelines, IaC templates, cloud architecture, configurations, monitoring, and operational procedures. Knowledge transfer sessions may be provided to ensure client teams can operate, monitor, and maintain cloud and DevOps environments.

Ongoing support may include:

- Pipeline updates or extensions for AI/agent AI, analytics, or application workloads
- Cloud resource optimisation
- Security patching and configuration updates
- Environment scaling and orchestration

Technical and client-side requirements

The client is responsible for providing:

- Access to cloud accounts, source control, and infrastructure environments
- Identification of key stakeholders and subject-matter experts
- Defined policies for security, compliance, and change control
- Network connectivity, identity, and access integration for CI/CD and automated deployments

Outage and maintenance management

Planned maintenance, updates, or optimisation activities are scheduled in coordination with the client to minimise disruption. In the event of a service-affecting issue attributable to the service provider's deliverables, remediation is undertaken at no additional cost.

For issues arising from factors outside agreed scope (e.g., third-party cloud outages, client-managed changes), support may be provided under separate engagement or retainer arrangements.

Hosting options and locations

The service supports public, private, hybrid, and multi-cloud environments. Hosting and infrastructure selection is guided by functional, security, regulatory, and cost requirements. Where required, the service provider can host environments or CI/CD platforms under agreed SLA and governance terms.

Data access on exit

Clients retain ownership of all source code, IaC templates and scripts, configurations, deployment scripts, and cloud resources created during engagements. All artefacts are delivered in industry-standard formats upon exit, with residual data securely deleted or anonymised in accordance with retention agreements and regulatory requirements.

Security and governance

Security and governance are embedded in all phases of cloud and DevOps delivery, aligned with ISO/IEC 27001, ISO/IEC 42001 (for AI/agentic AI workloads), and cloud shared responsibility models. This includes:

- Role-based access and least-privilege enforcement
- CI/CD pipeline auditability and traceability
- Compliance with regulatory and contractual requirements
- Monitoring, logging, and alerting for security events
- Governance alignment for AI/agentic AI solutions deployed via cloud or DevOps pipelines



Responsibilities are shared between the service provider, client, and any third-party cloud providers, with clear allocation of accountability per engagement.