END-TO-END DATA & AI TRANSFORMATION

Service Definition

TRIDENT
INTELLIGENT SOLUTIONS

19 JANUARY 2026

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

Contents

Service overview

The End-to-End Data and AI Transformation service provides a full lifecycle approach to enabling public sector organisations to design, implement, and embed modern data and artificial intelligence capabilities. The service spans strategic assessment and architecture

design through to data platform delivery, advanced analytics and AI solution development, deployment, operationalisation, and workforce enablement.

Delivery is structured as a phased transformation programme tailored to organisational maturity, policy context, and risk profile. Activities may include current-state and maturity assessment, target-state architecture and operating model design, governance and assurance setup, data platform implementation, analytics and AI solution development, MLOps and operational processes, change management, and skills uplift. Solutions may be deployed in customer-managed, service provider-managed, or third-party cloud environments, depending on agreed requirements and constraints.

Data backup, restore, and disaster recovery

Backups of data, code, models, configurations, pipelines, and transformation artefacts are performed at predefined intervals and protected through access controls and encryption in line with ISO/IEC 27001 standards. Backup frequency and retention periods are defined per engagement or workstream, based on business, regulatory, and contractual requirements.

Disaster recovery and business continuity arrangements define roles, responsibilities, and recovery procedures across data platforms and AI solutions. These arrangements are reviewed periodically to reflect changes in scope, architecture, or risk. Where third-party platforms or cloud services are used, their resilience and continuity controls are incorporated under a shared responsibility model, supporting information availability and continuity.

For each engagement, documentation covers:

- Assets backed up
- Backup frequency and retention
- Storage location
- Restoration procedures
- Testing schedules
- Roles and responsibilities

Onboarding and offboarding support

Onboarding

Following contract agreement, a Transformation Lead, Delivery Manager, and multi-disciplinary delivery team are assigned to the engagement. Delivery follows a programme-based approach, combining structured governance with Agile delivery practices where appropriate.

A mobilisation and kick-off phase is conducted to confirm objectives, scope, success measures, and delivery approach. Governance, assurance, and reporting arrangements are established at this stage. A Transformation Initiation Document (or equivalent) is produced and

approved, defining vision, scope, roadmap, roles and responsibilities, dependencies, risks, and success criteria.

During onboarding, secure access is provisioned to required data, systems, and environments. Alignment is also achieved on data governance, ethical AI principles, information security expectations, and applicable public sector legal and regulatory requirements.

Offboarding

At agreed transition points or at the conclusion of the engagement, a formal offboarding and handover process is conducted. This includes walkthroughs of architectures, platforms, AI solutions, MLOps processes, and governance arrangements, as well as training and knowledge transfer for customer teams where required.

All deliverables and artefacts—including strategies, architectures, code, models, pipelines, documentation, and operational procedures—are formally handed over to the customer, except where components are hosted or managed under a separate ongoing agreement. In the event of early termination, a controlled exit process and closure document are provided to support an orderly transition.

Service constraints

The service is delivered during standard business hours unless otherwise agreed. Delivery is dependent on customer readiness, availability of data and stakeholders, and timely provision of agreed inputs and decisions.

Service levels

Service levels, including delivery milestones, responsiveness, availability, and support expectations, are defined and agreed at the outset of the engagement. Service levels are tailored to the scale, complexity, and criticality of the transformation programme and are documented in the applicable statement of work or programme agreement.

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.

After-sales support

Following completion of the transformation or individual phases, a formal handover supports transition to business-as-usual operation. Comprehensive documentation is provided covering platforms, pipelines, models, MLOps processes, governance, and operational procedures.

Ongoing support and managed services may be provided where required, including platform operation, AI model monitoring and retraining, optimisation, and continuous improvement.

These services are agreed on a case-by-case basis and delivered under retainer-based or time-and-materials arrangements.

Technical and client-side requirements

The customer is responsible for identifying appropriate executive sponsors, business owners, technical leads, security and governance contacts, and operational stakeholders to support effective decision-making and delivery.

The service provider requires appropriate access to customer-managed environments, including cloud platforms, data sources, and development and testing environments, in line with agreed deployment models. Access controls and permissions are provisioned in accordance with customer policies and the principle of least privilege.

Any additional technical or organisational prerequisites are identified during onboarding and managed through programme governance.

Outage and maintenance management

Where operational platforms or solutions delivered as part of the transformation fall within the service provider's responsibility, issues attributable to delivered components are investigated and remediated at no additional cost, subject to agreed scope and acceptance criteria.

Issues arising from factors outside scope, such as customer-managed infrastructure changes, upstream data issues, third-party platform failures, or enhancement requests, may be supported under agreed maintenance or managed service arrangements. Planned maintenance is coordinated to minimise disruption.

Hosting options and locations

Solutions may be deployed within customer-managed infrastructure, including public cloud or on-premises environments, under a shared responsibility model. Where required, the service provider can host solutions on behalf of the customer for an additional fee.

Hosting providers, geographic locations, data residency, resilience characteristics, and security controls are agreed per engagement and documented as part of the solution design.

Data access on exit

Customers retain full ownership of all customer-provided data, derived datasets, models, code, configurations, and artefacts developed during the engagement. Upon exit, all agreed assets are made available in industry-standard formats to support continued operation or transition.

Reasonable transition support is provided for a defined period, subject to engagement terms. Any residual customer data held by the service provider is securely deleted or anonymised in accordance with agreed retention schedules and applicable regulations.

Security

Security is embedded throughout the service lifecycle and aligned with recognised standards, including ISO/IEC 27001, public sector security principles, and applicable cloud shared responsibility models. This includes:

- Information security governance with defined roles and responsibilities
- Risk-based security controls proportionate to data sensitivity and AI risk
- Role-based access control and least-privilege principles
- Encryption of data in transit and at rest where appropriate
- Monitoring, logging, and auditability
- Supplier and shared responsibility management
- Secure information lifecycle and exit management

Security responsibilities are shared between the service provider, the customer, and any relevant third-party providers, with control ownership defined per engagement.