
DATA SCIENCE AND ADVANCED ANALYTICS

Service Definition



19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTIONS

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

Contents

Service overview	1
Data backup, restore, and disaster recovery.....	2
Onboarding and offboarding support	2
Service constraints	3
Service levels.....	3
After-sales support	4
Technical and client-side requirements.....	4
Outage and maintenance management	4
Hosting options and locations	5
Data access on exit	5
Security	5

Service overview

The Data Science and Advanced Analytics service provides end-to-end design, development, and operationalisation of advanced analytical solutions that enable organisations to extract actionable insights from complex data. The service covers activities from discovery and



analytical readiness through to model development, validation, deployment, and on-going support.

The service includes predictive and explanatory modelling, statistical analysis, machine learning, natural language processing, and other advanced analytics techniques. Solutions are designed to support improved decision-making, forecasting, operational efficiency, and service delivery across a wide range of use cases, including but not limited to performance optimisation, risk analysis, customer insight, demand forecasting, and text or document analytics.

The service is delivered through a structured, project-based engagement model. Activities may include problem definition, data exploration and preparation, feature engineering, model selection and development, validation and testing, integration with data platforms or downstream systems, deployment, and transition to operational use. 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 analytical datasets, feature sets, models, code, notebooks, and configuration 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 on a project-by-project basis according to business, regulatory, and contractual requirements.

Disaster recovery and business continuity plans define roles, responsibilities, and recovery procedures and are reviewed periodically to reflect changes in service scope or risk. Where third-party analytics platforms or cloud services are used, their resilience and continuity controls are incorporated under a shared responsibility model. These measures collectively support ISO 27001 requirements for information availability and continuity.

For each project, the following is documented:

- What data, models, and artefacts are backed up
- Backup frequency
- Storage location
- Restoration procedures
- Testing schedule
- Roles and responsibilities

Onboarding and offboarding support

Onboarding

Following contract agreement, a Delivery Manager and appropriate data science delivery team are assigned to the engagement. Delivery is conducted using either a structured waterfall or Agile methodology, depending on the scale, complexity, and analytical maturity of the project.

A kick-off workshop is held to introduce key stakeholders, confirm the agreed scope, and establish governance, communication, and delivery arrangements. A Project Initiation Document (or Discovery Initiation Document where applicable) is produced and approved by key stakeholders. This document defines objectives, scope, delivery plan, roles and responsibilities, governance arrangements, and key risks and dependencies, and serves as the primary reference throughout delivery.

During onboarding, the service provider works with the customer to provision secure access to required data sources, analytics environments, tools, and platforms. Alignment is also achieved on analytical objectives, data governance requirements, ethical considerations, information security expectations, and relevant legal or regulatory constraints.

Offboarding

At the conclusion of the engagement, a formal offboarding workshop and handover session is conducted to support transition of analytical solutions to the customer. This session covers analytical approaches, model assumptions, performance characteristics, operational considerations, and agreed next steps, and may include training for relevant customer teams where required.

All solution artefacts, including models, feature definitions, code, notebooks, configurations, and technical documentation, are formally handed over to the customer, except where solutions are hosted or managed by the service provider under an ongoing agreement.

In the event of early termination, a closure workshop is held to assess the status of all in-scope items and agree required actions. A Project Closure Document is provided to support an orderly and controlled exit.

Service constraints

Service delivery depends on access to client systems, datasets, and subject-matter experts. Model accuracy depends on data quality, completeness, and availability. Integration with client systems may require additional approvals or resources. Scheduled maintenance, model retraining, or updates may temporarily affect availability. Large-scale analytics projects or complex machine learning models may require phased delivery. Ongoing support, monitoring, and optimisation are provided under separate agreements unless specified. Clients must provide access, permissions, and staff participation to achieve full service benefits.

Service levels

Service levels, including delivery milestones, response times, model performance expectations (where applicable), and support hours, are defined and agreed at the commencement of each engagement. These service levels are tailored to the analytical use case, criticality of outputs, and the customer's operational and business requirements.



Agreed service levels are documented in the applicable statement of work or support agreement and are reviewed periodically to ensure continued alignment with service usage, risk profile, and contractual obligations.

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 delivery of the data science or advanced analytics solution, a formal handover is conducted to support transition to operational use. This includes comprehensive documentation covering analytical methods, data inputs, feature engineering, model logic, validation results, assumptions, and limitations.

Ongoing maintenance and support services are available where required and are agreed on a case-by-case basis. These services may be provided under a retainer-based support arrangement or on a time-and-materials basis. Maintenance activities may include model retraining, recalibration, performance monitoring, enhancements, and adaptation to changes in underlying data or business requirements.

Technical and client-side requirements

The customer is responsible for identifying relevant business, analytical, technical, security, and governance stakeholders to support decision-making, approvals, and effective day-to-day collaboration throughout the engagement. The service provider will provide guidance on required roles and responsibilities to support successful delivery.

Depending on the agreed delivery and deployment model, the service provider requires appropriate access to customer-managed environments, including analytics platforms, data platforms, development and testing environments, or on-premises infrastructure. Access permissions and security controls are agreed in advance and provisioned in accordance with customer security policies and the principle of least privilege.

Any additional technical prerequisites, such as data availability, compute capacity, identity integration, or third-party analytics tools, are identified and agreed during onboarding to ensure timely and effective service delivery.

Outage and maintenance management

In the event of a service outage or operational issue attributable to defects or errors within the scope of the delivered analytical solution and under the service provider's responsibility, remediation will be undertaken at no additional cost. This includes investigation, root cause analysis, and corrective action necessary to restore normal operation, subject to agreed scope and acceptance criteria.



Where issues arise from factors outside the agreed scope, such as upstream data quality issues, customer-managed infrastructure changes, third-party platform failures, or requests for enhancements, support may be provided under an agreed maintenance arrangement on a retainer or time-and-materials basis.

Planned maintenance activities, including updates, recalibration, or enhancements, are scheduled in coordination with the customer wherever practicable to minimise disruption. Roles, responsibilities, escalation paths, and service boundaries are defined per engagement to support effective incident and maintenance management.

Hosting options and locations

Advanced analytics solutions may be deployed within the customer's existing infrastructure, including customer-managed cloud analytics platforms or on-premises environments. In these scenarios, the service provider supports deployment and integration within agreed scope, while the customer retains responsibility for the underlying infrastructure under a shared responsibility model.

Where required, the service provider can host analytical solutions on behalf of the customer for an additional fee. Hosted deployments utilise cloud-based infrastructure selected to meet functional, security, regulatory, and data residency requirements. Hosting provider, geographic location, resilience characteristics, and security controls are agreed and documented per engagement.

Data access on exit

Customers retain full ownership of all customer-provided data, derived datasets, models, features, code, and analytical artefacts developed during the engagement. The service provider acts as a data processor and does not retain customer data beyond what is necessary to deliver the services.

Upon service exit, all agreed data sets, models, code, and documentation are made available to the customer in mutually agreed, industry-standard formats to support continued use or migration. Reasonable assistance is provided during a defined transition period, subject to the terms of the engagement. Any residual customer data retained 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 information security standards, including ISO/IEC 27001, and applicable cloud shared responsibility models. This includes:

- **Information Security Governance**

Defined security roles, responsibilities, and decision-making authority per engagement.



- **Risk-Based Security Controls**
Controls selected based on data sensitivity, analytical methods, and deployment model.
- **Access Control**
Role-based access and least-privilege principles applied to analytics environments and data.
- **Data Protection and Encryption**
Encryption of data in transit and at rest where appropriate.
- **Monitoring, Logging, and Auditability**
Logging of relevant events to support monitoring, investigation, and audit requirements.
- **Supplier and Shared Responsibility Management**
Clear allocation of responsibilities where third-party platforms are used.
- **Information Lifecycle and Exit Management**
Secure data handling, retention, and deletion on service exit.

Security responsibilities are shared between the service provider, the customer, and any relevant third-party platform or infrastructure providers. Roles, responsibilities, and control ownership are defined per engagement to ensure proportionate risk management and compliance with contractual, regulatory, and operational requirements.