
DATA STRATEGY AND ADVISORY 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
Data access on exit	4
Security	4

Service overview

The Data Strategy and Advisory service provides expert, independent guidance to support public sector organisations in defining, maturing, and operationalising their data capabilities.



The service focuses on assessing current-state maturity, identifying gaps and opportunities, and developing practical, prioritised, and achievable data strategies aligned to organisational objectives, policy drivers, and service outcomes.

The service encompasses assessment of data infrastructure, data governance and management practices, analytics and insight capabilities, operating models, and organisational readiness, including skills and ways of working. Outputs include actionable roadmaps, prioritised high-value use cases, target-state architectures, and recommendations designed to support sustainable adoption of data capabilities and measurable improvements in decision-making, efficiency, and service delivery.

The service is delivered through a structured, advisory-led engagement model. Activities may include stakeholder engagement, maturity assessments, discovery workshops, data and analytics landscape reviews, governance and operating model design, benefits identification, and development of phased delivery roadmaps. The service may be delivered as a standalone engagement or as a precursor to delivery services such as data engineering, advanced analytics, or AI solution development.

Data backup, restore, and disaster recovery

Where the service involves the handling or creation of assessment artefacts, documentation, or limited datasets, these materials are stored securely and protected through access controls and encryption in line with ISO/IEC 27001 standards. Backup frequency and retention periods are defined in accordance with the nature of the engagement and applicable contractual requirements.

Given the advisory nature of the service, disaster recovery arrangements primarily relate to the availability and integrity of documentation and working artefacts rather than operational systems. Roles, responsibilities, and recovery procedures are defined as appropriate to the engagement. Where third-party collaboration or document management platforms are used, their resilience and continuity controls are incorporated under a shared responsibility model.

For each engagement, the following is documented where applicable:

- What artefacts or data are backed up
- Backup frequency
- Storage location
- Restoration procedures
- Roles and responsibilities

Onboarding and offboarding support

Onboarding

Following contract agreement, a Delivery Manager and an appropriately skilled advisory team are assigned to the engagement. Delivery is conducted using a structured advisory or Agile approach, depending on the scale and scope of the engagement.



A kick-off workshop is held with key stakeholders to confirm objectives, scope, success measures, and delivery approach. Governance, communication, and engagement arrangements are established at this stage. A Project Initiation Document or equivalent engagement plan is produced and agreed, defining objectives, scope, milestones, roles and responsibilities, key assumptions, and risks.

During onboarding, the service provider works with the customer to agree access to relevant documentation, data summaries, systems, and stakeholders required to support assessments and analysis. Alignment is also achieved on information security expectations, data sensitivity, ethical considerations, and relevant public sector policy, legal, or regulatory requirements.

Offboarding

At the conclusion of the engagement, a formal offboarding and close-out workshop is conducted to present findings, recommendations, and agreed next steps. This session supports knowledge transfer and ensures stakeholders understand the proposed roadmap, priorities, and dependencies.

All deliverables, including assessment reports, strategies, roadmaps, business cases, and supporting materials, are formally handed over to the customer. In the event of early termination, a closure workshop is held to review progress and agree the status of all in-scope deliverables. A Closure Document is provided to support an orderly and transparent exit.

Service constraints

The Data Strategy and Advisory service is delivered during standard business hours, unless otherwise agreed. The service is advisory in nature and does not include responsibility for the implementation or operation of technical solutions unless explicitly agreed as part of a separate delivery engagement.

Service levels

Service levels, including delivery milestones, responsiveness, and availability for workshops and stakeholder engagement, are defined and agreed at the commencement of each engagement. Service levels are tailored to the scale, duration, and criticality of the advisory engagement and the customer's governance and decision-making timelines.

Agreed service levels are documented in the applicable statement of work and are reviewed as necessary to ensure continued alignment with engagement objectives and constraints.

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 Data Strategy and Advisory engagement, a formal handover is conducted to support customer understanding and ownership of the outputs. This includes walkthroughs of strategies, roadmaps, and recommendations, and clarification of assumptions, dependencies, and risks.

Further advisory support may be provided where required, including roadmap refinement, benefits tracking, governance support, or preparation for delivery phases. Such support is agreed on a case-by-case basis and may be provided on a time-and-materials or retainer basis, depending on customer needs.

Technical and client-side requirements

The customer is responsible for identifying appropriate business, digital, data, analytical, security, and governance stakeholders to support effective engagement, decision-making, and approvals throughout the advisory engagement.

The service provider may require access to relevant documentation, high-level data summaries, system overviews, and policy or governance materials. Any access requirements are agreed in advance and managed in accordance with customer information security policies and the principle of least privilege.

Where technical assessments are included, any prerequisites, such as system access, architecture diagrams, or inventory information, are identified during onboarding to ensure timely and effective delivery.

Data access on exit

Customers retain full ownership of all information, documentation, and artefacts created or provided during the engagement. The service provider acts as a data processor where applicable and does not retain customer information beyond what is necessary to deliver the service.

Upon service exit, all deliverables and agreed working materials are provided to the customer in industry-standard formats. Following completion of the exit process, any residual customer information held by the service provider is securely deleted or anonymised in accordance with agreed retention schedules and applicable legal or regulatory requirements.

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.