END-TO-END DIGITAL TRANSFORMATION

Service Definition

19 JANUARY 2026

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

Contents

Service overview

The End-to-End Digital Transformation Service supports organisations in planning and delivering comprehensive technology-enabled change across their operations. The service helps

customers modernise processes, systems, and ways of working to improve efficiency, resilience, and customer outcomes.

The service can cover the full transformation lifecycle, including discovery and assessment, strategy and roadmap definition, target operating model and architecture design, platform and application modernisation, data and integration capabilities, and the delivery of bespoke software solutions. Engagements are tailored to the customer's environment and priorities, and may include cloud adoption, systems integration, workflow automation, and analytics.

Delivery is carried out using structured and iterative methods, with a focus on security, scalability, and operational sustainability. Governance, risk management, and compliance considerations are embedded throughout the engagement, alongside change management and knowledge transfer to support adoption and long-term value realisation.

The service may be delivered as a fully managed end-to-end engagement or as modular components, allowing customers to engage at specific stages of their digital transformation while maintaining coherence across strategy, delivery, and operations.

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. Delivery is conducted via a programme-based approach combining structured governance with Agile methods as appropriate.

A mobilisation and kick-off phase introduces stakeholders, confirms objectives and success measures, establishes governance and communication arrangements, and sets the delivery approach. A Transformation Initiation Document (or equivalent) is produced and approved, defining scope, roadmap, roles and responsibilities, risks, and key dependencies.

During onboarding, secure access is provisioned to relevant systems, environments, and documentation. Alignment is also achieved on information security, regulatory requirements, ethical principles, and organisational policies.

Offboarding

At the conclusion of the engagement or at agreed transition points, a formal offboarding and handover process is conducted. This includes walkthroughs of digital platforms, architectures, operational processes, and governance arrangements, and may include training and knowledge transfer for relevant staff.

All deliverables, including strategies, architectures, software artefacts, code, models, operational procedures, and documentation, are formally handed over, except where components are hosted or operated under ongoing agreements. In cases of early termination, a closure workshop and Transformation Closure Document are provided to ensure an orderly transition.

Service constraints

The service is delivered during standard business hours unless otherwise agreed. Delivery is dependent on customer readiness, timely provision of inputs, stakeholder availability, and decision-making.

Service levels

Service levels, including delivery milestones, responsiveness, and availability for workshops or support, are agreed at the outset and documented in the statement of work. Levels are tailored to the scale, complexity, and criticality of the digital transformation programme and are reviewed periodically to ensure alignment with organisational priorities.

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, a formal handover supports transition to business-as-usual operation. Documentation covers platforms, applications, data pipelines, AI models, security controls, operational procedures, and governance arrangements.

Ongoing support or managed services can be provided, including application maintenance, AI monitoring and retraining, platform optimisation, security updates, and continuous improvement. These services are agreed on a case-by-case basis under retainer-based or time-and-materials arrangements.

Technical and client-side requirements

The customer is responsible for identifying appropriate stakeholders, including executive sponsors, business owners, technical leads, and governance contacts, to support decision-making and coordination throughout the engagement.

The service provider requires secure access to relevant systems, environments, and documentation. Access and permissions are provisioned in line with customer policies and the principle of least privilege. Any additional technical prerequisites, such as network access, identity integration, or system dependencies, are identified during onboarding.

Outage and maintenance management

Where platforms, applications, or services delivered as part of the programme are managed by the service provider, outages attributable to delivered components are remediated at no additional cost, subject to agreed scope.

Issues arising from factors outside the agreed scope, such as customer-managed infrastructure, third-party platform failures, or enhancement requests, may be addressed under agreed maintenance arrangements. Planned updates and enhancements are coordinated to minimise disruption.

Hosting options and locations

Solutions may be deployed within customer-managed infrastructure, including cloud platforms or on-premises systems, under a shared responsibility model. The service provider can also host solutions on behalf of the customer, subject to agreed commercial and security arrangements. Hosting locations, resilience characteristics, and controls are agreed per engagement.

Data access on exit

Customers retain full ownership of all data, software artefacts, models, configurations, and documentation developed during the engagement. Upon exit, all agreed assets are provided in

standard formats to support continued operation or transition. Residual customer data held by the service provider is securely deleted or anonymised in line with retention schedules and regulatory requirements.

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.