AI AND GENERATIVE AI SOLUTION DEVELOPMENT

Service Definition

19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTIONS

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

TRIDENT
INTELLIGENT SOLUTIONS

Contents

Service overview

The AI and Generative AI Solution Development service provides end-to-end design from discovery and AI readiness to development, deployment, and on-going support of artificial intelligence solutions. The service encompasses the use of data, models, platforms, and tools to design, build, test, and operationalise AI and Generative AI capabilities across a range of use cases, including but not limited to analytics, automation, decision support, and content generation.

The service is delivered through a structured, project-based engagement model. Activities may include requirements definition, data preparation, model selection or development, system integration, testing, deployment, development of their service, relevant API's and frontends 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 data, models, code, and configuration are performed at predefined intervals and protected through access controls and encryption in line with ISO 27001 standards. Backup interval 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 regularly reviewed to reflect service or risk changes. Where third-party platforms 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 we document:

- What is backed up
- How often
- Storage location
- Restoration procedure
- Testing schedule
- Roles and responsibilities

Onboarding and offboarding support

Onboarding

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

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

During onboarding, Trident Intelligence works with the client to provision secure access to required data, systems, tools, and environments necessary to deliver the services. Alignment is also achieved on applicable ethical principles, data usage requirements, information security expectations, and relevant legal or regulatory considerations.

Offboarding

At the conclusion of the engagement, a formal offboarding workshop and handover session is conducted to support transition of the solution to the customer. This session covers solution overview, operational considerations, and agreed next steps, and may include training for relevant customer teams and stakeholders where required.

All solution artefacts, including source code, models, configurations, and associated technical and operational documentation, are formally handed over to the customer, except where the solution is hosted by the service provider. In hosting scenarios, code access and handover arrangements are defined in the applicable hosting or support 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 in advance of contract termination to support an orderly exit.

Service constraints

Service delivery depends on timely access to client systems, data, and subject-matter experts. Solution performance and reliability are influenced by data quality, model selection, prompt design, and system integration complexity. Generative AI outputs may vary and cannot be guaranteed to be fully deterministic, accurate, or free from bias or model limitations.

Cloud infrastructure and model usage costs may vary based on solution design, scale, and deployment requirements. Scheduled maintenance, model updates, or changes to third-party AI services may temporarily affect availability or behaviour. Large-scale deployments or integration with legacy systems may require phased delivery. Ongoing monitoring, optimisation, governance, and support are provided under separate agreements unless specified. Clients must provide appropriate access, permissions, and engagement to achieve full service benefits.

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.

Service levels, including performance targets, availability expectations, response times, and support hours, are defined and agreed at the commencement of each engagement. These service levels are tailored to the nature, criticality, and deployment model of the solution, as well as the customer's operational and business requirements.

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

After-sales support

Following delivery of the AI or Generative AI solution, a formal handover is conducted to support a smooth transition to operational use. This handover includes the provision of comprehensive documentation covering solution architecture, configurations, models, code repositories, operational procedures, and any agreed support or maintenance requirements. Knowledge transfer sessions may also be provided to ensure relevant customer teams are equipped to operate and manage the solution effectively.

Ongoing maintenance and support services are available where required by the customer 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, depending on the nature of the support required and the customer's operational needs. Maintenance activities may include model updates and enhancements.

Technical and client-side requirements

The customer is responsible for identifying relevant client-side stakeholders, including business, technical, security, and governance contacts, to support effective decision-making, approvals, and day-to-day coordination throughout the engagement. The service provider will provide guidance on the roles and responsibilities necessary for project completion to guide the customer's identification of stakeholders.

Depending on the agreed delivery and deployment model, the service provider will require appropriate access to customer-managed environments, such as cloud tenants, development and testing environments, or on-premises infrastructure, in order to deploy, configure, and test the solution. Access requirements, permissions, and security controls are agreed in advance and provisioned in accordance with the customer's information security policies and the principle of least privilege.

Any additional technical prerequisites, such as network connectivity, identity integration, data availability, or third-party services, are identified and agreed during the onboarding phase 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 solution and under the service provider's responsibility, remediation will be undertaken at no additional cost to the customer. This includes investigation, fault isolation, and corrective action necessary to restore normal service operation in a timely manner, subject to the agreed service scope and acceptance criteria.

Where an outage or issue arises from factors outside the agreed scope of responsibility, such as changes to customer-managed infrastructure, third-party platform failures, data issues, or requests for enhancements or modifications, support may be provided under an agreed maintenance arrangement. Such support is delivered either through a retainer-based model or on a time-and-materials basis, as outlined in the after-sales support and maintenance terms.

Maintenance activities, including planned updates, patches, or enhancements, are scheduled in coordination with the customer wherever practicable to minimise disruption. Roles, responsibilities, escalation paths, and service boundaries for outage response and ongoing maintenance are defined per engagement to ensure clarity and effective incident management.

Hosting options and locations

AI and Generative AI solutions can be deployed within the customer's existing infrastructure or hosting environment, including customer-managed cloud platforms across any major provider or on-premises servers. In these scenarios, the service provider supports solution deployment, configuration, and integration within agreed scope, while the customer retains responsibility for the underlying hosting environment in accordance with the agreed shared responsibility model.

Where required, the service provider can also host the solution on behalf of the customer for an additional fee. Hosted deployments will utilise cloud-based infrastructure selected to meet the customer's functional, security, regulatory, and data residency requirements. The specific hosting provider, geographic location, 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, trained models, source code, configurations, and solution artefacts developed during the engagement. In most circumstances, the service provider acts solely as a data processor on behalf of the customer and does not retain customer data beyond what is necessary to deliver the services.

Upon service exit, all agreed data sets, models, software artefacts, and associated documentation are made available to the customer in mutually agreed, industry-standard formats to support continued operation, maintenance, or migration to alternative platforms or service providers.

Reasonable support for the extraction and transfer of data, models, and software assets is provided for a defined transition period, subject to the terms of the engagement. Following completion of the exit process, any residual customer data retained by the service provider is securely deleted or anonymised in accordance with agreed data retention schedules, security standards, and applicable legal or regulatory requirements.

Security

Security is embedded throughout the service lifecycle and is aligned with recognised information security standards, including ISO/IEC 27001, as well as applicable cloud provider shared responsibility models. Examples of this alignment include:

- **Information Security Governance**
  Security roles, responsibilities, and decision-making authority are defined for each engagement.
- **Risk-Based Security Controls**
  Security controls are selected and applied based on the nature of the service, data sensitivity, and deployment model.
- **Access Control**
  Access to systems, data, and environments is restricted to authorised individuals using role-based access controls and the principle of least privilege.
- **Data Protection and Encryption**
  Data is protected through encryption in transit and at rest where appropriate.
- **Monitoring, Logging, and Auditability**
  Security-relevant events are logged and monitored to support incident detection, investigation, and audit requirements.
- **Supplier and Shared Responsibility Management**
  Where third-party platforms or cloud providers are used, responsibilities for security controls are defined in accordance with shared responsibility models.
- **Information Lifecycle and Exit Management**
  Data handling, retention, and secure deletion on service exit are managed in accordance with defined procedures.

Appropriate technical and organisational security measures are applied based on the nature of each engagement. These may include identity and access management, encryption of data in transit and at rest, secure API and integration controls, monitoring and logging, and the maintenance of audit trails to support oversight and compliance.

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 and agreed for each engagement to ensure proportionate risk management and alignment with contractual, regulatory, and operational requirements.


TRIDENT
INTELLIGENT SOLUTIONS