

CUSTOM SOFTWARE DEVELOPMENT

Service Definition



19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTIONS

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

Contents

Service overview	2
Scope of services	2
Onboarding and engagement initiation	3
Service constraints	4
Service levels and support	4
After-sales support	5
Technical and client-side requirements	5
Outage and maintenance management	5
Hosting options and locations	5
Data access on exit	6
Security and governance	6

Service overview

The Custom Software Development service provides end-to-end design, development, deployment, and support of bespoke software applications tailored to client-specific business needs. The service covers full lifecycle delivery, from requirements gathering through design, development, testing, deployment, and ongoing maintenance.

Capabilities include:

- Design and development of web, mobile, and enterprise applications
- Integration with data platforms, analytics, BI, and AI/agent AI solutions
- Cloud-native, hybrid, or on-premises application deployment
- Application architecture and software engineering best practices
- Automated testing, CI/CD pipelines, and DevOps integration
- Security, governance, and compliance controls aligned with ISO/IEC 27001 and other regulatory frameworks
- Scalable, high-performance, and resilient software solutions

The service is delivered through structured, project-based or Agile engagements, ensuring alignment with business objectives, technical constraints, and operational requirements.

Scope of services

Software design and development

- Requirements gathering, user stories, prototypes/wireframes (where required), and functional specifications
- Solution architecture, design patterns, data model, API specs, integration design, and technical documentation
- Full-stack software development (frontend, backend, APIs, integrations)
- Tech stack agnosticism, integrating with the clients' preferred or existing technology stacks where appropriate
- Integration with data pipelines, analytics dashboards, AI/agent AI models, and third-party systems

- Scalable, modular, and maintainable software solutions

Cloud and DevOps integration

- Cloud-native or hybrid deployment strategies
- CI/CD pipeline design and automated build/deployment processes
- Infrastructure-as-Code (IaC) implementation for reproducible environments
- Monitoring, logging, and operational support

Quality assurance and testing

- Unit, integration, system, and user acceptance testing
- Automated testing frameworks for consistent quality assurance
- Security and vulnerability testing aligned with ISO/IEC 27001 and DevSecOps practices
- Contract-first design (e.g., Open API Spec), schema validation, automated linting

Security, compliance, and governance

- Role-based access controls, least-privilege principles, and secure coding practices
- Data protection and encryption at rest and in transit
- Alignment with regulatory frameworks and internal governance policies
- Auditability, traceability, and operational monitoring

Maintenance and support

- Bug fixes, performance optimisation, and minor feature enhancements
- Software upgrades, patching, and environment updates
- Knowledge transfer and documentation for ongoing operations
- Optional extended support for mission-critical applications

Onboarding and engagement initiation

Following contract agreement, a Delivery Manager and software development team are assigned. A kick-off workshop confirms scope, objectives, stakeholders, governance arrangements, and engagement logistics.



A Project Initiation Document (PID) or equivalent is agreed, defining scope, deliverables, timelines, roles, responsibilities, and quality governance arrangements.

Service constraints

- Delivery relies on access to client systems, stakeholders, and required development environments
- Application performance and functionality may depend on external integrations and data quality
- Cloud or on-premises deployment requires client-provided resources and platform configurations
- Compliance and security alignment require active client engagement

Service levels and support

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.

Support is tailored per engagement:

Standard Support: Remote assistance during business hours for bug fixes, troubleshooting, and operational guidance.

Enhanced Support: Extended business hours, proactive monitoring, and minor feature enhancements, with a named technical contact.

Premium Support: 24/7 coverage for mission-critical applications, proactive monitoring, rapid escalation, and a dedicated Software Delivery Lead.

Severity Classifications:

- **Severity 1 (Critical):** Production application outage; immediate response
- **Severity 2 (High):** Major functionality disruption impacting business operations
- **Severity 3 (Medium):** Partial functionality limitation or non-critical issues
- **Severity 4 (Low):** Minor queries, cosmetic issues, or enhancements

After-sales support

Following deployment, a formal handover includes all code, configurations, architecture documents, and operational procedures. Knowledge transfer sessions ensure client teams can maintain, monitor, and enhance the application.

Ongoing maintenance may include:

- Bug fixes, performance tuning, and minor feature updates
- Integration updates with AI, data, or analytics platforms
- Security patching and compliance alignment

Technical and client-side requirements

The client is responsible for:

- Access to development environments, source control, and infrastructure
- Identification of key stakeholders and subject-matter experts
- Policies and approvals for security, compliance, and operational governance
- Network connectivity, identity, and access integration

Outage and maintenance management

Planned maintenance, updates, or performance optimisations are scheduled to minimise disruption. Service-affecting issues attributable to deliverables are remediated at no additional cost. Issues outside agreed scope, such as third-party outages or client-managed changes, may be supported under separate agreements.

Hosting options and locations

Applications can be deployed in client-managed cloud or on-premises environments. The service provider can also host applications under agreed SLA and governance terms. Hosting selections are guided by functional, security, regulatory, and cost requirements.

Data access on exit

All source code, configurations, scripts, and documentation are delivered to the client upon completion. Any residual data or artifacts retained by the service provider are securely deleted or anonymised in accordance with agreed retention schedules and regulatory requirements.

Security and governance

Security and governance are embedded throughout the software lifecycle:

- Role-based access, least-privilege principles, and secure coding practices
- Encryption and data protection
- CI/CD auditability and operational monitoring
- Alignment with ISO/IEC 27001, regulatory requirements, and internal governance policies

Responsibilities are shared between the service provider, client, and any third-party service providers, with clear ownership defined per engagement.