Cielo Costa

SERVICE DEFINITION
Lot 2a: Compliance and Assurance Bespoke Application Development

| **Author**: Nicki Greene

| **Published**: 28th January 2026

Contents

1. Service Overview

This service provides the design, build and deployment of bespoke cloud-native applications directly into the customer's Azure environment. Applications are developed using modern frameworks, secure engineering practices and cloud platform services.

We specialise in delivering configurable solutions that support compliance, audit, assurance and governance workflows. Typical capabilities include obligation tracking, audit management, evidence repositories, structured workflows, corrective action tracking, dashboards and reporting. These elements are tailored to each customer's processes and deployed securely within their Azure tenant, ensuring full isolation and customer control over data, identity and infrastructure.

2. Service Scope

The service includes:

- Module identification and discovery to assess which compliance, audit or assurance accelerator best fits the customer's needs.
- Implementation and configuration of the selected module, including workflows, templates, permissions and data structures tailored to the customer's environment.
- Identification of additional customisations required to meet specific requirements (available for delivery via Lot 3 Cloud Support Services).
- Integration with existing systems through APIs or secure connectors to enable the module's features.
- Use of the customer's identity provider (for example Microsoft Entra ID) with MFA.
- Onboarding to the solution, including deployment, access setup, configuration guidance and documentation.
- Support and bug fixes during agreed delivery and support periods.

The service does not include:

- Hosting in a supplier-operated environment
- Provision of PSN, VPN or dedicated network services
- Customer-side Azure subscription costs

3. Technical Architecture

Applications are deployed entirely into the customer's chosen Azure region (typically UK or EEA).
Typical components may include:

- Azure App Services for client interfaces and APIs
- Azure Functions for workflow automation
- Azure Storage and Cosmos DB or SQL Database for audit, evidence and action data
- Configurable templates for audits, obligations or workflows
- Application Insights for telemetry, performance and diagnostics
- Managed Identities and Entra ID authentication

The architecture is modular, allowing features such as audits, evidence, actions or dashboards to be extended over time. All components run within the customer’s tenant to ensure full separation and security.

4. Onboarding

Onboarding includes:

- Kick-off and requirements confirmation
- Access setup to the customer’s Azure environment
- Discovery of compliance, audit or assurance workflows and data structures
- Architecture and design workshops
- Agreement of configuration templates and workflow patterns
- Environment preparation guidance
- Knowledge transfer on deployment, configuration and administration

User guides and handover documentation are supplied as part of onboarding.

5. Offboarding and Exit Support

At contract end, customers retain ownership of all resources in their Azure environment.
We provide guidance to support:

- Exporting data from databases and storage in JSON or CSV
- Extracting logs or telemetry if requested
- Safe removal of supplier access
- Handover of deployment pipelines and artefacts

Additional support (such as environment decommissioning or migration) can be delivered under a separate agreement.

6. Service Levels

Availability

Because the service runs entirely in the customer's Azure tenant, availability is governed by Microsoft's underlying platform SLAs.
For any supplier-hosted components (for example a centrally hosted API), we target 99.5% availability on a best-efforts basis.

Performance

Performance depends on the customer's selected Azure configuration. We design applications following cloud-native best practice to ensure scalability and responsiveness.

Support Hours

Standard support is provided Monday to Friday, 9am–5pm (UK time), via Zendesk or email.
Enhanced support can be arranged under additional commercial terms.

7. Backup, Restore and Disaster Recovery

As applications are hosted in the customer's Azure environment, backup and DR behaviour follows the customer's Azure policies.
Common Azure defaults include:

- Automatic database backups
- Application restore points
- Availability zone redundancy (when enabled)

We advise on appropriate configuration and can help customers adopt suitable DR patterns.

8. Outage and Maintenance Management

For customer-hosted deployments:

- Outages and platform maintenance notifications are received directly via Azure.
- Customers manage infrastructure-level maintenance windows.

For any centrally hosted supplier components:

- We notify customers of planned maintenance by email.
- Critical incidents are escalated to technical leads immediately.
- For major incidents, we provide a formal RCA.

9. Access and Authentication

User authentication is performed through the customer's identity provider (for example Microsoft Entra ID).
Supported authentication methods include:

- Identity federation (OpenID Connect / OAuth2)
- MFA enforced through the customer's IdP
- Username/password (as enforced by the customer's IdP)

Management and administrative access is role-restricted and protected using MFA and least-privilege principles.

10. Management Interface Access Controls

Access to management interfaces is restricted to authorised staff with defined operational roles.
All access is logged and time-limited, and support channels (for example Zendesk) use permission-controlled access to ensure appropriate handling of customer information.

11. Audit and Logging

Audit logs, telemetry and system activity data are captured through Azure's native monitoring tools (for example Application Insights and platform logs).
Customers may access logs directly from their own Azure subscription.
Where logs are held in supplier-hosted components, customers may request audit information through support.
Major incidents include a formal Root Cause Analysis (RCA).

12. Data Separation

Each customer's deployment runs entirely within their own Azure tenant, ensuring full separation of data, compute and storage from other customers.
No customer data is shared or co-located.

13. Security Approach

Our security practices include:

- Cyber Essentials Plus certified organisation
- Secure development lifecycle with code review and dependency scanning
- Annual external penetration testing or after significant change
- TLS 1.2+ encryption for all components
- Azure-native security (RBAC, encrypted storage, managed identities)
- Supplier-defined vulnerability and incident management processes

14. Service Constraints

- Maintenance windows for centrally hosted supplier components are notified in advance.
- Customisation is limited to configuration, workflow and role management.
- Code-level modifications require additional commercial development.
- Performance and availability depend on the customer's Azure infrastructure.

15. Technical Requirements

Customers require:

- An active Azure subscription
- A configured identity provider (for example Microsoft Entra ID)
- Administrative access to deploy resources
- Appropriate network and governance policies to host the solution
- An active Microsoft 365 tenancy (if using SharePoint or M365 integration)