

SERVICE DEFINITION

Lot 3: Cloud Support Services



| **Author:** Nicki Greene

| **Published:** 28th January 2026

Contents

1. Service Overview	3
2. Service Scope.....	4
3. Onboarding	6
4. Offboarding and Exit Support	7
5. Service Levels.....	8
6. Aftersales Support	9
7. Backup, Restore and Disaster Recovery	11
8. Outage and Maintenance Management	11
9. Security Approach.....	13
10. Hosting Options and Locations.....	15
11. Service Constraints	15
12. Technical Requirements.....	16

1. Service Overview

This service provides ongoing Cloud Support and Continuous Improvement across the customer's Microsoft cloud estate, ensuring that services, applications and underlying components remain stable, secure, up-to-date and aligned with operational requirements. It covers both reactive and proactive support activities, ranging from troubleshooting and service requests to planned improvements and optimisation.

The scope of the service is intentionally broad so customers can use Lot 3 for a wide range of Cloud Support outcomes. Examples include:

- Configuration and administration of Microsoft 365 services (such as Entra ID, Exchange Online, Teams, SharePoint Online, and Microsoft security and compliance settings).
- Creation, enhancement or restructuring of SharePoint sites, information architecture, document management and collaboration solutions.
- Support, maintenance and enhancement of Power Platform solutions including Power Apps, Power Automate flows and Power BI datasets/dashboards.
- Azure platform support, including troubleshooting, configuration, optimisation and ongoing operational management of Azure App Services, Functions, Storage and other cloud components.
- Assistance with systems integration, business process automation, data migration and general cloud solution maintenance.
- Third-line support for Microsoft 365, Azure and custom applications.
- Continuous improvement activities such as feature enhancements, optimisation, refinement of workflows, new modules or extended reporting.

Where customers have a solution delivered under Lot 2a, Lot 3 provides the route to extend or enhance that solution — for example, adding new workflows, refining user experience, creating reporting dashboards, introducing new modules, improving integrations, or delivering operational updates and improvements aligned to evolving business needs.

2. Service Scope

This service provides flexible Cloud Support and Continuous Improvement across the customer's Microsoft cloud ecosystem. It is designed to provide 3rd line support for day-to-day operations, resolve issues, implement configuration changes, and deliver enhancements that improve productivity, stability and value from cloud services. Typically, it provides specialist support in addition to a managed service. The scope is intentionally broad to accommodate a wide range of customer requirements.

Included in this service

- Incident resolution and troubleshooting for Microsoft 365, Azure services, custom applications, Power Platform solutions, and integrations.
- Service request fulfilment, including configuration changes, permission updates, environment adjustments, and advanced configuration changes.
- Microsoft 365 support and administration, such as Entra ID configuration, Teams management, SharePoint permissions, Exchange Online settings, compliance centre assistance and general platform optimisation.
- SharePoint site creation and evolution, covering information architecture, content organisation, page design, site configuration and governance updates.
- Power Platform support, including creation, updates and enhancements for Power Apps, Power Automate flows and Power BI datasets, dashboards and refresh processes.
- Azure platform support, including configuration assistance, optimisation, diagnostics, monitoring, and operational improvements to services such as App Services, Functions, Storage and Databases.
- Continuous Improvement (CI) tasks such as usability improvements, workflow refinements, enhanced reporting, integration updates, dependency refreshes, small development items and architecture optimisation.
- Operational housekeeping, including certificate and key renewal, version updates, performance reviews and security posture improvements.
- Service delivery management, including monthly reporting, ticket reviews, trend analysis and recommendations for improvement.
- Enhancement and extension of Lot 2a solutions, including new workflows, additional functionality, extended reporting, UI improvements or deployment of new modules.

- Liaison with Microsoft and other third party providers on the customer's behalf where required.

Not included in this service

- 1st and 2nd line support
- Hosting or management of environments outside the customer's Microsoft cloud tenant.
- Any Microsoft features, services or previews that are not generally available.
- Full DR or backup management unless explicitly requested and scoped.

3. Onboarding

Onboarding introduces the customer and their solutions into the Cloud Support service and establishes the processes, access, and documentation required to begin 3rd-line support and continuous improvement activities. The onboarding approach ensures a smooth transition from project delivery or a previous support arrangement into an ongoing support relationship.

Onboarding includes:

- **Service transition activities** to understand the customer's environment, cloud configuration and the solutions in scope for support.
- **Review of existing documentation**, including architecture diagrams, configuration notes, solution overviews, release history and any known issues or dependencies.
- **Technical access setup**, including required permissions to Microsoft 365, Azure services, SharePoint, Power Platform environments, custom applications, integrations and any associated tools.
- **Validation of support readiness**, confirming that the solution meets the requirements for 3rd-line support, including appropriate documentation, access paths, environments and configuration clarity.
- **Knowledge transfer sessions** with relevant customer teams or the delivery team (for newly delivered Lot 2a solutions) to ensure a clear understanding of architecture, workflows, dependencies and operational considerations.
- **Agreement of communication channels**, escalation paths, service contacts and ticket-raising process for incidents, service requests and continuous improvement items.
- **Initial environment review**, identifying potential risks, dependency updates, configuration gaps or recommended improvements before support begins.
- **Hypercare period**, where required, to stabilise newly delivered or recently updated solutions before they enter standard support operations.
- **Handover of onboarding materials**, including support guide, escalation points, availability commitments, ticketing responsibilities and service overview.

Onboarding ensures that all supported services — whether Microsoft 365 components, SharePoint structures, Power Platform solutions, Azure services, or custom applications — are correctly understood, accessible and ready for successful 3rd-line support.

4. Offboarding and Exit Support

Offboarding ensures a controlled and secure transition when the service ends or when the customer chooses to move to another support arrangement. As all supported solutions and services operate within the customer's own Microsoft cloud environment, the customer retains full ownership and control of all data, configurations, and cloud resources throughout the contract.

Offboarding includes:

- **Support termination planning**, ensuring clarity on timelines, responsibilities and cut-over arrangements.
- **Handover of relevant documentation**, including configuration notes, architectural information (where held), CI backlog summaries, environment observations, and any applicable technical artefacts created as part of the service.
- **Export of ticket history**, service reporting, CI recommendations, and aggregated support insights upon request.
- **Guided transition**, supporting the movement of 3rd-line responsibilities to another provider or internal team, including knowledge-transfer sessions where required.
- **Safe removal of Cielo Costa access**, including the revocation of Azure roles, Microsoft 365 permissions, SharePoint admin rights, Power Platform environment access, and any system-specific permissions granted for the purposes of support.
- **Confirmation of closure activities**, including validation that all agreed actions, updates, and outstanding issues have been addressed or handed over.

As all environments and data reside in the customer's Microsoft cloud tenant, no customer data is removed, hosted, or controlled by Cielo Costa. If additional offboarding activities are required (such as migration support, solution decommissioning or extensive knowledge-transfer programmes), these can be arranged under Lot 3 as additional support services.

5. Service Levels

Service Levels define how support is delivered, how quickly customers can expect responses, and the performance expectations for the Cloud Support service. This service operates exclusively at the **3rd-line level**, focusing on complex, technical tasks that require specialist expertise across Microsoft 365, SharePoint, Power Platform, Azure and custom cloud applications.

Support Hours

Standard support is available **Monday to Friday, 9am–5pm UK time**, excluding UK bank holidays.

Support outside these hours can be arranged under separate commercial terms.

Response and Resolution Targets

The following targets apply to all supported solutions:

- **First Response:** 90% of incidents and service requests responded to within **two working days**.
- **Resolution / Proposed Resolution:** 90% of incidents and service requests resolved, or a proposed resolution provided, within **four working days**.

Resolution SLAs may be paused where customer input is required (for example, confirmation, data, access or approval).

Continuous Improvement items or enhancement requests are not subject to SLA timeframes and will be prioritised based on customer direction.

Major Incident Handling

Critical or high-severity issues follow a **Major Incident process**, including:

- immediate escalation to senior technical staff
- ongoing updates to customer stakeholders
- accelerated investigation and remediation
- a **formal Root Cause Analysis (RCA)** for major incidents

Performance

Performance of customer-hosted services depends on the configuration and capacity of the customer's Microsoft cloud tenant.

Where performance issues relate to Azure or Microsoft 365 platform behaviour, we investigate and escalate to Microsoft as required.

Availability

As all supported services run within the customer's Microsoft cloud environment, platform-level availability is governed by the relevant Microsoft SLAs.

Where Cielo Costa operates any supplementary components for monitoring or diagnostics, availability is provided on a **best-efforts basis**.

Service Reporting

Monthly service reporting may include:

- ticket volumes and trends
- SLA performance
- CI activity progress
- recommendations and improvement opportunities
- major incident summaries (where applicable)

6. Aftersales Support

After-sales support is provided through our structured 3rd-line Cloud Support and Continuous Improvement service. This ensures customers continue to receive expert assistance and enhancements long after a system or feature has been deployed. The service provides ongoing operational assurance and sustained value across the customer's Microsoft cloud ecosystem.

Ongoing support services

Following onboarding, Cielo Costa provides continued 3rd-line support for the applications and cloud services in scope. This includes advanced troubleshooting, configuration changes, optimisation and assistance with issues that cannot be resolved by first- or second-line teams.

Continuous Improvement (CI)

Customers may request enhancements, refinements or optimisations at any time.

Continuous Improvement activities include:

- workflow changes
- performance tuning
- usability or UI improvements
- enhancements to SharePoint, Power Apps, Power Automate or Azure components

- integration updates
- reporting extensions
- small development tasks or logic updates

All CI items are triaged, estimated and scheduled in collaboration with customer stakeholders.

Ticketing and communication

Customers raise support needs via agreed channels (typically email or a ticketing portal). Updates are provided throughout the lifecycle of incidents, service requests and CI items, with escalation paths agreed during onboarding.

Service reviews and reporting

Regular service reviews are provided to maintain clear visibility of service performance and upcoming needs. These may include:

- ticket volumes and SLA performance
- analysis of trends and recurring issues
- review of completed and upcoming CI work
- recommendations for improvement
- updates on risks, dependencies or environment changes

Post-deployment support for Lot 2a solutions

Solutions delivered under Lot 2a can be extended, supported or enhanced through this service. After-sales support includes:

- stabilisation after release
- technical investigation of issues
- refinements to workflows, UI or performance
- new modules or feature extensions
- adjustments based on live usage feedback

Customer empowerment

Where customers wish to take on more configuration or platform ownership, we provide knowledge-transfer sessions and guidance as part of after-sales support.

7. Backup, Restore and Disaster Recovery

As all supported solutions operate within the customer's own Microsoft cloud tenant, responsibility for backup, restore and disaster recovery (DR) rests with the customer's Microsoft 365 and Azure configuration. This service provides **3rd-line technical support, guidance and improvement activities**, rather than performing direct backup or DR operations on the customer's behalf.

Our role includes:

- **Advising on appropriate backup and retention configurations** for SharePoint, Exchange Online, OneDrive, Power Platform environments, and Azure services.
- **Identifying gaps or risks** in existing backup, retention or business continuity settings during routine support or onboarding.
- **Supporting customers in configuring or improving** backup policies, data retention, soft-delete and recovery options within their Microsoft cloud environment.
- **Assisting with restore activities** where these require advanced technical input (such as restoring Power Apps components, SharePoint lists/libraries, Azure resources or configuration elements).
- **Supporting DR rehearsals**, failover planning, dependency reviews and readiness testing as part of Continuous Improvement.
- **Providing guidance** on how customer environments can align to Microsoft's resilience and availability recommendations.
- **Escalating platform-level issues to Microsoft**, where backup, restore or DR behaviour depends on Microsoft 365 or Azure internal operations.

Backup and DR entitlements for customer-hosted services are ultimately governed by Microsoft platform capabilities and the customer's selected configuration. Where customers require enhanced backup or DR solutions, extended support can be provided through additional scoped work under Lot 3.

8. Outage and Maintenance Management

Outage and maintenance management defines how service-affecting events are handled and how planned changes are coordinated to minimise disruption. As all solutions run within the customer's Microsoft cloud tenant, platform-level availability is governed by Microsoft. Our role at 3rd-line is to diagnose complex issues, coordinate remedial actions, communicate clearly, and implement safe technical changes within the customer's environment.

Unplanned outages (Incidents)

- **Detection & triage:** When a service-affecting issue is reported or detected, we perform advanced diagnostics, identify likely root causes, and confirm affected components.
- **Coordination:** We collaborate with customer stakeholders and, where necessary, liaise with Microsoft or other vendors to restore service.
- **Communication:** We provide timely incident updates to nominated contacts throughout the lifecycle of the outage.
- **Recovery & validation:** We implement fixes, validate recovery and monitor for recurrence.
- **RCA for major incidents:** A formal Root Cause Analysis is produced for major incidents, including corrective actions and recommendations.

Planned maintenance (Changes)

- **Change governance:** All 3rd-line maintenance and configuration changes follow agreed change and release processes, including risk assessment, approvals and, where appropriate, pre-change testing.
- **Maintenance windows:** Changes are scheduled in customer-approved windows to reduce business impact; emergency changes may be executed outside windows with expedited approval.
- **Pre-production testing:** Where feasible, changes are tested in non-production environments before release.
- **Notification:** Planned works are communicated in advance with scope, impact, timings and rollback plans.
- **Post-change review:** We verify success criteria, monitor for issues and document the outcome.

Customer responsibilities (shared model)

- Maintain a **change calendar** and nominate approvers for change requests.
- Provide **access and test environments** where pre-change validation is required.
- Inform us of **planned business events or freezes** that could affect maintenance scheduling.
- Ensure **licensing, capacity and governance policies** support the intended change.

Technical housekeeping

- Proactive tasks (e.g., **certificate/secret rotation**, dependency and API version updates, telemetry improvements) are planned and executed as part of Continuous Improvement to reduce risk of service disruption.

Platform-level events

- For Microsoft 365 or Azure platform incidents outside customer control, we assist with **impact assessment**, **workarounds** and **escalations**, providing status updates until normal service is restored.

After-hours and emergency work

- Out-of-hours maintenance or emergency work can be arranged under separate commercial terms; communications and approvals are handled through the agreed major-incident/change processes.

9. Security Approach

Security underpins all aspects of the Cloud Support service. As Cielo Costa operates exclusively at the 3rd-line support level within the customer's Microsoft cloud environment, our security model ensures that access, data, and administrative activity are handled safely and in accordance with industry best practice and the customer's own governance controls.

Security certification

- Cielo Costa is a **Cyber Essentials Plus certified** organisation, demonstrating that our systems and processes meet the UK Government's standard for secure configuration, access control, malware protection, and vulnerability management.

Access security

- All access to customer environments uses **Multi-Factor Authentication (MFA)** enforced by the customer's identity provider (such as Microsoft Entra ID).
- Access follows strict **least-privilege principles**, with permissions granted only for the duration and scope required to perform specific 3rd-line support activities.
- Administrative access is **time-limited**, monitored and removed as part of offboarding or after specific tasks are completed.
- No customer credentials are stored or retained by Cielo Costa.

Data security

- All supported services and data remain within the **customer's Microsoft cloud tenant**.
- Cielo Costa does **not** extract, store, replicate or otherwise hold customer production data.
- Any diagnostic information temporarily captured during troubleshooting is deleted once the ticket or activity is complete.
- File transfers or sensitive information exchanges follow secure protocols agreed with the customer.

Operational security

- All configuration changes, fixes and enhancements follow agreed **change and release processes**, ensuring secure execution and full auditability.
- Logging and auditing of privileged access are performed via the customer's Microsoft cloud platform.
- Our processes include **root cause analysis** for major incidents, with identified corrective actions implemented through Continuous Improvement where appropriate.

Vulnerability management

- Potential security issues are identified through ongoing monitoring, dependency checks, secure development practices, and Azure/Microsoft 365 platform alerts.
- High-severity vulnerabilities are escalated immediately and managed using our internal incident and change processes.
- Security improvements and best-practice recommendations are incorporated into Continuous Improvement activities.

Secure development and engineering practices

- For enhancements or fixes requiring code changes, Cielo Costa follows a secure development lifecycle involving code review, dependency scanning, controlled release processes and pre-deployment testing where applicable.

Platform-level security

- Customers benefit from the underlying security of Microsoft 365 and Azure, including data encryption at rest and in transit, role-based access controls, secure identity management and continuous platform hardening.

Customer responsibilities

- The customer retains responsibility for platform-level configurations, licensing, conditional access policies, device security and tenant governance.
- The customer is responsible for informing Cielo Costa of any internal policy changes or new compliance requirements affecting access or security posture.

10. Hosting Options and Locations

All services supported under this Lot are hosted entirely within the customer's Microsoft cloud tenant. Cielo Costa provides no hosting services under this Lot

11. Service Constraints

The Cloud Support service operates within defined boundaries to ensure safe, controlled and effective delivery of 3rd-line support and continuous improvement. These constraints clarify what can and cannot be delivered within the scope of this Lot 3 service.

3rd-line support only

- This service provides **advanced 3rd-line support** for Microsoft 365, SharePoint, Power Platform, Azure services and custom cloud applications.
- **1st- and 2nd-line support activities**—such as routine triage, end-user questions, password resets, licence changes or basic administration—are out of scope and remain the customer's responsibility.

Change and maintenance governance

- All configuration updates, fixes and improvements requiring environment changes follow the customer's **approved change process**.
- Emergency work is subject to accelerated approval but still follows agreed governance.
- Maintenance windows must be agreed in advance and scheduled to minimise disruption.

Customisation and enhancement boundaries

- Lot 3 supports **configuration changes, enhancements and small development items**, but does not deliver full-scale projects or extensive new functionality (these require a separate statement of work).

- Enhancements to applications delivered under **Lot 2a** can be made under Lot 3, but significant architectural changes or new modules may require separate scoping.

Environment requirements

- The customer is responsible for ensuring the **Microsoft cloud environment is correctly licensed**, governed and operational.
- Cielo Costa relies on the customer providing **appropriate admin access**, test environments and required permissions.

Platform limitations

- Support is dependent on the availability and behaviour of Microsoft 365 and Azure services; global platform outages or degradation are outside the control of Cielo Costa.
- Features still in **Preview** or not in **General Availability** cannot be supported.

Scope of supported technologies

- Support is provided only for **in-scope solutions** that have been formally onboarded.
- Third-party systems or integrations not documented during onboarding may require additional assessment before support can be offered.

Customer responsibilities

- The customer must provide timely approvals, access, information and clarifications required to progress support or CI work.
- Failure to provide access or required details may pause SLA timers and delay resolution.

Optional tooling and monitoring

- Proactive monitoring, dashboards or custom tooling are implemented only where agreed as part of Continuous Improvement and are not provided by default.

12. Technical Requirements

To deliver effective 3rd-line Cloud Support, certain technical prerequisites must be in place within the customer's Microsoft cloud environment. These requirements ensure

that Cielo Costa can investigate issues, implement changes, and deliver continuous improvement safely and securely.

Microsoft 365 environment requirements

- A functioning Microsoft 365 tenant with the relevant services licensed and enabled (such as SharePoint Online, Teams, Exchange Online, Power Platform and the Microsoft 365 admin centre).
- Appropriate administrator roles available for assignment (for example: SharePoint Administrator, Teams Administrator, Exchange Administrator, Power Platform Administrator, Compliance Administrator, or equivalent).
- Ability to grant delegated or time-limited administrative access for 3rd-line support activities.

Azure environment requirements

Where Azure services or custom applications are in scope, customers must provide:

- Access to the Azure tenant and relevant subscriptions/resource groups.
- A minimum of contributor-level permissions (or equivalent custom role) for affected resources to support investigation, configuration or CI activities.
- Access to relevant Azure services such as App Services, Functions, Storage Accounts, Key Vault, Databases, API Management or other components being supported.

Power Platform requirements

Where Power Apps, Power Automate or Power BI are part of the service scope:

- Access to the relevant environments (Dev/Test/Prod as applicable).
- Permission to view and modify apps, flows, connectors, data sources and solution components.
- Admin centre access sufficient for environment insights, DLP policy review and troubleshooting.

SharePoint and collaboration requirements

- Access to SharePoint Online admin tools and affected site collections.
- Ability to modify site structures, permissions, metadata, content types and governance settings where needed.

Identity and access prerequisites

- Customer-managed identity provider such as Microsoft Entra ID.

- MFA enforced for all administrative access (supplier and customer).
- Ability to assign and revoke privileged roles as required for support.

Networking and governance

- Any required allow-listing, firewall rules or conditional access policies must be in place to permit secure support access.
- Where integration points or APIs are supported, customers must provide access details, secrets, certificates or connection information securely.

Service desk and engagement requirements

- Defined points of contact for technical approval, change control and service escalations.
- Agreed ticket-raising process and communication channels.
- Access to documentation, architectural diagrams, test environments or previous release history where available.

Customer responsibilities

- Maintain licensing and governance of their Microsoft cloud environment.
- Provide timely approval, information and access needed to progress 3rd-line support or Continuous Improvement work.
- Ensure any dependent third-party systems remain operational and accessible.