cloud bridge

AWS Platform Management Core

Service Description

August 2025

aws PARTNER Advanced Tier Services

Document Control

Author:	Philip Reeve
Date created:	15/01/2024
Classification:	Public
Document type:	Service Description

Version	Modified Date	Description	Modified By
V0.1	15/01/2024	Initial draft	Philip Reeve
V1.0	30/01/2024	Initial release	Philip Reeve
V1.1	15/03/2024	General updates	Philip Reeve
V1.2	01/10/2024	Updated monitoring solutions, added RACI matrix to Appendix	Philip Reeve
V1.3	13/06/2025	Updated terms for Onboarding on Section 6	Caithlyn Santos
V1.4	18/08/2025	Major updates to several sections	Philip Reeve

Table of Contents

1 Overview

Our core Managed Service, Platform Management Core, epitomises our mission to seamlessly integrate with your team and enhance your AWS journey. Our service is crafted to deliver transformative outcomes—maximising your efficiency, empowering your team, simplifying complexities, and providing flexible financial options.

2 Scope of Core Management

To provide clarity on the boundaries of Platform Management Core, we define a standard scope of AWS services that fall under day-to-day management. These are the foundational services most commonly deployed across customer environments and represent the baseline of what we manage within this service.

A full list of in-scope services, along with explicit exclusions, is available in **Appendix – In-Scope Services**. Customers should review this carefully to ensure it aligns with their environment. Any services outside this scope can be managed under a separate Statement of Work (SOW) or extended managed service.

2.1 Monitoring & Alerting

We understand the importance of maintaining visibility and control over your AWS workloads. Our monitoring solutions provide flexible options to meet your unique needs, ensuring you can confidently manage your cloud environment. We offer two tiers of monitoring: a native AWS option using built-in tools like Amazon CloudWatch, and an enhanced premium add-on featuring advanced capabilities through a third-party product.

We focus on monitoring and prioritising your critical production workloads as standard.

2.2 Native Monitoring

Our default monitoring solution leverages AWS-native tools to provide comprehensive visibility into your infrastructure and application performance. By utilising Amazon CloudWatch, we deliver real-time monitoring of metrics, logs, and alarms across your AWS resources, enabling proactive management and faster incident resolution.

Alerts generated by CloudWatch are automatically sent to our ITSM ticketing solution, where they are picked up by our support engineers for prompt investigation and response. This integration ensures seamless incident management, keeping your AWS environment secure and optimised without the complexity of additional software.

See Appendix for standard alarm configurations.

2.2.1 Public Website Availability Monitoring

In addition to native CloudWatch monitoring, our standard service includes **basic availability checks** for customer-facing websites and web applications. We use lightweight third-party tools to perform HTTP(S) checks from multiple locations, ensuring your endpoints remain reachable and responsive.

Alerts generated from these checks are automatically integrated into our service desk for investigation and response, helping to minimise downtime and maintain user confidence.

This standard capability focuses on endpoint availability only. More advanced synthetic transaction monitoring and in-depth application performance observability are available under our Enhanced Observability (System Operations Suite).

2.3 Enhanced Observability (System Operations Suite)

Our Enhanced Observability service, delivered as part of our **System Operations suite**, provides deep insight into your AWS platforms and infrastructure. This capability is **powered by leading third-party observability vendor technologies**, giving you advanced visibility well beyond native AWS monitoring.

We can deliver:

- **24/7 monitoring** of AWS platforms and infrastructure with proactive detection of potential issues.
- **Comprehensive observability** across compute, containerised environments (ECS, EKS, Kubernetes, Docker), and key application workloads.
- **In-guest OS and application monitoring**, covering metrics such as SQL performance and system health.
- **Custom dashboards** that present health and performance metrics most relevant to your environment.
- **Web and application availability checks**, including synthetic transactions to simulate user behaviour and validate response times, authentication, and content delivery.

This enhanced layer of monitoring ensures we can detect and resolve issues rapidly, helping to safeguard availability, performance, and user experience across your AWS estate.

2.4 AWS Incident and Change Management

Cloud Bridge provides a robust support system capable of managing a wide range of requests, from urgent incidents to general advice and planned change requests. Our comprehensive support desk system ensures that every issue is addressed promptly and efficiently, minimising impact on your business operations. Our proactive approach not only resolves incidents quickly but also analyses patterns to prevent future problems. We maintain a transparent and efficient change management process to ensure that all modifications are properly assessed, approved, and implemented without disrupting your services.

- **Efficient handling of incidents, general inquiries, and change requests**
- **Proactive problem management to prevent future issues**
- **Transparent and controlled change management process**

2.4.1 Service Responsibilities

Cloud Bridge provides AWS management under a **co-managed model**, where we act as an extension of your team while ensuring clear boundaries of responsibility. The following activities are included within Platform Management Core for the AWS services listed in **Appendix – In-Scope Services**:

What We Manage:

- **Provisioning and Decommissioning** – Creation and removal of supported AWS resources.
- **Configuration Changes** – Implementation of configuration changes (e.g., IAM policies, security groups, resource settings), always tracked through a logged change request.
- **Optimisation** – Application of performance, security, and cost optimisations identified through health checks and reviews. Where cost-saving opportunities are identified (e.g., resizing instances), we will provide recommendations and, where approved, implement them.
- **Backups** – Operation of AWS Backup for in-scope resources, ensuring backup policies are applied and monitored.

- **Incident Response** – Investigation and response to alerts or customer-reported issues. We respond both proactively (based on monitoring alerts) and reactively (based on tickets), and always document actions within our service desk.
- **Best Practice Guidance** – Ongoing advisory support aligned to the AWS Well-Architected Framework.

Boundaries of the Service

To protect both parties and ensure clarity, the following boundaries apply:

- **Effort Threshold** – Day-to-day management covers standard tasks and small-scale changes (e.g., deploying a new EC2 instance). **Larger projects, migrations, or architectural changes** (e.g., deploying an entire new application or re-architecting a workload) fall outside this scope and will be delivered under a Professional Services Statement of Work (SOW).
- **Risk Management** – Proactive changes are applied where they pose no risk of detrimental impact. Where changes could affect availability, performance, or security, we will first consult with the customer and follow change management procedures.
- **Co-Managed Model** – Customers may continue to manage their own AWS resources directly. We request that customers inform us of planned changes to avoid confusion with incident responses.
- **Customer Responsibilities** – Customers retain full ownership and responsibility for:
    - Application code, data, and business logic.
    - Governance and decision-making over IAM design, security policies, and compliance frameworks (Cloud Bridge can advise but does not own these decisions)

2.4.2 Global Service Desk and Engineering Coverage

Our service desk and engineering teams operate across multiple global regions, providing resilient 24/7 coverage. This is our **standard operating model** to ensure availability and continuity of service.

If your organisation has **compliance, regulatory, or contractual requirements** that mandate support staff be restricted to specific geographies, these requirements must be made clear during onboarding so they can be assessed and addressed appropriately.

2.5 Regular Health Checks

Regular health checks are a cornerstone of our service, ensuring that your AWS infrastructure remains optimised for performance, security, and cost efficiency. These reviews are instrumental in identifying any misalignments or improvements needed, helping to maintain a robust and efficient cloud environment.

- **Regular optimisation checks for performance, security, and cost**
- **Continuous improvements based on detailed assessments**

3 Service Exclusions

To establish clear boundaries and expectations for MS:Core, it is crucial to specify what is not included within the standard scope of our service offering. The following are exclusions from the MS:Core service package; however, should you require assistance in these areas, they can potentially be addressed under a separate Statement of Work (SOW), tailored specifically to meet these needs.

- **Support for Customer's Applications** – Routine support, troubleshooting, and maintenance for applications developed or managed by the customer are not covered.

- **DBA (Database Administrator) Related Services** – Database administration tasks such as performance tuning, schema management, and backup recovery are not included.
- **Architectural Design Revisions** – Major revisions or redesigns of existing architectural frameworks are excluded from the standard service package.
- **Implementation of New Infrastructure / Software** – The setup and implementation of new infrastructure or software platforms not identified during the initial service activation are not included.
- **General System Administration or Fault Resolution of Operating Systems Managed by the Customer** – General system administration tasks or troubleshooting and resolution of issues within customer-managed operating systems are not covered.
- **End User Desktop / Client Support, Application Installations, and Upgrades** – Support for end-user desktop environments, including client-side application installations and upgrades, is not included in MS:Core.
- **OS and Application Patching** – OS patching services are available under our Systems Operations Suite services; application-level patching is not covered.
- **Geography-Specific Staffing** – Our support model operates globally across multiple regions. Any requirement for support staff to be restricted to specific geographies for compliance, regulatory, or contractual reasons is excluded unless explicitly scoped and agreed separately.

4 Customer Responsibilities

To ensure the success of Platform Management Core, customers must actively participate in the onboarding and ongoing management process. Our service is most effective when customers invest time and resources to transfer knowledge, provide access, and collaborate closely with our teams.

- **Onboarding** – Support and assist our service delivery teams during onboarding to ensure a timely and smooth transition. This includes allocating appropriate subject matter experts (SMEs), completing prerequisite activities, and making key personnel available for workshops and knowledge transfer.
- **Knowledge Transfer and Handover** – Provide sufficient time and input to enable Cloud Bridge to assume management responsibility for in-scope services. Customers who invest in structured handover and offload management activity to us see significantly greater success with the service.
- **Engagement and Feedback** – Collaborate with your dedicated account manager and service delivery manager by providing necessary access, timely feedback, and specific requirements to help us refine and optimise service delivery. Provide timely responses to open tickets and requests until successfull closure.
- **Regular Cadence / Reviews** – Participate in regular service reviews (typically monthly), where performance, incidents, and optimisation opportunities are discussed and agreed.
- **Compliance with Guidelines** – Adhere to recommended practices and changes advised through regular reviews and health checks, ensuring the AWS environment remains aligned with operational, security, and compliance standards.
- **Change Transparency** – Inform Cloud Bridge of any customer-initiated changes made directly in the AWS environment. This avoids confusion and ensures our monitoring and incident response processes remain accurate and effective.

5 Onboarding

To ensure a consistent and scalable onboarding experience for customers transitioning into our Managed Services offering, we have implemented a standardised onboarding package that is aligned to the customer's monthly AWS spend. This approach allows us to provide predictable effort, clearly defined deliverables, and consistent onboarding quality.

5.1 Onboarding Overview

Each onboarding engagement includes a dedicated onboarding SME and project management oversight to guide the customer from pre-requisites through to service readiness and transition into Business-as-Usual (BAU) support.

The following onboarding components are included by default:

- **Pre-onboarding preparation and prerequisites:** Validation of access, documentation, and key contacts
- **Kick-off session** with the customer and service team, including timeline confirmation and role assignments
- **AWS security posture** producing an actionable remediation plan
- **Configuration of AWS support tooling**, such as alarm integrations and ticket escalation routing
- **CloudPulse dashboard setup** (where applicable)
- **Knowledge transfer session** and document hand-off
- **Deployment of 24/7 monitoring** based on our standard alarm configuration (see Appendix – Standard CloudWatch Alarms)
- **BAU task alignment and RACI setup**, including request, incident, and change management processes
- **Service readiness validation**, transition sign-off, and handover to the operations team
- **Onboarding project management**, including internal delivery tracking and reporting to the customer

The onboarding effort is strictly limited to AWS Platform Management onboarding and does not include workload-specific consulting, re-architecture, or third-party tooling integrations unless explicitly scoped.

The end-to-end onboarding process and its milestones will be discussed and agreed with the assigned Project Manager and Customer Success Lead.

5.2 Onboarding Exclusions

To maintain clarity and ensure the onboarding scope remains focused and deliverable, the following items are not included in the standard onboarding fee:

- Configuration of **custom monitoring solutions** beyond the defined standard alarm set
- Refactoring of **IAM roles**, permission boundaries, or trust policy realignments
- **Landing zone redesign** or remediation for multi-account structures
- Integration of **third-party tooling** (e.g., SIEMs, CMDBs, enterprise ticketing systems)
- Establishment of **compliance-specific baselines** (e.g., PCI, CIS, GxP)
- **Workload-level onboarding**, including deep dives into CI/CD pipelines, application infrastructure, or deployment pipelines

- **Onboarding of additional service lines** (e.g. Sentinel One and Commvault/Druva)

Where any of the above are required, they will be scoped separately through the Professional Services team and delivered under a separate Statement of Work (SOW).

6 Service Management

Our service management approach ensures a seamless, efficient, and effective operation of the Platform Management Core service. We provide a dedicated service manager who acts as your primary point of contact. This manager is responsible for overseeing the delivery of services, managing the service relationship, and ensuring that the service aligns with your strategic business objectives. Regular service reviews are conducted ton a monthly basis to discuss service performance, Cost optimisation, Security, Green Ops, upcoming changes, and continual improvement opportunities.

Through our Customer Success program, we aim to align our deliverables to provide a service which helps you achieve you business goals.

6.1 Reporting and Reviews

Cloud Bridge is committed to maintaining transparent communication and ensuring customers have full visibility of their managed AWS environment. Reporting and reviews form a key part of Platform Management Core.

6.1.1 Reporting Deliverables

Customers will receive structured reports that include:

- **Monthly Service Delivery Report**
    - Service actions completed in the reporting period.
    - Ticket activity (incidents, requests, changes) with trends and root causes.
    - Compliance against agreed SLAs and KPIs.
    - Security and operational notifications (e.g., AWS bulletins, end-of-support notices).
    - Patch levels and maintenance updates.
    - Health insights across compute, storage, networking, and database services.
    - Cost optimisation opportunities and sustainability metrics (where applicable).
- **Quarterly Trend & Optimisation Report**
    - Long-term service trends (recurring issues, recurring alerts).
    - Recommended optimisations (cost, security posture, performance).
    - Strategic improvements and roadmap actions.
- **Ad-Hoc Reports**
    - Additional extracts or analysis (e.g., compliance reporting, AWS health notifications, ticket snapshots) are available on request.

6.1.2 Review Cadence

Customers will receive regular reviews on the below cadence, unless requested otherwise:

- **Monthly Service Review Meeting** – Led by your Service Delivery Manager (SDM) or Customer Success Manager (CSM), focusing on the monthly report findings, actions, and upcoming changes.
- **Quarterly Strategic Review** – Broader review of service performance, trends, and alignment to business objectives.

Reports are typically delivered **in advance of scheduled review meetings** and distributed to named customer contacts via email.

7 Incident, Change and Problem Management

Tickets are raised through the following methods:

- Email: support@Cloud-Bridge.co.uk
- OOH case logging phone number: 01628 965200
- Cloud Bridge Web Portal: https://cloudservices-support.zendesk.com/hc/en-gb
- Chat via Cloud Bridge Web Portal: https://cloudservices-support.zendesk.com/hc/en-gb
- Automated email alerts: support@Cloud-Bridge.co.uk

7.1 Incident Management

Cloud Bridge operates a structured incident management process designed to minimise disruption and restore normal service operation as quickly as possible. All incidents are managed under a single framework, with categorisation aligned to SLA priority levels (P1–P4).

7.1.1 Scope of Incidents

Incidents cover a wide range of events that may impact your AWS environment. These include, but are not limited to:

- Alerts generated by monitoring tools (e.g., CloudWatch, third-party observability tools).
- Customer-reported issues (via the service desk, phone, or email).
- Proactively identified issues by Cloud Bridge engineers.

Incidents are categorised at logging in line with agreed SLA priorities (see Service SLAs).

7.1.2 Our Responsibilities

As part of incident management, Cloud Bridge is responsible for ensuring incidents are recorded, investigated, and resolved as efficiently as possible. This includes:

- **Logging** – Every incident is logged in our service desk (Zendesk) to ensure full auditability. Alerts from monitoring systems may be logged automatically.
- **Triage** – Engineers begin triage immediately upon picking up the incident, gathering context and isolating the issue.
- **Escalation Path** – Incidents follow a structured escalation chain:
    1. First/Second Line Engineer
    2. Team Lead
    3. Specialist Engineer
    4. Service Management
    5. Director-level escalation (if required)

- **AWS Escalation** – If the customer has Partner-Led Support or an active AWS support plan, Cloud Bridge will escalate to AWS on the customer's behalf and manage the case lifecycle.
- **Communication** – Customers receive regular updates in line with SLA priority (e.g., P1 hourly, P2 every 2 hours, etc.). Updates are logged in the ticket for traceability.
- **Resolution & Closure** – Once resolved, incident details, actions, and root cause are documented in the ticket.

7.1.3 Customer Responsibilities

To ensure incidents are prioritised and resolved effectively, customers are responsible for providing context and validation where needed. This includes:

- **Impact Identification** – Customers must identify the business impact of an incident when logging it to ensure correct prioritisation.
- **Validation** – Customers are requested to validate fixes, particularly where application testing is required. If no response is received, tickets will be closed after a pre-agreed timeframe, but can be reopened if further issues occur.
- **Transparency** – Customers should inform Cloud Bridge of planned changes or events that may trigger alerts, to avoid confusion with genuine incidents.

7.1.4 Scope Boundaries

Incident management focuses on AWS platform services under Platform Management Core. To ensure clarity of scope:

- Incident management covers **AWS services in scope of Platform Management Core only** (see Appendix – In-Scope Services). Customer applications and data are outside this scope.
- Recurrent or underlying issues identified during incident management may be raised as **Problem Management** items for root cause analysis. Where the resolution requires architectural redesign or significant project work, this will be delivered under a separate Professional Services Statement of Work (SOW).

7.2 Change Management

Cloud Bridge follows structured change management protocols to ensure that all changes to your AWS environment are controlled, approved, and documented. This protects service availability and ensures accountability for every modification.

7.2.1 What Constitutes a Change

A "Change" is defined as **any modification to your AWS environment**, including but not limited to:

- Configuration of an existing resource (e.g., updating a security group, resizing an instance, modifying IAM permissions).
- Addition of a new resource (e.g., deploying a new EC2 instance, adding a new S3 bucket).
- Deletion of an existing resource (e.g., decommissioning instances, removing a VPC component).

7.2.2 Our Approach to Change

- **Change Logging** – Every change is logged in our service desk (Zendesk), regardless of whether it is raised by Cloud Bridge or by the customer. This ensures a complete audit trail.
- **Approval Model** –
    - No change is applied without explicit customer approval **if it could have a detrimental impact on service availability, security, or costs**.

- For minor, low-risk activities, customers may agree to a set of **standard pre-approved changes** that do not require approval each time. Even in these cases, a change will always be logged.

- **Execution & Scheduling** – Approved changes are scheduled at appropriate times to minimise disruption. Stakeholders are notified in advance of significant changes.
- **Transparency** – Change records include details of the request, approvals, impact assessment, rollback plan, and validation steps.

7.2.3 Customer Involvement

- Customers are responsible for providing business impact context for requested changes, as they will always have the best understanding of their applications.
- Customers must validate changes where business-level testing is required (e.g., application testing after a database change).
- If required, Cloud Bridge can attend **Customer Change Advisory Board (CAB) meetings** to discuss and present changes. Attendance must be requested and booked in advance.

7.2.4 Scope Boundaries

- Day-to-day operational changes (e.g., adding a single instance, adjusting monitoring alarms) are included in Platform Management Core.
- Larger-scale initiatives (e.g., workload migrations, VPC redesigns, or deployment of full new applications) are outside this scope and will be delivered under a separate Professional Services Statement of Work (SOW).

7.3 Problem Management

Problem Management is an integral part of Platform Management Core. It focuses on identifying and eliminating the underlying causes of incidents to prevent recurrence, improving overall service quality and stability of your AWS environment.

7.3.1 Our Responsibilities

Cloud Bridge takes a proactive role in analysing incidents and implementing long-term fixes where possible. This includes:

- **Root Cause Analysis (RCA)** – Conducting thorough investigations into significant or recurring incidents to determine their underlying causes.
- **Problem Logging** – Ensuring all problems are formally logged in our service desk for traceability, whether identified by Cloud Bridge or raised by the customer.
- **Resolution & Workarounds** – Developing and implementing permanent fixes where possible, or documenting workarounds if resolution requires wider architectural changes.
- **Continuous Improvement** – Identifying trends across multiple incidents and recommending improvements to reduce the likelihood of future problems.

7.3.2 Customer Responsibilities

Effective problem management requires input from customers to provide context on the business impact and application behaviour. Customers are responsible for:

- **Providing Context** – Supplying relevant details about application dependencies and business processes that may influence problem resolution.
- **Validation** – Testing and confirming that implemented fixes or workarounds resolve the problem in their business context.

- **Collaboration** – Working with Cloud Bridge to approve and schedule any changes arising from problem investigations.

7.3.3 Scope Boundaries

Problem management within Platform Management Core is limited to AWS services in scope of this service. To ensure clarity of responsibility:

- Problems identified at the **application or data layer** remain the responsibility of the customer.
- Problems that require **major architectural redesign or project work** will be flagged for Professional Services delivery under a separate Statement of Work (SOW).

8 Service Level Agreement (SLA)

The priority levels which drive the SLAs are based on the impact to the business and its users.

8.1 Response SLA

Cloud Bridge provides **response SLAs** (time to acknowledge and begin working on an incident) but not **fix SLAs**. Due to the varied and complex nature of AWS environments, resolution times cannot be guaranteed. Our commitment is to engage promptly, apply appropriate resources, and provide regular updates until resolution.

	Incident	Change/Request	Problem
Ticket Logged	15 mins	15 mins	
P1 – Urgent(*)(**)	15 mins	30 mins	1 hour updates
P2 - High(**)	1 hour	1 hour	2 hour updates
P3 - Medium(**)	4 hour	4 hour	4 hour updates
P4 - Low(**)	12 hour	12 hour	12 hour updates

**To ensure the fastest possible response, any P1 incident should be logged by telephone or immediately followed up with a telephone call. This guarantees that our engineers are engaged without delay.*

***P1 (Urgent) and P2 (High) incidents are measured against SLA targets on a 24/7 basis. P3 (Medium) and P4 (Low) incidents are measured against SLA targets only during Business Hours (Monday–Friday, 09:00–17:00 local time).*

8.1.1 SLA Category Description

Priority Level / Name	Description
Urgent	A service / system which is critical for day-to-day operations is unavailable. A significant number of staff members are not able to perform their functions. The incident affects a large number of customers. The incident has the potential for major financial loss or damage to the organisation's reputation.

High	One or more departments is affected. A service / system which is significant for day-to-day operations is unavailable. The incident's sphere of impact is expanding rapidly, or quick action may make it possible to limit its scope. Financial loss and damage to the organisation's reputation are possible. Time-sensitive work or customer actions are affected. The incident affects high-status individuals or organisations (i.e., upper management or major clients).
Medium	Only a small number of users are affected. None of the services lost are critical. Financial loss and damage to the organisation's reputation are limited in scope.
Low	The effects of the incident appear to be stable. Affected services are optional and used infrequently. Important or time-sensitive work is not affected. No critical services are involved, and there is little or no potential for financial loss or loss of reputation.

8.2 Escalation

For all technical related matters, the support team have clear escalation routes to their higher-level technical colleagues and also to our 3rd party suppliers with whom we have underpinning support contracts in place with.

Escalation routes and contact numbers for any issues the customer feels are not being progressed in line with their expectations will be provided to all customers and this will give them access to the Cloud Bridge management team within and outside of normal working hours.

8.3 AWS Compute Service Level Agreement

AWS will use commercially reasonable efforts to make the Included Services each available for each AWS region with a Monthly Uptime Percentage of at least 99.99%, in each case during any monthly billing cycle (the "Service Commitment"). In the event any of the Included Services do not meet the Service Commitment, you will be eligible to receive a Service Credit

Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for the individual Included Service in the affected AWS region for the monthly billing cycle in which the Unavailability occurred in accordance with the details found via the following link: https://aws.amazon.com/compute/sla/

9 Appendix – RACI

9.1 Service Delivery Management

PROCESS ID	SERVICE / ACTIVITY	MSP	Customer
	General		
1.1	Assign Service Delivery Manager to Customer	A, R	I
1.2	Schedule Monthly / Quarterly Cadence for Service Reviews	A, R	C
1.3	Attendance on Service Reviews	R	R
1.4	Monitor strategic initiatives	R	A
1.5	Recommend changes and enhancements to service portfolio	A, R	C
1.6	Participate in Customer Critical Incident Reviews as required	R	A
1.7	Vendor Management and Escalations (e.g. AWS, LogicMonitor etc)	A, R	C, I
	Service Reviews		
1.8	Conduct and lead Monthly / Quarterly Service Reviews	A, R	C, I
1.9	Create Service Reporting	A, R	I
1.10	Review current service delivery including SLAs/KPIs, Incident, Change, Request, Project status	A, R	C
1.11	Identify areas of unsatisfactory service	A, R	C
1.12	Develop improvement recommendations	A, R	C
	Service Level Management		
1.13	Monitor and report on Service Level compliance	A, R	I
1.14	SLA exception management (SLA suspension)	A, R	C
1.15	SLA breach escalation, analysis and mitigation	A, R	I
1.16	Customer feedback and improvement actions	A, R	C
1.17	SLA review and adjustments	A, R	I
	Customer Success Management		
1.18	Deliver elements of Customer Success Program	A, R	C
1.19	Perform Customer Satisfaction Survey	A, R	C

9.2 Event Management / System Reporting

PROCESS ID	SERVICE / ACTIVITY	MSP	Customer
	General		
2.1	Real-time Performance Monitoring (CPU, Memory, Disk, Network)	A, R	I
2.2	Automated alerts setup and management (LogicMonitor, StatusCake, AWS natvie)	A, R	C
2.3	Log collection and analysis	A, R	I
2.4	Service uptime monitoring	A, R	I

Event, Incident and Problem Management

PROCESS ID	SERVICE / ACTIVITY	MSP	Customer
	General		
3.1	Validate, log and track events / calls from authorised users / customers	A, R	I
3.2	Own issues and problems reported by authorised users	A, R	C, I
3.3	Route, transfer or ecalate events / calls into Incidents via relevant Support Personnel	A, R	I
3.4	Incident identification and logging	A, R	R
3.5	Incident categorisation and prioritisation	A, R	R
3.6	Initial assignment and triage	A, R	I
3.7	Notify requester of ticket status	A, R	I
3.8	Incident escalation management	A, R	C
3.9	Incident resolution	A, R	C
3.10	Problem identification and logging	A, R	C, I
3.11	Perform Root Cause Analysis for Problems	A, R	C, I
3.12	Remediation of Problems	A, R	C, I
3.13	Identify and remediate application Problems	I	A, R
3.14	Incident documentation and reporting	A, R	R

3.15	Event / Call / Incident Closure	A, R	C, I
3.16	Post-incident review	A, R	R
3.17	Knowledge Base updates	A, R	I

9.3 Change Management

PROCESS ID	SERVICE / ACTIVITY	MSP	Customer
	General		
4.1	Raise Change and gather requirements	I	A, R
4.2	Classify / Prioritise Change	I	A, R
4.3	Assume responsibility for Change Requests received via Customer CM Process	R	A
4.4	Review (risk /impact analysis) and plan Change Request in accordance with Customer CM Process	R	A, C
4.5	Support Customer Change Advisory Board (CAB) if required	R	A
4.6	Coordinate and as applicable test proposed changes prior to change approval.	R	C, I
4.7	Develop contingency or rollback procedures for planned changes	R	A
4.8	Review and accept contingency or rollback procedures for planned changes	A, R	R
4.9	Support Customer Change Advisory Board (CAB) if required	C, I	A, R
4.10	Approve Change within customer CM process	I	A, R
4.11	Change scheduling and communication	R	A, R
4.12	Change implementation	A, R	C, I
4.13	Post-Implementation Review	R	A
4.14	Emergency Change Management	R	A
4.15	Change rollback planning	R	A
4.16	Notice of upcoming Maintenance Window	C, I	A, R

9.4 Request Fulfilment

PROCESS ID	SERVICE / ACTIVITY	MSP	Customer
	Request Fulfillment Support		
5.1	Request submission	I	A, R
5.2	Receive, review and update Request	A, R	C, I
5.2	Authenticate Requester	A, R	C, I
5.4	Verify Requested Service	A, R	I
	Request Logging and Categorisation		
5.5	Request Logging	A, R	I
5.7	Request Categorisation	A, R	I
	Request Prioritisation		
5.8	Request Prioritisation	A, R	C, I
5.9	Request Escalation (if necessary)	A, R	C, I
	Request Actioning and Monitoring		
5.10	Request Actioning and Monitoring	A, R	I
5.11	Request Monitoring	A, R	I
	Request Closure and Evaluation		
5.12	Notify User of Fulfillment	A, R	I
5.13	Request Closure	A	C, I
	Standard Requests		
5.14	User access and permission management	R	A
5.15	Software installation and configuration	R	A
5.16	User account setup and deactivation	R	A
5.17	Simple change requests (e.g., password resets, user account updates))	R	A

9.5 Security Management

PROCESS ID	SERVICE / ACTIVITY	MSP	Customer
	Security Management		
6.1	Customer infrastructure security and/or establishing baseline for security compliance process as determined and agreed to during customer onboarding.	R	C
6.2	Monitoring malware on instances provisioned through the Change Management process	R	I
	Security Access Management		
6.3	Manage the lifecycle of users, and their permissions for local directory services, which are used to access AWS Managed Services	I	R
6.4	Operate federated authentication system(s) for customer access to AWS console/APIs	C	R
6.5	Accept and maintain Active Directory (AD) trust from AWS Managed Services AD to customer managed AD	C	R
6.6	During onboarding, create cross-account IAM Admin roles within each managed account	C	R
6.7	Secure the AWS root credential for each account	R	I
6.8	Define IAM resources for Managed Environment	R	C
6.9	Manage privileged credentials for OS access for AWS engineers	R	I
6.10	Manage privileged credentials for OS access provided to customer by AWS	I	R
6.11	MFA management	R	I
6.12	Security patch management	R	R

10 Appendix – In Scope Services

Service Category	Included	Services
Analytics	Partial	**Included:** Athena, CloudSearch, AWS Data Exchange, EMR, AWS Glue, AWS Glue DataBrew, Kinesis, AWS Lake Formation, Amazon OpenSearch Service, QuickSight, Amazon Redshfit, Amazon SageMaker **Excluded:** AWS Clean Rooms, Amazon Data Firehose, Amazon DataZone, AWS Entity Resolution, Amazon FinSpace, Managed Apache Flink, MSK,
Application Integration	Partial	**Included:** Amazon AppFlow, Amazon EventBridge, Managed Apache Airflow, Amazon MQ, Simple Notification Service, Simple Queue Service, Step Functions, SWF

		Excluded: AWS B2B Data Interchange
Blockchain	No	**Included:** None **Excluded:** Amazon Managed Blockchain
Business Applications	Partial	**Included:** Amazon Connect, Amazon Simple Email Service **Excluded:** AWS AppFabric, Amazon Chime, Amazon Chime SDK, AWS End User Messaging, Amazon One Enterprise, Amazon Pinpoint, AWS Supply Chain, AWS Wickr, Amazon WorkDocs, Amazon WorkMail
Cloud Financial Management	Yes	**Included:** Billing and Cost Management, AWS Billing Conductor, AWS Marketplace **Excluded:** None
Compute	Partial	**Included:** AWS AppRunner, Batch, EC2, EC2 Global View, EC2 Image Builder, Elastic Beanstalk, Lamdba, Lightsail, Serverless Application Repository **Excluded:** AWS Outposts, Parallel Computing Service, AWS SimSpace Weaver
Containers	Partial	**Included:** Elastic Container Registry, Elastic Container Service, Elastic Kubernetes Service **Excluded:** Red Hat OpenShift Service on AWS
Database	Partial	**Included:** Aurora and RDS, Aurora DSQL, Amazon DocumentDB, DynamoDB, ElastiCache, Amazon MemoryDB **Excluded:** Amazon Keyspaces, Neptune, Oracle Database@AWS, Amazon QLDB, Amazon Timestream
Developer Tools	Partial	**Included:** CloudShell, CodeArtifact, CodeBuild, Amazon CodeCatalyst, CodeCommit, CodeDeploy, CodePipeline, X-Ray, Amazon Q Developer (including Amazon CodeWhisperer) **Excluded:** AWS AppStudio, AWS AppConfig, Cloud9, AWS FIS, Infrastructure Composer
End User Computing	Yes	**Included:** AppStream 2.0, WorkSpaces, WorkSpaces Secure Browser, WorkSpaces Thin Client **Excluded:** None
Front-End Web and Mobile	No	**Included:** None **Excluded:** AWS Amplify, AWS AppSync, Device Farm, Amazon Location Service
Game Development	No	**Included:** None **Excluded:** Amazon GameLift Servers, Amazon Gamelift Streams
Internet of Things	No	**Included:** None

		Excluded: IoT Analytics, IoT Core, IoT Device Defender, IoT Device Management, IoT Events, AWS IoT FleetWise, IoT Greengrass, IoT Sitewise, IoT TwinMaker
Machine Learning	Partial	**Included:** Bedrock, Amazon Bedrock AgentCore, Amazon CodeGuru, Amazon Comprehend, Amazon Kendra, Amazon Lex, Amazon Polly, Amazon Q, Amazon Q Business, Amazon Rekognition, Amazon SageMaker AI, Amazon Textract, Amazon Transcribe, Amazon Translate **Excluded:** Amazon Augmented AI, Amazon Comprehend Medical, AWS DeepComposer, AWS DeepRacer, Amazon DevOps Guru, Amazon Forecast, Amazon Fraud Detector, AWS HealthImaging, AWS HealthLake, AWS HealthOmics, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Monitron, AWS Panorama, Amazon Personalize,
Management and Governance	Partial	**Included:** AWS AutoScaling, CloudFormation, CloudTrail, CloudWatch, AWS Compute Optimizer, AWS Config, Control Tower, Amazon Grafana, AWS Health Dashboard, Incident Manager, Launch Wizard, AWS License Manager, AWS Organizations, AWS Resilience Hub, AWS Resource Explorer, Resource Groups & Tag Editor, Service Catalog, Service Quotas, Systems Manager, Trusted Advisor, AWS User Notifications, AWS Well-Architected Tool **Excluded:** Amazon Prometheus, AWS Proton, AWS Telco Network Builder
Media Services	No	**Included:** None **Excluded:** AWS Deadline Cloud, Elastic Transcoder, Elemental Appliances & Software, Amazon Interactive Video Service, Kinesis Video Streams, MediaConnect, MediaConvert, MediaLive, MediaPackage, MediaStore, MediaTailor
Migration and Transfer	Partial	**Included:** Application Discovery Service, AWS Application Migration Service, Database Migration Service, DataSync, AWS Migration Hub, AWS Snow Family, AWS Transfer Family, AWS Transform **Excluded:** Amazon Elastic VMware Service, AWS Mainframe Modernization
Networking and Content Delivery	Yes	**Included:** API Gateway, CloudFront, AWS Data Transfer Terminal, Direct Connect, Global Accelerator, Route 53, VPC **Excluded:** AWS AppMesh, AWS Cloud Map, Application Recovery Controller
Quantum Technologies	No	**Included:** None **Excluded:** Amazon Braket
Robotics	No	**Included:** None **Excluded:** AWS RoboMaker
Satellite	No	**Included:** None **Excluded:** Ground Station

Security, Identity and Compliance	Yes	**Included:** AWS Artifact, AWS Audit Manager, Certificate Manager, Cognito, Detective, Directory Service, AWS Firewall Manager, GuardDuty, IAM, IAM Identity Center, Amazon Inspector, Key Management Service, AWS Private Certificate Authority, Resource Access Manager, Secrets Manager, Security Hub, Security Hub CSPM, AWS Security Incident Response, Security Lake, WAR & Shield **Excluded:** CloudHSM, Amazon Macie, AWS Payment Cryptography, AWS Signer, Amazon Verified Permissions
Storage	Yes	**Included:** AWS Backup, EFS, AWS Elastic Disaster Recovery, FSx, Recycle Bin, S3, S3 Glacier, Storage Gateway **Excluded:** None

11 Appendix – Standard Cloud Watch Alarms

Service	Check	Alert Criteria
EC2	EC2 status check - Failed system	Alert on failure
EC2	EC2 status check - Failed instance	Alert on failure
EC2	CPU	Alert on breaches above 90%
EC2	Credit Balance Check (Burstable instances only)	Alert on balance drop below 20
Autoscaling group	Set desired, minimum and maximum capacity	Alert if drops below minimum
Autoscaling group	EC2 autoscaling group ‚Äì number of instances	Alert if group drops to zero (adjustable based on healthy/unhealthy host count)
Target Group	Target response time	Alarm when response exceeds 5 seconds
Target Group	Target connection errors	Alarm when connection fails once
Target Group	Healthy/unhealthy host count	Healthy host count lower than X amount for X minutes - alert after 3 periods. Current set up: Alarm when 2 instances are unhealthy within 15 minutes.
EBS Volumes	Read/Write operations	Trigger an alarm if read/write throughput exceeds X mb/s for 5 minutes
EBS Volumes	Latency	Trigger an alarm if latency exceeds 50ms for 5 minutes

EBS Volumes	Queue depth	Monitor queue depth
RDS Instances	CPU Utilisation	Monitor CPU usage
RDS Instances	Database Connections	Trigger an alarm if database connections exceeds X amount
RDS Instances	Read/Write IOPS	Monitor read/write IOPS
RDS Instances	Free storage space	Trigger an alarm if free storage space drops below X GB for 10 minutes
RDS Instances	Swap usage	Monitor swap usage
RDS Instances	Disk Queue Depth	Monitor disk queue depth
RDS Instances	Freeable memory	Requires ‚Äòenhanced monitoring‚Äô ‚Äì will incur costs for CW logs
DynamoDB	Read/Write Capacity	Monitor read/write capacity
DynamoDB	Throttled Requests	Trigger an alarm if throttled requests exceeds 5 per minute
DynamoDB	Latency	Monitor latency
DynamoDB	System Errors	Monitor system errors
Lambda Functions	Invocation Count	Monitor invocation count
Lambda Functions	Duration	Trigger an alarm if duration of invocations exceeds 2 seconds for 5 minutes
Lambda Functions	Error Count	Monitor error count
Lambda Functions	Throttles	Monitor throttles
ELB	Target response time	Alarm when response exceeds 5 seconds
ELB	Request Count	Monitor request count
ELB	Latency	Monitor latency
ELB	Healthy/Unhealthy Host Count	Trigger an alarm if healthy host count drops below X
S3 Buckets	Request Count	Monitor request count
S3 Buckets	Error count	Trigger if error count exceeds a particular number
API Gateway	Latency	Monitor latency
API Gateway	Integration Latency	Monitor integration latency
API Gateway	4XX/5XX Errors	Monitor 4XX/5XX errors
ECS/EKS	CPU/Memory usage	Trigger an alarm if exceeds 90% for 3 minutes

ECS/EKS	Running task count	Monitor running task count
ECS/EKS	Service Metrics	Monitor service metrics
SNS/SQS	Delivery failures	Trigger if number of delivery failures exceeds 5 per minute