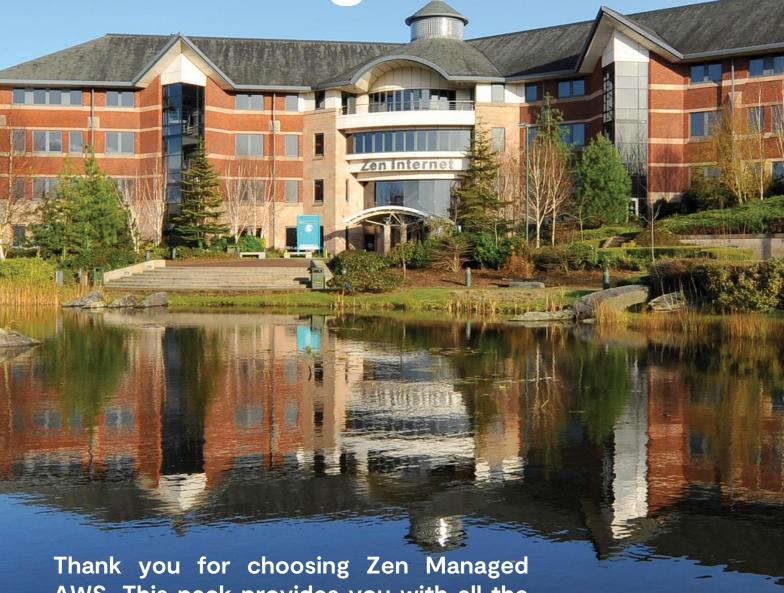# Managed AWS

zen

Thanks for choosing Zen

Thank you for choosing Zen Managed AWS. This pack provides you with all the information and guidance you need to order any new services and manage your existing Zen Managed AWS.

Ordering services & product enquiries

Service offering

Managed AWS use cases vary in the deployment approaches taken to achieve the customer's desired business outcomes. It is important to note that within this document there may be some delivery and management difference as per the solution requirements.

To order new Public Cloud Managed Hosting services, Cloud adoption, or to enquire about product specific information, availability and pricing:

Stage	Contact
Order enquiry and placement	Zen Account Manager

Core business hours

Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays)
Weekend / Bank Holidays – Closed

Order placement – key stages

○ Requirements capture and design stage:
A Customer Solution Architect (CSA) assigned to review and capture your requirements as part of the Zen Cloud Managed Hosting solution design.

○ Project management:
Depending on the complexity of the solution being deployed, a Project Manager will be assigned to initiate and co-ordinate the build and deployment activities.

Note that for Cloud adoption purposes migration activities will be defined and co-ordinated in-line with the solution.

Requirement for the activity to be project managed will be identified by Zen at the requirement capture stage.

○ Quote generated (including project management, licencing and supporting network integration where appropriate).

○ Quote accepted and Order form completed by the Customer.

Order acceptance and delivery

Data validation is completed prior to acceptance of an order. Incorrect / missing data will lead to a delay in order acceptance and service provision.

Following receipt of an order, the Zen Order Management team will process the order within 3 working days.

An order acceptance email, containing a unique order reference number will be emailed to the pre-designated customer order contact.

Service provision enquiries & updates

Stage	Contact
Complex New service development Cloud Adoption	Zen Account Manager / Project Manager

Core business hours

Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays)
Weekend / Bank Holidays – Closed

Cloud build

Build and Cloud adoption activities will be carried out in collaboration with the customer as per solution requirements. Build times may vary depending on solution complexity.

Activity	Description
Solution Build	As agreed in project scope of works

Service enablement

The Managed Cloud environment will be deployed upon completion of the requisite build and/or Cloud adoption activities.

Services that compliment the operations of the Cloud service , for example monitoring and reports, vary from solution to solution will be defined throughout the Cloud Build Stage. Requirements will be recorded by ways of playbooks and will be referred to throughout the lifespan of the Managed service.

Note: Any amendments to the operational requirements will be agreed with the customer and aligned CSA.

In-life service issues
Incident management

Stage	Contact
In-life service issues	Zen Cloud Support Team 01706 902 190 managed.hosting@zen.co.uk

🗓 Core business hours

Stage	Incident Cover
P1 – Critical/P2 - High	24/7/365
P3 - Normal / P4 - Low	Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays) Weekend / Bank Holidays – Closed

Proactive incident logging

In-line with with the monitoring of the agreed complimentry services at point of build, components within the Customers Managed Solution are monitored and managed 24/7/365 by the Zen Cloud Support Team.

Monitoring alerts will be proactively triaged by the Zen Cloud Team who will determine the appropriate function for further diagnostics. The team will endeavour to contact the customer's pre-agreed in-hours / out-of-hours order specific technical contact at the earliest opportunity.

Note that alerts and alarms may be actioned for P3 and P4 instances as defined within the build stage of the Managed Cloud Solution.

Planned engineering works and Incident notification

Any network wide incidents or maintenance activities which may affect Public Cloud services will be published on the Service status pages outlined below:

https://servicealerts.zen.co.uk

Note: Individual notification may be issued to customers dependent on the severity/impact specific to their service.

Reactive incident logging

The customer must:

- Be a Named Contact on the account and compliant with GDPR requirements.

- Be able to provide the Zen reference pertaining to the service affected by the issue.

- Provide the description of the issue being experienced and any (additional) reasonable information requested by the Service Desk.

- Ensure that they have carried out all reasonable diagnostics to eliminate any external factors that could be the potential cause of the service issue. Note: Additional checks may be requested by the Zen Cloud Support team to support identification of the root cause. A diagnostics check list can be provided to the customer on request.

Incident acceptance and resolution

Once a service fault has been established and to support timely resolution, the customer must provide a Named Contact who will be responsible for;

- Receiving incident updates via email or phone and sharing that internally to the affected site users,

- Owning the problem from a customer's perspective,

- Consenting to any potential charges that may be applicable,

- Providing site availability should Zen need to dispatch an Engineer to the customer's premises.

- Providing a named contact who can;

  - ✓ provide site access for supplier engineers (if required),

  - ✓ Testing service post resolution,

  - ✓ Confirming that service has been resumed in order for the incident to be closed.

Service enablement

Priority	Impact Definition	Support Hours	Initial Response	Considered Response
P1	Business Critical. A Severe incident that results in the loss of a critical service e.g. line of business application	24/7	Within 15 minutes	Within 60 minutes
P2	Degraded Service. An incident that results in intermittent loss or degraded performance of a critical service e.g. line of business application	24/7	Within 1 hour	Within 2 hours
P3	General Issue. Non-critical service affecting issue	Business hours	Within 1 business hour, or by 10am next business day	Within 4 business hours, or by midday next business day
P4	General query. A change request, technical query or best practice request	Business hours	Within 1 business day	Within 1 business day

Note: By definition, P1 and P2 Incidents can only apply to Production Services.

P1 or P2 incidents reported by customers must be followed up by a telephone call to the Zen Service Desk.

Roles and responsibilities

The below RACI table provides an overview of the responsibilities of Zen and the customer, for activities in the lifecycle of an aplication running within the managed environment.

- "R" – Responsible party that does the work to achieve the task

- "A" – Accountable party reviews the task or deliverable to deem it complete.

- "C" – Consultated; a party whose opinions are sought, typically as SME's (subject matter experts) and with whom there is bilateral commmunication.

- "I" – Informed party whose is informed on progress, often only on completion of the task or deliverable.

Note that while "Informed" is given its own category on the RACI matrix, we actively encourage open communication between Zen and the customer stakeholders at all stages of our service delivery. In many cases there will be dependency on timely reponses and actions to support the effective delivery of Zen's activities.

Category	Sub Service	Customer	Zen
Monitoring	Management of infrastructure, systems and services for the collection of metrics and logs	C, I	R, A
	Management of alarms against metric and log data		
	Management of monitoring dashboards		
	Review of monitoring data for changes or trends and taking remedial action where required		
	Optimisation of existing alarms and thresholds based on input from reviews, incidents and/or events		
	Monitoring of the AWS account	I	R, A
	Monitoring of the AWS Hosted Infrastructure	I	R, A
Weekly Billing Reviews	Week-on-week Billing Reviews	I	R, A
Billing Alerts	Discrepancies identified regarding billing that surpass the set threshold	I	R, A
	Subject to appropriate onboarding, tagging of resources can be enabled to aid when filtering alerts	C, I	R, A
Alarms	Monitoring your AWS environment and responding to alarms based on metrics which are defined in the onboarding process	I	R, A

Category	Sub Service	Customer	Zen
Change & Security alerts	Monitoring of: • IAM policy changes • EC2 instance changes • Console sign-in failures • Authorisation failures • Security group changes • Cloud Trail changes • Gateway changes • VPC changes • ACL changes • EC2 large instance changes	C, I	R, A
Identity & Access Management	Configuration of the AWS Identity and Access Management (IAM), within Master and associated Accounts	C, I	R, A
	AWS root account management in line with AWS best practices, including storage of the physical Multi-factor Authentication (MFA) token		
	Provision and management of user identities in line with customer requirements		
	Provision and management of user and system access policies in line with customer requirements		
	Delegation of AWS IAM access in line with customer requirements		
	Providing recommendations where there are opportunities to revoke permissions		
Network Access Control	Configuration of: • VPC security groups • VPC network ACL's • AWS WAF rules	I	R, A
Encryption & Credentials	Private keys (AWS Key Management Service)	I	R, A
	Certificates (Amazon Certificate Manager)		
	Credential Management (AWS System Manager Parameter Store)		

Category	Sub Service	Customer	Zen
Audit & Compliance	Audit and Compliance logging through AWS CloudTrail	I	R, A
Security Maintenance	Remediation of Best Practice findings regarding security issues	C, I	R, A
Cost Management	Remediation of Best Practice findings regarding cost anomalies	C, I	R, A
Usage	Remediation of Best Practice findings regarding usage issues	C, I	R, A
AWS Trusted Advisor	Remediation of Best Practice findings regarding AWS Trusted Advisor issues	C, I	R, A
Availability	Remediation of Best Practice findings regarding availability issues	C, I	R, A
Reliability Management	Monitor infrastructure and service capacity levels acting when required	I	R, A
	Ensure systems are kept up to date with critical software updates		
	Ensure data assets are protected with regular and verified backups		
	Review infrastructure resiliency and provide recommendations for improvement		
	Review reliability metrics and provide recommendations for improvement		
Capacity	Management of AWS service limits	I	R, A
	Management of production infrastructure built within the AWS account		
Software Updates	Software updates patching on the infrastructure	C, I	R, A
	Software updates patching of a subset of onboarded application resources (certain applications apply)		
Operating System Updates (patching only)	AWS ECI AMIs used by ephemeral EC2 instances (AWS Auto-scaling Groups) AWS EC2 static instances	C, I	R, A

Category	Sub Service	Customer	Zen
Application Updates	User defined applications maintained to the latest stable patch	C, I	R, A
Third-Party Managed Service Updates	Patching of a managed resource within the AWS account	R, A	C, I
Backups	All agreed data, backed up into AWS	C, I	R, A
Performance Management	Review performance metrics in accordance with the runbooks defined for the various components of the customer system	I	R, A
	Review performance dashboards and "AWS Trusted Advisor – Performance" tooling		
	Document performance-related findings for use by service management		
	Reactive investigation of service reported as degraded		

Root Cause Analysis (RCA)

Following closure of a P1 Incident, a review will be conducted to determine the nature of the issue to understand:

- Impact of the incident

- Timeline of events

- Assessment of suitability of monitoring and metrics

- Identify lessions learned

- Recommendations for avoiding a repeat incident

- Action plan including new run book updates (where applicable)

Standard lead time for an incident RCA report is 10 working days. Route cause analysis for P2 incident will be considered and reviewed where appropriate and may be subject to professional service charges.

Escalation matrix
Incident management

You can escalate through the following stages using the escalation criteria specified below:

	Level	Zen	Customer	
Considered response time 4 working hours CC Level 3, Level 1 & Zen Service Manager (If applicable)	Level 4	Customer Experience Director	Senior Management	Escalate via Manager
Considered response time 3 working hours CC Level 2, Level 1 & Zen Service Manager (If applicable)	Level 3	Head of Customer Engineering	Manager	Maintain escalation Level 3 contact Escalate to Level 4 if Escalation Criteria met at Level 3
Considered response time 2 working hours **Initial acknowledgement** 1 working hour CC Level 1	Level 2	Zen Cloud Support Manager support.escalations@zen.co.uk	Service Desk	Maintain escalation Level 2 contact Escalate to Level 3 if Escalation Criteria met at Level 2
Escalation Entry, Qualification and Acceptance Preferred method: Telephone	Level 1	Service Desk managed.hosting@zen.co.uk 01706 902 190	Service Desk	**Escalation Request** Preferred method: Telephone

Escalation Criteria:

- Poor quality of updates
- Customer is not satisfied at the way that the incident is being managed
- Agreed plan of action or timescales at a specific escalation level are not met
- The support team have not responded to an email within target response time of 8 working hours
- Frequency of updates does not meet what has been agreed with the customer

Note: Escalations can only be raised by the Customer contacts who are registered as named contacts against the Order for which the escalation is being requested on

Escalations will be accepted and managed: Mon – Fri 09:00-17:00 (Escalations outside of these hours will be managed on a best endeavours basis)

Change management

Stage	Contact
In-life change & Information requests	Zen Service Desk 01706 902 902 managed.hosting@zen.co.uk

📅 Core business hours

Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays)
Weekend / Bank Holidays – Closed

Request for change

Any customer-initiated Request For Change (RFC) for the Managed Cloud Environment will need to be requested via the Zen Service Desk by either telephone or email. When making contact the customer must;

- Ensure that the requested is submitted by designated / authorised change approver on the account and compliant with GDPR requirements.

Note: Zen will not normally initiate an RFC for operational changes to the way we deliver an existing Managed Service where there will be no customer facing impact (for instance, change to a monitoring threshold). For changes that may cause operational impact to the Managed Service, the Zen Service Desk will contact the customer prior to implementing the change.

When requesting a change, the customer must provide:

- Relevant RFC document(s) to provide clear and comprehensive details of the requested change.

- The customer lead contact name(s), contact details and availability (Working hours and outside working hours if applicable) for the purposes of;

  ✓ Authorising change implementation,

  ✓ Authorising change window for non-standard changes,

  ✓ Testing and post change success validation.

All requests are logged as a P3 priority as standard. Should there be a requirement to escalate the prioritisation level of the request, the Zen Service Desk will need to be contacted via telephone.
See Service Desk Prioritisation Target response Times.

A Zen Engineer will agree appropriate change priority levels depending on customer urgency and impact statement.

Any change request work required to be completed outside of core business hours will be subject to an additional charge.

Change classification

Level	Change Definition	Notification and Approval
1	Pre-approved planned changes which are well understood and documented that do not need specific planning and can be implemented as BAU. • A Simple and routine change which could cause no loss of service and/or resilience impact if it goes wrong. • Code deployment to customer applications. Note that in the case of there being approved code pipelines in place to de-risk code deployments, RFCs are not required.	Logged and confirmed via a ticket Implemented within 2 working days
2	Planned changes that may be service impacting, have not been pre-approved and require planning on a per case basis. • A complex and/or non-routine change. • The addition and/or removal of new and existing infrastructure components. • A change to existing Services which could result in potential loss of service and/or resilience (either by design or inadvertently). • Consideration of requirement for Statement of Works (SOW) and/or rollback plan. • Has impact on overall costs.	Reviewed and delivery approach agreed within 10 working days. Implementation schedule will be agreed with the customer.
3	An emergency Change due to: • An ongoing incident resulting in loss of service. • A security vulnerability being actively exploited. • A security vulnerability at high risk of being exploited.	Where reasonable or practical, confirmed via ticket system, or verbally by phone.

Note: Changes requested out of business hours may be subject to further design activities and professional service charges.

Level 1 – Pre-approved change

Pre-approved changes will follow and agreed workflow and will be defined within the run books.

If change is requested to be outside of core operational hours the change may be subject to professional service charges.

Level 2 – Planned change

All other non-emergency changes will follow the below high-level process within a 'Change Request' ticket:

- Confirm that a change needs to be made
- Identify what needs to be changed
- Complete and impact assessment associated with the change and confirm the change level
- Identify who needs to be engaged with the change
- Plan and document the change, creating a Statement of Works as necessary
- Acquire appropriate approval
- Implement the change
- Test for success
- Close the change
- Review learning points if necessary, holding a post-change review meeting where appropriate

Important: Deviations from the Planned Change or Change Window

The implementer will take immediate remedial action to escalate in order to bring the change within the change window or will not progress with the change starts to deviate from the plan in terms of activities or time. At this point the change will be re-assessed and arranged for a suitable time.

If the change is complex in nature, or is requested to be implemented outside of core operational hours professional service charges may be applicable.

Level 3 – Unplanned / Emergency change

During a service or security incident Zen may initiate immediate changes outside of the normal change process in order to reaonsably restore normal service. Reasonable efforts will be made to liaise with the customer during the incident to agree the appropriate remediation activities.

Change approval

Changes are subject to an element of approval across all change levels. It is important to note that approval is sought to confirm the holistic impact of a change. As such, changes may be initially rejected by either party and subject to further consultation.

The following table outlines approval responsibility across the change types.

Zen		Customer
Level 1 Changes Pre-approved	Zen Service Desk	Confirmed in advance Notification provided via ticketing
Level 2 Changes Planned	Zen Service Desk / Zen Cloud Engineering	Nominated customer change approver
Level 3 Changes Emergency	Incident owner will assess the situation and make contact where appropriate. All changes will be documented in accordance with the change process.	Customer Incident contacts where appropriate

⚙ Maintenance

Notification

Zen will triage incoming maintenance notifications from AWS to assess their actual or potential service impact.

For services considered at risk as part of the notified maintenance activity, Zen Service desk will liaise with the pre-determined named contact to identify any required mitigation. Note that this may invoke the change control process.

Zen-led maintenance activities

Planned maintenance: At times Zen may be required to schedule maintenance activities which may cause some disruption to service. Zen will endeavour to perform routine maintenance activities during the specified window as agreed during the onboarding process.

Where work is required to take place outside of the specified window, Zen will endeavour to provide notification 10 working days prior to the maintenance activity.

Exceptions: Emergency Maintenance (but not limited to) resolve an incident, resolve a known error, to ensure Regulatory compliance etc.

Emergency maintenance: maintenance activities may be deemed as a mandatory emergency requirement to resolve (but not limited to) compliance and/or security advisories.

Zen reserve the right to apply an emergency maintenance window to carry out these maintenance activities. We will endeavour to provide as much notice as possible but this may not be possible in all situations.

Customer-led maintenance activities

On occasion, customers may need to carry out on-site maintenance activities that may impact connectivity within the managed solution. (e.g. on-site power maintenance). It is recommended that the customer informs.

Zen of the maintenance at least 24 hours in advance to ensure monitoring alarms and subsequent call outs are suppressed.

Stage	Contact
Customer-led maintenance	Zen Service Desk 01706 902 190 managed.hosting@zen.co.uk