



Managed Cloud

G-Cloud 15 Service Definition

1. Summary

Jisc is an AWS Consulting Partner and AWS Government Reseller with extensive expertise in the AWS platform, this allows us to become your strategic business partner at any stage of cloud maturity. We can assist and facilitate procurement, design and delivery of AWS with a support wrapper and ongoing full life-cycle management.

Jisc is also a Microsoft Cloud Solution Provider (CSP). We have extensive expertise in the Microsoft Azure platform allowing us to become your strategic business partner at any stage of cloud maturity. We can assist and facilitate the procurement, design and deployment of Microsoft Azure services with a support wrapper and ongoing full life-cycle management.

2. Service Description

The Jisc Managed service allows organisations to procure and use technologies and services from the catalogues from both AWS and Microsoft Azure, managed and supported with the expertise and experience of Jisc. We can help you to improve your cloud security posture and manage your cloud spend.

The Managed service is primarily designed to look after the day today management of your VM's along with any supporting infrastructure such as networking, security and identity management. We can also manage many of the other Cloud services but in this case, pricing will be based on our rate card.

Our managed service is typically bought in conjunction with buying your cloud consumption through us. However, if you have an alternative procurement route you can still buy a managed service from Jisc.

We will create and configure your AWS account(s), including the provision of a hardware MFA to protect the root user. We will provide you with access to an 'administrator' user if you require it. Likewise with your Azure tenancy we will create and configure secure access for your staff to access your infrastructure.

We offer 3 tiers of service level known as Basic, Professional and Enterprise as detailed in table below (these are designed to help you choose the right level of support required):

Please note it may be that you already have some of these features in place and that they are therefore not required. In these cases, it is not a requirement for these to be managed by Jisc, although, we are happy to provide a review.

Service Features	Basic	Professional	Enterprise
Support Hours	08:00 -18:00 (Mon-Fri)	24 x 7 x 365	24 x 7 x 365
Monitoring of VM's & infrastructure, proactive alerts & reactive support	08:00 -18:00 (Mon-Fri)	24 x 7 x 365	24 x 7 x 365
Security alert monitoring of your infrastructure	08:00 -18:00 (Mon-Fri)	24 x 7 x 365	24 x 7 x 365
Re-active alerts for your public facing web services	08:00 -18:00 (Mon-Fri)	24 x 7 x 365	24 x 7 x 365
Service Level Agreement	✓	✓	✓
Service onboarding	✓	✓	✓
Vendor escalation	✓	✓	✓
Technical support via ITSM portal	✓	✓	✓
Problem management	✓	✓	✓
Ongoing cost reporting via FinOps	✓	✓	✓
Website availability reports - monthly	✓	✓	✓
Cloud management platform	✓	✓	✓
Service Features	Basic	Professional	Enterprise
Account/Relationship manager	✓	✓	✓
Consumption reports (self service)	✓	✓	✓
Backup configuration & verification	✓	✓	✓
Service offboarding	✓	✓	✓
Change requests (Additional charges may apply)	✓	✓	✓
Anti-malware		✓	✓
Windows & Linux O/S Patching & verification		✓	✓
Automated power on/off scheduling		✓	✓
Patch reports - monthly		✓	✓
Website availability reports - monthly		✓	✓
Advanced monitoring of VM's using third party tools		✓	✓
Service review meetings - quarterly		✓	
Service review meetings - monthly			✓
Access to Jisc's AWS/Azure solution Architects			✓
Health & performance recommendation reports - monthly			✓
Security review - Annual			✓
Augmented FinOps (self service)			✓
Full lifecycle FinOps (self service)			✓

2.1 Monitoring of VM's and infrastructure, proactive alerts and reactive support

We will configure monitoring of your VM's and will send alerts when agreed thresholds are exceeded including:

- Memory
- CPU
- Storage
- Network traffic

The alerts will be sent by email to a distribution group you specify during setup of the managed service.

We will provide you with access to and configure the appropriate dashboards including those for monitoring security alerts. Any configuration changes will be agreed with you because they may result in increased consumption charges.

2.2 Anti-malware

We include the setup and configuration of the following anti-malware solutions only, either Windows Defender or CrowdStrike's Falcon product, cases where we have built your environment, we will work with you to agree the anti-malware configuration and update schedule. If you already have an established environment and update-schedule we can provide a review of what you have in place during the managed service onboarding.

Please note there are additional charges for this Managed service of £5 per VM per month and licensing costs of any third-party anti-malware software.

2.3 24/7 Monitoring

- 24/7 monitoring of VM's and supporting infrastructure, proactive alerts and reactive support.
- 24/7 security monitoring using native tools covering your managed infrastructure.
- 24/7 Pro-active alerts if your public-facing web services hosted in your infrastructure, managed by Jisc become unavailable. Monthly report detailing their overall availability.
- 24/7 support for P1 incidents.

2.4 FinOps

Access to the full features and reports available from our FinOps tool these include:

- AI-Informed Insights:
 - Augmented FinOps provides enhanced cost observability and analysis through AI/ML-informed insights. These insights cater to various personas and perspectives, empowering better decision-making regarding cloud costs.
 - It ensures that you have a clear understanding of your cloud spending patterns and can take proactive measures to optimize costs.
- Full Lifecycle FinOps

- The FinOps functionality applies insights and automation across all resource stages, from provisioning to decommissioning.
 - By integrating cost considerations throughout the entire lifecycle, you can make data-driven decisions for your cloud resources.
 - This approach helps prevent cost anomalies before they occur and maximizes optimization efforts.
- Cloud Right Approach
 - The FinOps framework facilitates the convergence of public and private clouds. It allows organizations to manage diverse cloud computing resources as a single entity.

2.5 Automated power on/off scheduling

Automated power on/off scheduling for VM's according to your requirements to help minimise your AWS costs.

2.6 Information Assurance

Our managed service is designed to support the secure hosting of OFFICIAL information assets. Jisc along with AWS and Azure are ISO27001 and ISO 9001 certified organisations and will use as required appropriately certified management infrastructure, network connectivity, staff security clearance and processes to deliver the service.

3. Service Onboarding

Service on-boarding is managed as part of the contract start-up and typically happens at the end of a Jisc Cloud Design & Deployment or Jisc Cloud Professional services project. Onboarding covers the configuration of the tenant or Organization to ensure ongoing delivery of the managed service.

Where we are taking on the management of an existing estate, we will undertake a review of your infrastructure including your existing security configuration. We will agree with you whether any updates are required, how quickly they need to be made and who will make them¹. The review and any updates undertaken by Jisc will be undertaken as change requests and charged on a T&M basis.

Onboarding has the following requirements that must be met:

- Compliance with G-Cloud (Digital Marketplace) procurement processes including Account Holder agreement to Jisc Terms and Conditions for Jisc Cloud Services.
- Compliance with either the AWS Customer Agreement, which can be found at <https://aws.amazon.com/agreement/> or with the Microsoft Azure Customer Agreement which can be found at <https://azure.microsoft.com/en-gb/support/legal/subscription-agreement>.
- Provision of an authorised and validated purchase order.
- Correct handover of ownership on relevant AWS accounts or for Microsoft Azure if you are not buying your consumption through us, we require that your subscriptions are linked to our Partner ID using the Partner Admin Link (PAL) or Digital Partner of Record (DPOR) mechanisms.

¹ Jisc reserves the right not to support insecure customers.

4. Service Offboarding

Service termination is defined as end of contract without transfer of services to a new provider or customer function. In this case, on service termination Jisc will close and delete any accounts or tenancies, access controls and resources and reconfigure any managed service components that we are using. Off boarding of VM's, AWS RDS instances or Azure managed relational databases, and any data is the customer's responsibility and should be completed prior to termination.

Jisc can provide a migration path collaborating with your new provider or function. This would be a standalone chargeable project.

Service termination is defined as end of contract, without transfer of services to a new provider or customer function. In this case, on service termination Jisc will delete access controls and resources and reconfigure any managed service components that we are using. Once complete, we will close and delete any AWS accounts/Azure Tenants. Off boarding of VM's, databases and customer data is the customer's responsibility and should be completed prior to termination.

Jisc can provide a managed migration path (working alongside your new provider or function). This is provided as a standalone project and will incur rates and charges per the Jisc Cloud Migration service.

5. Customer Responsibilities

Customers have the following responsibilities in relation to the Managed service. You must provide accurate contact and payment details on AWS or Azure registration along with:

5.1 For AWS services

- You must comply with the Contract Terms and Conditions for Jisc Cloud Solutions and the AWS Customer Agreement at <https://aws.amazon.com/agreement/>
- You must follow designated procedures for logging incidents, service requests and change requests.
- You must agree to Jisc owning the management/payer account associated with your AWS accounts²
- If you buy AWS services through us but choose not to take our managed services you are responsible for the security of your AWS estate and for ensuring that your VM's and RDS SQL databases are patched, have up to date anti-malware installed and have adequate backups.

5.2 For Azure services

- As referenced in Clause 7.8 of the terms and conditions for Jisc cloud services, the Managed Azure service is subject to additional terms that we are required to pass on by Microsoft. These Microsoft Azure terms prevail over the terms and conditions for Jisc cloud services terms for those elements of the service which are supplied by Microsoft. These terms are set out below:

² As an AWS partner, we are required to own all management/payer accounts procured through us. In this case, 'own' means that the credentials (email address, password, and MFA device) used to access the root user must be managed by Jisc.

- The Microsoft Online Subscription Agreement: <https://azure.microsoft.com/en-gb/support/legal/subscription-agreement/> ; and
- The Customers' relevant Microsoft Cloud Agreement: <https://docs.microsoft.com/en-us/partner-center/agreements>
- You must follow designated procedures for logging incidents, service requests and change requests
- Where you are not buying your Azure consumption through us, you must allow your Azure subscriptions to be linked to our Partner ID using the Partner Admin Link (PAL) or Digital Partner of Record (DPOR) mechanisms.

Please note for any services that you don't wish or can't be managed by Jisc, you are responsible for the security of your infrastructure such as ensuring that your VM's and Databases are patched, have up to date anti-malware installed, and have adequate backups.

6. Service Management

Jisc is a proven service management specialist with extensive experience of service management implementation, operation and continual service improvement. All our operational processes are aligned with ITIL v3 and information assurance is provided through our ISO 27001 certification.

7. Support

Jisc provides support via our experienced cloud support engineers who act as your first point of contact for any service-related issues or queries that you may have. Support is provided during core hours of service, Monday to Friday between the hours of 08:00 - 18:00, excluding UK public holidays. Jisc offers the Professional and Enterprise Support offering on a 24-hour basis for P1 incidents only.

We strongly encourage you to buy Business Support for any AWS accounts hosting production workloads. Where you are buying AWS from us and we are unable to resolve an incident or change request, our team will function as intermediary between you and the AWS service desk. Where AWS is not purchased through us, you will be able to raise support calls directly with the AWS service desk yourself.

For Microsoft Azure, we include Microsoft support at no additional charge. Where we are unable to resolve an incident or change request, our team will function as a intermediary between you and the Microsoft service desk.

7.1 Incident Management

The Managed cloud service will follow ITIL incident management process guidelines to log, assign and diagnose incidents and to restore service operation as quickly as possible with minimum disruption, in line with the agreed hours of service.

The timings below indicate the target time to respond to an incident. In some cases, for example where there is widespread disruption to AWS or Azure, this may require us to triage the incident and raise a call against the cloud providers service desk. Once we receive a response, we will pass it back to the customer.

Service Incident	Basic	Professional	Enterprise
Priority 1 incidents			
Target response	30 mins	30 mins	30 mins
Target resolve	8 Hours	4 Hours	4 hours
Priority 2 incidents			
Target response	2 Hours	1 Hour	1 Hour
Target resolve	16 Hours	8 Hours	8 Hours
Priority 3 incidents			
Target response	4 Hours	2 Hours	2 Hours
Target resolve	24 Hours	12 Hours	12 Hours

7.2 Incident Priority Definitions

Priority 1 incidents: Service component failed or severely impaired resulting in serious business-wide impact or multiple users/services impacted.

Priority 2 incidents: Service component impaired resulting in a loss of functionality, or loss of access to a single or subset of users, but work can continue in an impaired manner.

Priority 3 incidents: Incident with minor or no direct impediments on the customer's business and/or is not time sensitive.

7.3 Service Requests and Change Requests

The Managed Cloud service will follow ITIL request fulfilment process to manage service requests and change requests. Where necessary, we will raise a call against the AWS or Azure service desk, returning the response to the customer as we get it.

Service/Change request response target	Basic	Professional	Enterprise
Our target to respond to standard change as defined by ITIL (a routine and low-risk modifications to your cloud infrastructure) is shown in the table. Other request types, normal, major and emergency, again as defined by ITIL processes will be assessed on a case-by-case basis, and we will then confirm the timeframe for completion. We will supply a quote for any associated charges for this work.	4 Hours	2 Hours	2 Hours

8. Account Management

Your account will be managed by our cloud service delivery team who will be your primary contact at Jisc for all service-related matters.

For Enterprise managed service customers, we will arrange monthly service review meetings (Via a phone or video call).

9. Ancillary Services

9.1 Cloud Professional Services.

Jisc's cloud Professional Services provide specialist technical consultancy to organisations using or planning to use cloud-based IT service delivery models. Jisc has a broad range of practical experience in relation to managing many aspects of cloud service design, migration and operation. We draw on this experience to offer organisations skilled, flexible and pragmatic resources to meet short-term business challenges and/or to contribute to, or lead, longer-term projects or cloud-centred IT transformation programmes.

9.2 AWS OVGA resell

As part of the ongoing development of the One Government Cloud Strategy, Crown Commercial Service (CCS) have signed a renewed Memorandum of Understanding (MoU) with Amazon Web Services (AWS). One Government Value Agreement 2.0 ("OGVA 2.0") takes the form of a three-year MoU between CCS and AWS. Developed based on feedback from public sector organisations, OGVA 2.0 incorporates additional benefits for government departments, agencies, and organisations across the wider UK public sector that help them derive greater value from AWS computing services.

Jisc is an AWS Consulting Partner and AWS Government Reseller with extensive expertise in the AWS platform, this allows us to become your strategic business partner at any stage of cloud maturity. We can assist and facilitate procurement of AWS via the OGVA agreement. This service is only available via the Jisc resell service for those organisations who qualify for and are purchasing via the OGVA Cloud Prime tier. Jisc offer our AWS managed cloud services customers a procurement route for their consumption via our AWS OGVA resell service in G Cloud 15 Lot 1a. The pre-requisites to join the Cloud Prime Tier are:

Agree to the minimum prerequisites of the Cloud Prime Tier, in respect of the minimum spend and spend commit requirements over the duration of the contract.

Jisc will sign a new, three-year Private Pricing Agreement with AWS as an authorised Public Sector partner based on OGVA 2.0-specific terms as agreed with CCS. You will sign a G-Cloud call-off contract with Jisc.

A contract for AWS Support for the duration of their OGVA 2.0 call-off contract. This can be either:

- AWS Enterprise Support Service
- or
- AWS Enterprise On-Ramp Support

10. Pricing

Please refer to the separate Jisc G-Cloud Service pricing document

11. Special Terms

Customers purchasing AWS consumption have the following responsibilities in relation to the service:

- You must provide accurate contact and payment details on Managed AWS registration.
- As referenced in Clause 7.8 of the Terms and Conditions for Jisc Cloud Services, the Managed AWS service is subject to additional terms that we are required to pass on by Amazon. These Amazon AWS terms prevail over the Terms and Conditions for Jisc Cloud Services terms for those elements of the service which are supplied by Amazon. These terms are set out below:
 - The AWS Customer License Terms, a separate agreement between you and Amazon Web Services, Inc., a current version of which is located here [**AWS+Reseller+Customer+License+Terms.pdf**](#)
 - The rights and restrictions located at <http://aws.amazon.com/serviceterms>, as updated by AWS from time to time, and as may be made available on any successor or related site designated by AWS
 - The terms and conditions of the AWS Customer Agreement located at <http://aws.amazon.com/agreement/>, where the rights and obligations of AWS shall be the rights and obligations of Jisc Services Limited
 - You must follow designated procedures for logging incidents and Change Requests
 - You must agree to Jisc owning the management/payer account associated with your AWS accounts.

Customers purchasing Microsoft Azure consumption have the following responsibilities in relation to the service:

- You must provide accurate contact and payment details on Managed Azure registration.
- As referenced in Clause 7.8 of the terms and conditions for Jisc cloud services, the Managed Azure service is subject to additional terms that we are required to pass on by Microsoft. These Microsoft Azure terms prevail over the terms and conditions for Jisc cloud services terms for those elements of the service which are supplied by Microsoft. These terms are set out below:
 - The Microsoft Online Subscription Agreement: Online Subscription Agreement | Microsoft Azure; and
 - The Customers' relevant Microsoft Cloud Agreement: Microsoft Customer Agreement templates - Partner Center | Microsoft Learn
 - You must follow designated procedures for logging incidents, service requests and change requests.
 - Where you are not buying your Azure consumption through us, we require that your subscriptions are linked to our Partner ID using the Partner Admin Link (PAL) or Digital Partner of Record (DPOR) mechanisms.