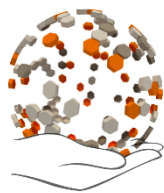


	PROCUREMENT ACTIVITY MANAGER 3.0
---	--

G-Cloud 15 Service Definition



Bringing your data together



Rembrace
SMART SOLUTIONS

e. support@rembrace.co.uk

w. www.rembrace.co.uk

1. Service Overview

Procurement Activity Manager (PAM) is a cloud-based Software as a Service (SaaS) platform designed to support organisations in developing, managing, and reporting on Cost Improvement Programmes (CIP). The service enables users to plan procurement activities, track savings initiatives, collaborate across teams, and produce dashboards and reports to support governance and decision-making.

PAM is intended for use by procurement, finance, and operational teams within public sector organisations, including NHS bodies, local authorities, and central government departments.

2. Service Description and Key Capabilities

PAM provides a single platform for managing procurement-related workplans and savings initiatives. Core capabilities include:

- Workplan and project management for procurement initiatives
- Savings tracking and forecasting
- Interactive dashboards and reporting
- Collaboration across teams and organisations
- Data quality checks and validation
- Workflow management for project milestones and approvals
- Contracts management functionality
- AI-assisted insights and forecasting (where enabled)

The service is modular and can be configured to align with customer requirements and organisational processes.

3. Technical Architecture

PAM is delivered as a multi-tenant SaaS application hosted on Microsoft Azure. All infrastructure and platform services are provisioned within UK-based Azure regions , unless otherwise agreed with the customer. (for example, Azure UK regions), with data storage and processing restricted to the United Kingdom.

Users access the service via a secure web interface using a modern web browser. No client-side installation is required.

The platform supports:

- Web-based user interface for end users and administrators
- Secure data storage and processing in UK-based Azure data centres
- Integration with external systems (for example, purchasing or finance systems) via agreed interfaces where required
- Mobile-responsive access for use on desktop and mobile devices

Azure-native security controls are used to protect the platform, including identity management, network security controls, logging and monitoring, and endpoint protection.

All infrastructure and platform services are provisioned within UK-based Azure regions, with data storage and processing restricted to the United Kingdom.

Users access the service via a secure web interface using a modern web browser. No client-side installation is required.

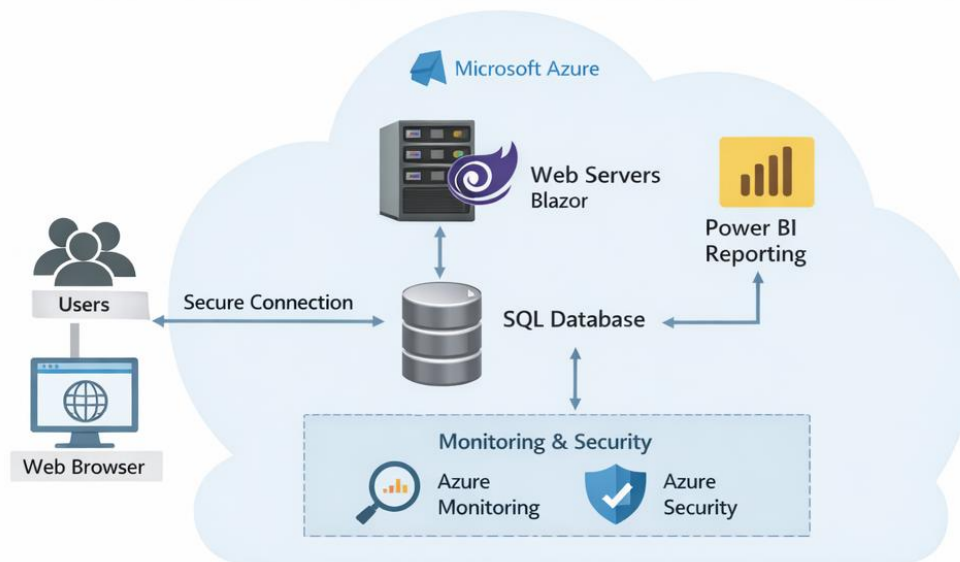
Figure 1: PAM System Architecture

Technical Architecture

PAM is hosted on Microsoft Azure within UK data centres, for example, in the Azure UK South and UK West regions.

The architecture of the PAM platform is illustrated below.

PAM System Architecture



Security and Compliance

Data Protection:

All customer data is stored and processed within UK data centres.

Customer data is not transferred outside the United Kingdom without explicit customer agreement.

4. Security and Compliance

Security is managed through organisational policies, technical controls, and operational processes.

4.1 Data Protection and Privacy

- Customer data is stored and processed in Microsoft Azure data centres located in the United Kingdom.
- Data is transmitted using industry-standard encryption protocols (TLS 1.2 or above).
- Customer data is logically segregated between tenants.
- Data handling is aligned with UK GDPR and Data Protection Act requirements.
- Customer data is not transferred outside the United Kingdom without explicit customer agreement.
- Data is transmitted using industry-standard encryption protocols (TLS 1.2 or above).
- Customer data is logically segregated between tenants.
- Data handling is aligned with UK GDPR and Data Protection Act requirements.

4.2 Security Certifications and Assurance

- The organisation holds Cyber Essentials and Cyber Essentials Plus certifications.
- Security controls are reviewed regularly to maintain alignment with certification requirements.
- The organisation aligns its cloud security approach with the NCSC Cloud Security Principles and industry good practice where applicable.

4.3 Identity and Access Management

- User authentication is required for all access to the service.
- Multi-Factor Authentication (MFA) is supported for user and administrative access.
- Role-based access controls restrict users to the minimum permissions required for their role.
- Administrative access is restricted and monitored.

4.4 Vulnerability and Patch Management

- Vulnerability assessments are performed using cloud-native tooling.
- Security patches and updates are applied in line with defined patch management processes.

4.5 Incident Management

- Security and operational incidents are logged, assessed, and managed using defined incident management procedures.
 - Escalation and resolution processes are documented and reviewed.
-

5. Availability and Resilience

- The service is designed for high availability and resilience.
 - Data is replicated across multiple hardware components to ensure durability.
 - Backups can be maintained in a secondary geographic location.
 - The service has a target availability of 99% measured monthly, excluding agreed maintenance windows.
-

6. Onboarding and Implementation

A standard onboarding approach is used and tailored to customer requirements.

Typical onboarding activities include:

- Requirements discovery and configuration planning
- Data migration and integration planning (where applicable)
- System configuration and validation
- User training and documentation provision
- Go-live support

Typical onboarding timelines are approximately 3–4 weeks, subject to scope and data migration requirements.

7. Service Management and Support

7.1 Support Channels

Support is provided via email and online ticketing, with optional web chat and onsite support (at additional cost).

7.2 Support Hours

Support is available during standard UK business hours, with severity-based response and resolution targets defined in the Service Level Agreement (SLA).

7.3 Service Reviews

Service review meetings can be conducted quarterly to review performance, incidents, and improvement actions.

8. Service Level Agreement (SLA)

8.1 Uptime Commitment

The service is provided with a target availability of 99% per calendar month.

8.2 Measurement and Service Credits

Uptime is measured using automated monitoring. Where availability falls below the agreed threshold, service credits may be applied in line with the SLA.

8.3 Incident Response

Incidents are categorised by severity with defined response and resolution targets. Escalation procedures are documented.

Category Level	Criteria	Response Time Within (business days)	Resolution Time Within (business days)
1	Severe: Complete degradation - all users and critical functions affected . Item or service completely unavailable.	1	2
2	Medium: Significant degradation - large number of users or critical functions affected . Primary business processes can continue.	1	3
3	Minor: Limited degradation - limited number of users or critical functions affected . Primary business processes can continue.	2	5

9. Accessibility

PAM is accessed through a web-based interface and is designed to be usable with modern browsers and assistive technologies. The organisation monitors accessibility standards and plans enhancements in line with WCAG guidance where appropriate.

10. Customisation and Configuration

The service supports configuration of datasets, workflows, and mandatory fields to align with organisational processes. Bespoke integrations and configurations may be provided by agreement.

11. Data Portability and Exit Management

At the end of the contract:

- Customer data is exported in an agreed CSV format and securely returned to the customer.
- Data is securely deleted from the service following customer confirmation.
- Confirmation of deletion is provided on request.

Support for migration to alternative platforms can be provided by agreement.

12. Service Constraints and Dependencies

- Real-time savings tracking requires integration with purchasing (PO) or finance (AP) systems.
 - The service requires internet connectivity and a supported web browser.
 - Some advanced features may require configuration or integration activities.
-

13. Continuous Improvement

The service is continuously developed and improved based on customer feedback, operational experience, and technology updates. Updates and enhancements are managed through controlled change management processes.

14. Contact and Supplier Information

Supplier contact details are provided separately in the Digital Marketplace submission and commercial documentation.

This service definition is provided for use within the G-Cloud framework and is intended to support public sector procurement and assurance activities.