MAXIRON

BRING STRENGTH TO YOUR DELIVERY



MaxIron Service Definition

Maximo Application Suite as a Service

G-Cloud 15 v1.0

TABLE OF CONTENTS

TABLE OF CONTENTS 1
1. Service Description 3
1.1 MAS applications and add-ons 4
1.2 Service Features 4
1.3 Service Benefits 5
1.4 Licensing options 5
1.5 Out of scope (unless separately agreed) 5
2. Data Backup, Restore, and Disaster Recovery 5
2.1 Data Backup and Restore 5
2.2 Disaster Recovery and Business Continuity 6
3. Onboarding and Offboarding Support 6
3.1 Training and documentation 6
4. Service Constraints 6
4.1 Maintenance Windows 6
4.2 Technical Requirements 6
5. Outage and Maintenance Management 6
5.1 Outage Handling 6
5.2 Maintenance Practices 7
6. Service architecture and deployment model 7
6.1 Deployment model 7
6.2 Tenant isolation and resource independence 7
6.3 Multi-cloud support 7
6.4 Hosting Locations 7
7. Service management 7
7.1 Support hours and channels 7
7.2 Response targets 8
7.3 Planned maintenance and change 8
7.4 Monitoring, backup and restore 8
7.5 Service Availability 8
8. Security 10
8.1 Data in transit 10
8.2 Data at rest 10

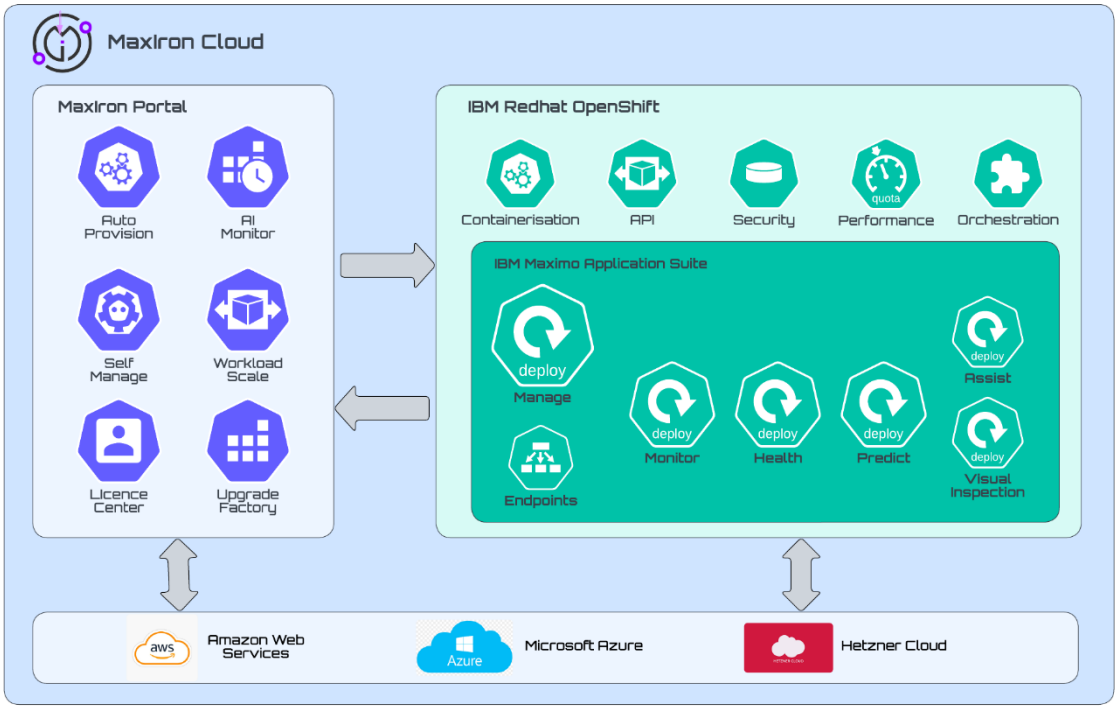
8.3 Vulnerability and patch management 10
8.4 Audit and logging 10
9. Data access, integrations and APIs 10
9.1 Integrations 10
9.2 APIs and documentation 10
9.3 Service constraints 10
10. End-of-contract and exit 11
10.1 Data extraction 11
10.2 Offboarding process 11
11. Service locations 11

1. Service Description

MaxIron provides IBM Maximo Application Suite (MAS) as a managed, tenant-isolated cloud service. We host and operate production and non-production MAS environments, including the underlying Red Hat OpenShift platform, to deliver a secure, resilient and supportable Maximo capability for asset-intensive organisations.

Our IBM Maximo Application Suite (MAS) solution is designed to help customers provision and consume MAS environments quickly with transparent costing and optimal performance. This service includes the ability to auto provision an environment of the required type in under two hours.

All infrastructure interactions with the environment happen via the MaxIron Portal. The portal solves the problem of having to understand the underlying infrastructure, application servers as well as Red Hat Open shift. All these services are abstracted from the user so that the focus is on getting an environment fast. The diagram below shows the portal capabilities.



Once the user is registered within or Portal then they can provision an environment within two hours. They will then have access to the other services to manage the environment.

About IBM Maximo Application Suite (MAS)

IBM Maximo Application Suite (MAS) is IBM's enterprise asset management and asset performance platform, delivered as a modular set of applications (for example Maximo Manage, Mobile, Health, Monitor, Predict and Visual Inspection). MAS is deployed using a container-based architecture on **Red Hat OpenShift (Kubernetes)**, and can be operated on supported public cloud or on-premises infrastructure, subject to IBM supportability and licensing.

MAS applications are enabled based on the buyer's required use cases and IBM entitlements. IBM MAS uses an entitlement model (including **AppPoints**) and OpenShift capacity requirements; sufficient entitlements must be held for the intended authorised use.

What MaxIron provides vs IBM

This service provides the managed cloud platform and operational capability required to run MAS (including the OpenShift platform, MAS platform layer, environment provisioning, monitoring, backup/restore, patching coordination and service desk support). IBM remains the software publisher for MAS; buyers either (a) bring their own IBM MAS entitlements (BYOL) or (b) procure licensing through MaxIron as part of the service (as documented in the Order Form).

1.1 MAS applications and add-ons

MAS is a suite of applications. Buyers can procure and enable the applications required for their use cases, subject to licensing and IBM AppPoints.

Our typical deployment pattern is:

- Maximo Manage (EAM) and Role-based Applications.
- Maximo Mobile (including app store client).
- Maximo Health.

Our further enhanced optional deployment pattern is:

- Maximo Monitor.
- Maximo Predict.
- Maximo Visual Inspection.
- Maximo Assist.
- Maximo Asset Investment Planning.
- Industry solutions and add-ons (where licensed).

1.2 Service Features

- Environment provisioning (non-prod/prod) and baseline MAS configuration
- OpenShift and MAS platform operations (monitoring, capacity, certificates, backups, routine housekeeping)
- Controlled change management for platform and MAS components (planned maintenance windows)
- Incident/request/problem management via service desk
- Tenant administration support (access changes, scaling requests, restore requests)
- Observability and operational reporting (availability, utilisation, event logging)

1.3 Service Benefits

- ❑ Environment provisioned in under 2 hours
- ❑ Run costs reduced by 30%
- ❑ Consumption based
- ❑ Supports SDLC through DevOps

1.4 Licensing options

Buyers can either (a) bring their own IBM MAS entitlements (BYOL), or (b) procure licensing through MaxIron as part of the service. Where MaxIron provides licensing, we will align entitlements and AppPoints to the agreed environments and applications in the Order Form.

1.5 Out of scope (unless separately agreed)

- Functional configuration of Maximo processes, workflows and security roles.
- Integration build (beyond standard connectivity and platform plumbing).
- Data cleansing, migration and reconciliation activities.
- Custom development or bespoke code changes.
- Third-party application or device support (unless explicitly included).

2. Data Backup, Restore, and Disaster Recovery

2.1 Data Backup and Restore

We provide hourly backups of all Maximo data using cloud-based storage solutions to ensure data integrity and security. Customers can restore their data to any previous state within 30 days.

2.2 Disaster Recovery and Business Continuity

Our disaster recovery strategy includes a failover to a secondary data centre in the event of a major incident. We guarantee a Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 15 minutes.

3. Onboarding and Offboarding Support

Onboarding is delivered through an agreed service transition plan. The typical onboarding steps are:

- Confirm scope: environments, applications, integrations, users and non-functional requirements.
- Provision environments and establish connectivity, SSO and certificate approach.
- Configure monitoring, backups and operational runbooks.
- Service desk setup: named buyer contacts, ticket categories and escalation routes.
- Operational acceptance: smoke tests, access validation and handover to steady-state.

3.1 Training and documentation

MaxIron provides onboarding guidance, operational documentation and administrator handover. Optional end-user and super-user training can be provided under a separate implementation or support work package.

4. Service Constraints

4.1 Maintenance Windows

Scheduled maintenance windows are typically reserved for weekends, from 2 AM to 6 AM, to minimize impact on business operations. Customers are notified at least two weeks in advance.

4.2 Technical Requirements

Adequate specifications and necessary software licenses must be verified.

5. Outage and Maintenance Management

5.1 Outage Handling

In the event of an unplanned outage, our emergency response team is mobilized to identify and resolve the issue. Customers are updated every hour regarding outage status and expected resolution time.

5.2 Maintenance Practices

Regular updates and patches will be applied during agreed-upon maintenance windows, with all changes thoroughly tested in a staging environment before being deployed to the live system.

6. Service architecture and deployment model

6.1 Deployment model

The service is delivered using a public cloud deployment model, with each buyer provisioned into a dedicated customer tenant. MAS workloads are deployed on Red Hat OpenShift (Kubernetes) with environment isolation and controlled capacity management.

6.2 Tenant isolation and resource independence

Each buyer tenant is deployed into isolated OpenShift namespaces with segregated supporting services. Resource quotas and limits (CPU/memory) are enforced per namespace, network policies restrict east-west traffic, and ingress routes, secrets and service accounts are separated per tenant. Clusters are sized with headroom and monitored continuously to prevent contention between tenants.

6.3 Multi-cloud support

MAS environments can be deployed on major hyperscale cloud providers (for example AWS or Microsoft Azure) depending on buyer requirements, data residency and connectivity constraints. The operating model and controls remain consistent across supported cloud platforms.

6.4 Hosting Locations

Cloud hosting is available in data centers located in the UK and Europe to comply with data sovereignty requirements.

7. Service management

7.1 Support hours and channels

Support is provided via Jira Service Management (email and online portal). Standard support is UK business hours (08:30–17:00 Monday to Friday, excluding public holidays).

Premium 24x7 cover for critical incidents can be added. All support is delivered remotely unless on-site services are separately agreed.

7.2 Response targets

Severity-based response targets are agreed in the Order Form. Typical targets are:

Severity	Example impact	Standard response target	Premium response target
P1 Critical	Major service outage or security-impacting incident	1 hour (business hours)	20 minutes (24x7)
P2 High	Material degradation or key function unavailable	4 hours (business hours)	4 hours (business hours)
P3 Medium	Issue with workaround available	24 hours (business hours)	24 hours (business hours)
P4 Low	Queries and service requests	Work begins within 8 hours (not measured)	Work begins within 8 hours (not measured)

7.3 Planned maintenance and change

Planned maintenance (for example platform patching or MAS patch application) is scheduled in agreed maintenance windows. Changes follow controlled change governance with impact assessment, non-production testing where applicable, and communication to buyer contacts.

7.4 Monitoring, backup and restore

We monitor platform health and key application services, including availability, utilisation and error conditions. Backups and restores are provided for MAS components and supporting services (for example databases and persistent storage) in line with the agreed service tier. Backup frequency, retention and recovery objectives are defined in the Order Form and can be tailored to buyer requirements.

7.5 Service Availability

We offer 99.9% uptime on our services, with comprehensive monitoring to ensure availability is met

8. Security

8.1 Data in transit

Data between the buyer and the service is protected using TLS 1.2 or above. Private connectivity options (such as VPN or dedicated links) can be implemented where required.

8.2 Data at rest

Data at rest is protected using encryption for persistent storage and managed database services, with encryption keys managed per the chosen cloud provider controls. Access to infrastructure components is restricted using least privilege, role-based access control and strong authentication.

8.3 Vulnerability and patch management

We track vendor security advisories (IBM, Red Hat and cloud providers), assess exposure, and apply patches through controlled release processes. Critical security patches can be expedited under an emergency change process with appropriate approvals and communications.

8.4 Audit and logging

Operational and security logs are collected for platform and application components. Buyers can request audit extracts relevant to their tenant, and Maximo provides application-level audit capabilities aligned to configured security roles.

9. Data access, integrations and APIs

9.1 Integrations

MAS supports integration through standard mechanisms including the Maximo Integration Framework (MIF), REST APIs and message-based patterns. Integration build and ongoing interface support can be delivered under implementation or support work packages.

9.2 APIs and documentation

MAS provides APIs for data access and automation. API documentation is available through IBM product documentation and, where applicable, OpenAPI/Swagger definitions for supported endpoints.

9.3 Service constraints

- Service is delivered remotely; on-site services are by agreement.

- Some changes require planned maintenance windows (for example platform upgrades).
- Performance depends on agreed sizing, connectivity and buyer integration patterns. Buyer is responsible for end-user devices, networks and identity provider configuration.
- Third-party dependencies may affect resolution times for some incidents.

10. End-of-contract and exit

10.1 Data extraction

At contract end, buyers can extract their data using standard Maximo capabilities, including:

Download to Excel from application views and reports (where enabled).

Export using the Maximo Integration Framework (MIF) and integration endpoints.

Database export (subject to access controls and agreed approach).

10.2 Offboarding process

Offboarding is coordinated through an agreed exit plan. This typically includes data extraction support, revocation of access, and decommissioning of environments following confirmation of successful data export. Data sanitisation is performed in line with secure deletion practices, including cryptographic erasure and secure wipe of allocated storage where applicable.

11. Service locations

Service delivery is provided from the United Kingdom and the European Economic Area.

Hosting locations are selected based on the buyer's required cloud region(s) and data residency requirements