HM Government
G-Cloud
Supplier

Fleet™
Cloud Software

IBM.
Gold
Business Partner

IBM Watson IoT Award
Winner 2017

Enabling the
Digital
Enterprise

FLEET SERVICE DEFINITION

G-Cloud 10
EAMS Group Cloud Software

Contents

Service Overview

EAMS Group's Enterprise Asset and Safety Management (EAM) Cloud Software solution is a world class service leveraging IBM's best of breed Maximo EAM software. Our Industry Solutions provide Buyers with a fully configured, industry specific solution using Maximo as a base platform and, coupled with our Cloud Support offering, accelerates speed to value for Buyers of an enterprise grade asset management solution.

- Under the services offered in the document, a Maximo SaaS solution, Buyers will receive a world class Enterprise Asset Management system built using the IBM Maximo framework, provided on a securely hosted cloud platform that is fully managed by EAMS Group thereby reducing the Buyer's risk and responsibility around system installation, support and maintenance. Buyers are encouraged to utilise and configure the system to match their goals and levels of asset and safety management maturityvia the SaaS operating model with EAMS Group Support, Data Migration, Onboarding and Offboarding services.
- Our SaaS service is available through a tiered approach based on the competency and maturity of your business (basic, advanced, world class). This flexibility allows Organisations to choose the appropriate level of service to match their requirements and offers the ability to grow their asset management capability over time without having to switch solutions with the business disruption this can cause.

EAMS Group provides a mobilisation / transition service as part of SaaS on-boarding with mobilisation costs optimised to match the level of service required to meet the Buyer's needs. Please refer to our Pricing Document for full details.

A breakdown of the product components offered at each service level is outlined below:

Product	Part Number	Basic	Advanced	World Class
IBM Maximo Asset Management	D0GYALL			
IBM Maximo Everyplace	-			
IBM Maximo Calibration	D03X4LL			
IBM Maximo Scheduler	D0AYULL			
IBM Maximo Health and Safety Manager	D0L7TLL			
IBM Maximo Anywhere	D10R9LL			
IBM Maximo Service Provider	D04XWLL			
IBM Maximo Transportation	D0GZNLL			
IBM Maximo Asset Configuration Manager	D03WYLL			
IBM MobileFirst	D1FSELL			
Additional Environment Max 25 Concurrent Users	EAMS001			
Basic Support Service (includes 20 incident hours)	EAMS002			
Advanced Support Service (includes 40 Incident hours)	EAMS003			
World Class Support Service (includes 60 incident hours)	EAMS004			

- Utilising our expertise in cloud hosted Maximo solutions we are able to rapidly provision and install systems as follows:

  Basic – 1 day
  Advanced – 2 days
  World Class – 3 days

- In order to assist in moving towards world class asset management, we would recommend reviewing our G-Cloud Cloud Support offering which provides Asset Management consulting and system implementation expertise and can be consumed in conjunction with the Cloud Software service.

EAMS Group is well positioned to provide software as a service from unparalleled experience in providing Maximo software as a service across our customer base, and our Maximo solutions that have enabled millions in savings;

- Whole life cost competitiveness: our SaaS and consultancy services provide a faster time to benefits
- Technical merit & functional fit: our IBM Premier Maximo status and as Patron of the Institute of Asset Management demonstrates the intersection of EAM Thought Leadership with Technical acumen
- Service Management: our projects are running at 99.90% SLA and are recommended by our customers
- Non-functional characteristics: our Technology laboratory are constantly evolving and pushing the future proof technology of our Maximo accelerators in BIM, RCM, IoT and many more.

Benefits & ROI

EAMS Group has undertaken asset management implementations with public and private organisations in the United Kingdom, Europe and the United States by using services available via the Cloud Support offering.

EAMS Group's Cloud Support services and Industry Solutions have been independently benchmarked as world leading, enabling proven benefits:

- 25-30% cost reduction in maintenance and renewals
- 7 fold improvements in workforce safety
- 40%+ increase in asset performance and reliability compared to traditional EAM solutions.

In addition to these quantifiable benefits, our clients benefit from significant improvements in their ability to implement continuous improvement in their Asset Management capabilities:

- Manage all assets in a common system platform
    - Maintain your entire asset register, preventive maintenance regimes, correct maintenance, labour workforce and asset related supply chain within a single system with interrelated modules, applications and reports giving a single source of truth and management point for your asset management capability

- Drive best practice industry processes
    - IBM Maximo is the best in class asset management system as rated by the independent Gartner as part of a report that ranked Maximo against other EAM systems highlighting industry specific functionality, high customer satisfaction and a mature community of EAM support resources and partners (EAMS Group)

- Speed – have an EAM system available in days
    - Our rapid deployment ability means a secure environment with the base Maximo platform installed can be provisioned within 4 hours

- Scalability – scale to an unlimited number of users
    - The only real limitation on the number of users the can utilise Maximo is linked to the number of users being paid for by the Buyer (licences), our elastic infrastructure approach to hosting allows the platform to be scaled as required to provide optimum system performance

- Solution cost – reduce total cost of ownership
  - Operational costs are reduced as Buyers are only paying for the service rather than expensive IT labour and costs associated with managing software instances

- No high up-front cost – Opex (not Capex)
  - No high up-front capex costs which used to be typical of introducing major IT solutions to an organisation, costs are now evenly spread over time as opex costs

- Reduced Buyer responsibility and risk (system installation and support)
  - EAMS Group are responsible for system installation and support, the Buyer can utilise the system safe in the knowledge that stability and up-time of the solution is being managed by EAMS Group

- EAMS Group will manage application and infrastructure (deployment, support, maintenance)
  - Our Support Division will manage all aspects related to deployment, support and maintenance of both the underlying hosted infrastructure platform and the software itself (excluding any system development which can be leveraged through our Cloud Support offering)

- Configurable platform – adapt to changing business requirements
  - A key differentiating benefit of Maximo as a software platform is its ability to be easily configured to meet client needs e.g. ability to create workflows to manage business processes and amend screen layouts. Administrative users can be granted such privileges via the inbuilt security model. EAMS Group can also provide advanced configurations or developments via our Cloud Support offering.

- Optimised system performance through our cloud hosted environment
  - The EAMS Group Support Division offers a comprehensive range of services targeted at optimising the performance of Asset and Management solutions through their expertise in managing hosted infrastructure

Main Features

The main product features available within our EAMS Group Maximo Enterprise Asset Management Cloud Software, are:

- Asset Management
  - Manage assets and make investment decisions to repair or replace throughout the asset lifecycle

- Work Management
  - Manage both planned and unplanned work activities, from initial request through completion and recording of actuals (resource utilisation)

- Service Management
  - Define service offerings, establish service level agreements (SLAs), proactively monitor service level delivery and implement escalation procedures

- Contract Management
  - Gain complete support for purchase, lease, rental, warranty, labour rate, software, master, blanket and user-defined contracts

- Inventory Management
  - Know the details of asset-related inventory and its usage including what, when, where, how many and how valuable

- Procurement Management
  - Support all phases of enterprise-wide procurement such as direct purchasing and inventory replenishment

- Mobile Ready
  - With Maximo Everyplace you can access the solution wherever you have connectivity from a smartphone or other supported mobile device, gaining real-time visibility into your operations

- Operational Reporting
  - Access to a large variety of reports spanning all applications including analysis, drill down, hierarchical and graphical reports with over 100 out-of-the-box reports available, there is also the ability to leverage Business Intelligence (BI) reporting through Cognos BI which comes as a product with Maximo (for assistance in enabling Cognos BI, please refer to our SCS offering)

Service Management

The philosophy of the EAMS Group Support Division is to build and maintain a collaborative and open relationship with Buyers, and harness this to provide an unparalleled support offering which is fully aligned with the evolving needs of our clients.

Clients of the EAMS Group Support Services benefit through:

- Improved system performance through our EAMS Group cloud hosted environment (Cloud Software offering)
- Access to industry expert consultants in Asset & Safety management to shape and drive ongoing continuous improvements and evolution of Asset and Safety management capability (via our Cloud Support offering)
- Access to highly skilled technical skills to ensure ongoing optimisation of the infrastructure and applications estate (via our Cloud Support offering)

Our Service Management offering can be procured at 3 levels based on the level of SaaS offering required. You choose to opt for (basic, advanced, world class). The distinction between these levels centres around the number of service hours' allocation available each month as follows:

Basic support service:

- Included free of charge as part of the basic Cloud Software solution
- Includes 20 support hours to be utilised for the resolution of incidents or service requests
- Unused hours automatically roll over to the next month's allocation (we do not adopt a use it or lose it policy)
- Services provided above and beyond the allocated hours will be charged as per the SFIA rate card
- Additional services are also available through our Cloud Support offering

Advanced support service:

- Refer to the Pricing Document for current pricing
- Includes 40 support hours to be utilised for the resolution of incidents or service requests
- Unused hours automatically roll over to the next month's allocation (we do not adopt a use it or lose it policy)
- Services provided above and beyond the allocated hours will be charged as per the SFIA rate card
- Additional services are also available through our Cloud Support offering

World Class support service:

- Refer to the Pricing Document for current pricing
- Includes 60 support hours to be utilised for the resolution of incidents or service requests
- Unused hours automatically roll over to the next month's allocation (we do not adopt a use it or lose it policy)
- Services provided above and beyond the allocated hours will be charged as per the SFIA rate card
- Additional services are also available through our Cloud Support offering

Key features of our service management offering are:

- Business Process Analysis and Improvement Consultancy (Cloud Support offering only)
    - Ability to analyse a client's use of the system(s) being supported and relate it to business processes, in order to define improvements in order to accelerate them to world class

- Asset Management System Support
    - We have the ability to support a range of packaged systems solutions covering the full spectrum of solution sets (i.e. core EAM; Mobility solutions and associated app stores; middleware integration platforms; data warehouse/BI toolsets) and integrations to external or 3rd party systems such as ERP (Enterprise Resource Planning) and Financial systems

- Service Desk Management
    - Utilising and adhering to the ITIL Framework for Service Management, service desk management is provided through best in class Zendesk software; EAMS Group provides a tailored support package which can include full level 1,2,3 support provision; integration with client IT support process and software; and comprehensive, transparent service management reporting

- Incident Management
    - Full incident management, incorporating automated adherence to service level agreements and unavailability service credit models

- Service Management and Reporting
  - Comprehensive and transparent service management reporting

- Service Monitoring
  - Proactive monitoring and reporting of all aspects of the service provision from software to infrastructure, aim to identify potential problems before they become incidents

- Change Management (Cloud Support offering only)
  - Identification and management of changes to the production environment, including full regression testing to ensure solution stability

- Configuration Management
  - The identification and management of upgrades and patches required to maintain a fully supported software environment

- Information Security Management & Governance
  - EAMS Group ensures all service provisions are compliant with the Client security management protocols and standards; EAMS Group policy; and international security management standards in line with ISO27001 and ISO27002:2013

- Systems Accounting and Auditing
  - Proactive tracking and central storage of log files, as well as the ability to provide auditable evidence of any problems or incidents

- Business Continuity/ Service Recovery
  - Robust hosted solutions aimed at providing 99.9% uptime at all times, ability to failover and restore service within minutes rather than hours

- Automated Load, Performance and Functional Testing (Cloud Support offering only)
  - Utilising enhanced toolsets to provide automated testing and analytics

- On-Call Support
  - A UK based support centre that is on-call for your business needs

- Software Licence Compliance Models
  - Ability to monitor and report on licence compliance for software managed by EAMS Group

- Training Support and Delivery (Cloud Support offering only)
  - Ability to provide day to day training and support to clients (outside of major programmes) for all solutions and products supported by EAMS Group

Service Level Agreements and Availability Credits

Severity	Definition	Target (per severity level)	Measured
1	• All or any part of the service is unavailable resulting in failure of business critical activities. Business critical activities include client services which cannot be mitigated (mitigation shall include the use of other available services); and/ or • The incident affects the overall security of the Buyer estate; and/ or • The incident has a detrimental impact on the Information Management operations of the Buyer declared by designated individuals within the Buyer's IT Department (IT Manager, Major Incident Managers, the EAMS Group Service Delivery Manager or the EAMS Group Security Manager). and/ or • The incident affects users at a critical location or more than 50% of users across all locations. • A list of severity 1 services will need definition but key services like business critical interfaces need to be included.	Service is restored or a work-around is agreed within 2 hours for 90% of incidents	24 hours, 7 days a week, including public holidays
2	Business activities are adversely affected resulting in some impact on business operations where; • The incident prevents at least one department from effectively performing key business activities; or • The incident causes a failure to redundant services that increases the risk to business critical activities.	Service is restored or a work-around is agreed within 6 hours for 90% of incidents.	24 hours, 7 days a week, including public holidays

Severity	Definition	Target (per severity level)	Measured
3	Business activities are adversely affected resulting in some impact on business operations where: ● The incident prevents users from effectively performing non key business activities; and/ or ● The Incident is limited in scope and scale. This includes equipment failures where due to redundancy and resilience, non-critical services are unaffected;	Service is restored or a work-around is agreed within 6 hours for 90% of incidents.	24 hours, 7 days a week, including public holi-days
4	● The service is not affected, e.g. queries, service requests; or ● The incident affects a service component that has a dependency on support parties that are not managed by the Buyer's IT Department; and/ or ● The incident affects a service component that cannot be fully supported	Reasonable en-deavours only.	SLA not measured.

An outage will be deemed to have started from the receipt of an incident relating to the outage to the Provider's Service Desk. The following are the targets for response for incidents based upon priority. The response made within the response target will guarantee a resolution or plan to resolve being made available to the Buyer.
The Buyer will determine, acting reasonably, into which severity category an issue falls.
The Provider shall use reasonable endeavours to respond to requests for Support Services promptly, and in any case in accordance with the following time periods:

Severity	Description	Response
4 - Info	Non- urgent	6 hours within support service hours
3 - Low	Non- urgent	4 hours within support service hours
2 - Medium	Urgent	30mins 24/7/365
1 – High	Urgent	15mins 24/7/365

In order to provision for an Out of Hours – On Call support facility, the Provider will ensure a support agent is available to respond to calls. The support agents will be rotated to cover the agreed SLA.

A forward schedule will be made internally. All incidents will route to the Provider's out of hours support agent through automated call forwarding that is triggered from the Provider's service desk solution even if a call is raised via email (once it has the correct severity).

The Provider shall ensure that it's response to a request for Support Services shall include the following information to the extent such information is relevant to the request: an acknowledgement of receipt of the request, where practicable an initial diagnosis in relation to any reported error, and an anticipated timetable for action in relation to the request.

The Provider shall use all reasonable endeavours to resolve issues raised through the Support Services promptly, and in any case in accordance with the SLA severity definitions above.

Actual support hours for any incident depends on support party availability for an affected service component as defined in the working assumptions below, as well as on the agreed severity of the incident.

The table below indicates the monthly service credits available to the Buyer should the SLA's detailed in section 3.1 not be achieved resulting in a reduction in application availability. The unavailability caused by an outage as a result of an incident or problem will be logged and tracked in Zendesk with the total length of time the unavailability occurred for recorded. This empirical data will be used to calculate any service credits for month.

We would require a review of these within 3 months once we have taken the service into support and gone beyond an agreed grace period with the Buyer.

Application Availability (%)	Service credit (% of subscription)
99.9	0
99.98 – 98.90	1%
98.89 – 97.90	2%
97.89 – 96.90	3%
96.89 – 95.90	4%
94.89 – 93.90	5%
93.89 – 92.90	6%
92.89 – 91.90	7%
91.89 – 90.90	8%
90.89 – 89.90	9%
<89.90	10%

Additional reference resources:

- EAMS Group Support Service Charter (pro-forma) available upon request

Infrastructure Management

Our cloud infrastructure is deployed utilising either Amazon Web Services (G-Cloud certified) or IBM SoftLayer (G-Cloud certified). Our infrastructure consultants are highly-skilled with experience of managing virtual cloud environments as well as Maximo software deployments meaning single instance optimised environments for Buyers can be provisioned within 4 hours.

Utilising AWS or SoftLayer creates a shared responsibility model between EAMS Group and the infrastructure provider. The provider will operate, manage and control the components from the host operating system and virtualisation layer down to the physical security of the facilities in which the services operate. In turn, EAMS Group assumes responsibility for and management of the guest operating system (including updates and security patches), other associated application software (Maximo), as well as the configuration of the provided security group firewall. This approach ensures that any hosted environment that is provisioned can be done so to meet the requirements of Buyers utilising G-Cloud services.

As part of our EAMS Group Support offering we provide capacity management of any hosted infrastructure and applications that we provide to clients. Under this approach, we proactively monitor the performance of both aspects and report on them to the client through the monthly service management meetings. This allows informed decisions to be taken with regard to when to upscale or downscale environments to keep in-line with the workload demand placed on them.

The services applied to the management of this infrastructure are:

- Patch Management
- Security Management
- Systems Monitoring
- Capacity Planning
- Incident Management
- Operational Testing
- Disaster Recovery
- Service Desk

All of the above services are managed by a skilled hosting manager who also acts as an application support manager to the benefit of our clients as they receive a more complete insight into the total operations of the application under support.

Use Case – DLR Metro: Docklands Light Railway (Keolis Amey Docklands)

The DLR Metro Production environment and Test environments are hosted within a single VPC (Virtual Private Cloud) which is segregated into 2 Public/Private Subnets for both Production and Test respectively. Internet facing components such as the IBM HTTP Server (IHS) is hosted within the Public subnets while content hosting aspects of the infrastructure related to DLR Metro such as Application Servers and Database Servers are secured in the Private subnet away from direct external access. Each of the Public/Private environment pairs is hosted within a different Amazon Availability Zone, eu-west1-a for Production and eu-west1-b for Test. An availability zone approximately equates to a physical hosting datacentre from which the design leverages an element of fault tolerance. Should the Production availability zone become inaccessible for a significant period of time, then a failover capability to the Test availability zone can be utilised in order to maintain service availability.
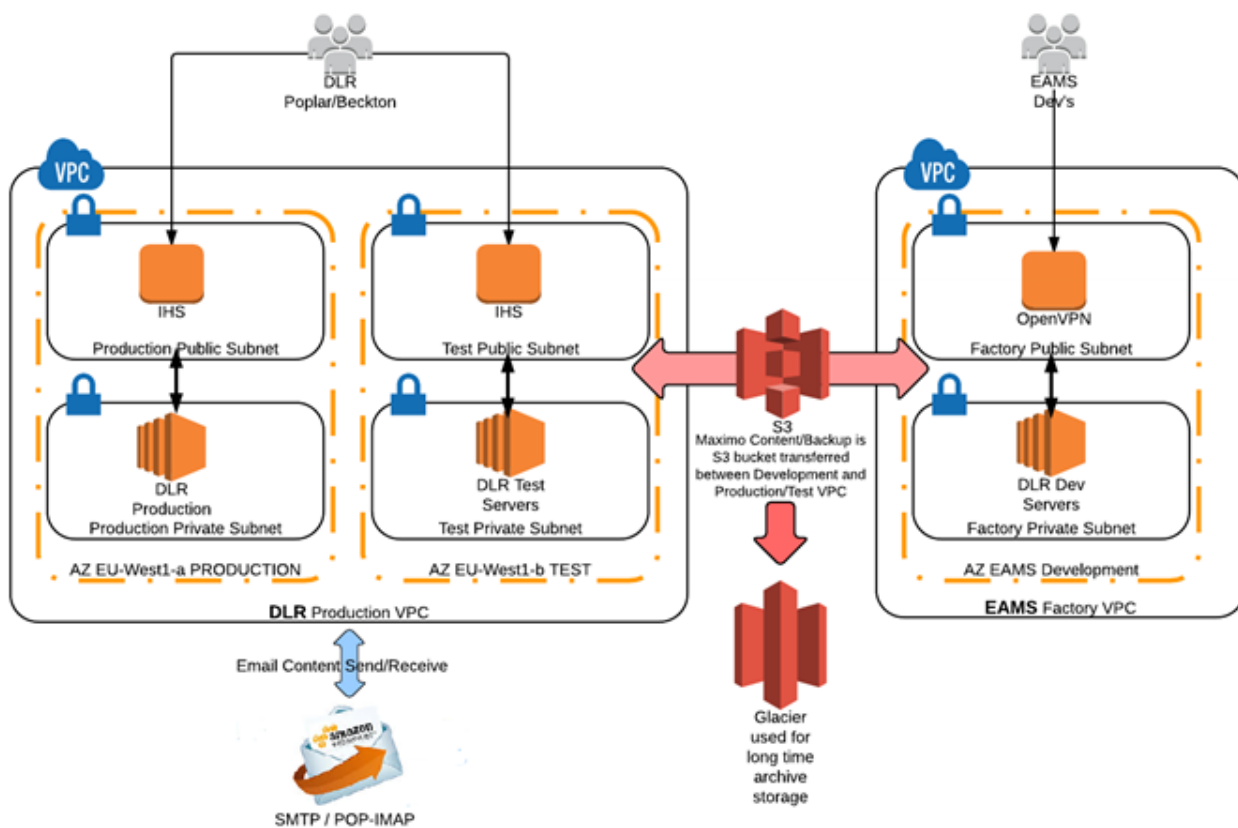
The objective of this design model is to aim to provide a 24/7/365 availability model with minimum risk of a failure or period of unavailability (outage).

Information Security Governance

The Cloud Security Guidance published by CESG lists 14 essential principles to consider when implementing cloud services. EAMS Group work closely with our infrastructure providers to ensure that the required levels of security and information governance are provided in all of our hosted solutions.

EAMS Group ensures all service provisions are compliant with the Client security management protocols and standards; EAMS Group policy; and international security management standards in line with ISO27001 and ISO27002:2013.

- Principle 1: Data in transit protection
  - Buyer data transiting networks should be adequately protected against tampering (integrity) and eavesdropping (confidentiality).
    - Network protection (denying your attacker access to intercept data)
    - Encryption (denying your attacker the ability to read data)

- Principle 2: Asset protection and resilience
  - Buyer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
    - Physical location and legal jurisdiction
    - Data centre security
    - Data at rest protection
    - Data sanitisation
    - Equipment disposal
    - Physical resilience and availability

- Principle 3: Separation between customers
  - Separation between different Buyers of the service prevents one malicious or compromised Buyer from affecting the service or data of another.
    - SaaS services built upon IaaS offerings may inherit some of the separation properties of the underlying IaaS infrastructure

- Principle 4: Governance framework
  - EAMS Group has a security governance framework that coordinates and directs our overall approach to the management of the service and information within it.

- Principle 5: Operational security
  - EAMS Group have processes and procedures in place to ensure the operational security of the service. The service is operated and managed securely in order to impede, detect or prevent attacks against it.
    - Configuration and change management
    - Vulnerability management
    - Protective monitoring
    - Incident management

- Principle 6: Personnel security
  - All EAMS Group employees will undergo an appropriate level of security screening for those individuals with access to Buyer's information or with the ability to affect their service.

- Principle 7: Secure development
  - Services are designed and developed to identify and mitigate threats to their security. Services which are not designed securely may be vulnerable to security issues which could compromise Buyer data, cause loss of service or enable other malicious activity.

- Principle 8: Supply chain security
  - EAMS Group ensure that its supply chain and any 3rd party entities satisfactorily support all of the security principles that the service claims to implement.

- Principle 9: Secure Buyer management
    - Upon mutual agreement, Buyers would be provided with the tools required to help them securely manage their services. Management interfaces and procedures are a vital security barrier in preventing unauthorised people accessing and altering Buyers' resources, applications and data.
        - Authentication of Buyers to management interfaces and within support channels
        - Separation and access control within management interfaces

- Principle 10: Identify and authentication
    - Buyer and service provider access to all service interfaces are constrained to authenticated and authorised individuals only. All cloud services will have some requirement to identify and authenticate users wishing to access service interfaces. Weak authentication or access control may allow unauthorised changes to a Buyer's service, theft or modification of data, or denial of service.

- Principle 11: External interface protection
    - All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them. If an interface is exposed to Buyers or outsiders and it is not sufficiently robust, then it could be subverted by attackers in order to gain access to the service or data within it. If the interfaces exposed include private interfaces (such as management interfaces) then the impact may be more significant.

- Principle 12: Secure service administration
    - The methods used by EAMS Group administrators to manage the operational service are designed to mitigate any risk of exploitation that could undermine the security of the service.

- Principle 13: Audit information provision to Buyers
    - Upon mutual agreement, Buyers would be provided with the audit records they need to monitor access to their service and the data held within it.

- Principle 14: Secure use of the service by the Buyer
    - EAMS Group will ensure that at all times, access to and use of the service for the Buyer and EAMS Group administrators remains secure

Additional reference Resources

- Amazon Web Services
    - AWS Compliance
    - AWS Security Centre

- IBM SoftLayer
    - SoftLayer Compliance
    - EAMS Group Information Security Governance Policy available upon request

Case Studies

DLR Metro Maximo

Business challenges
- A whole life asset management approach was contractually obligated with the award of a new DLR franchise
- The asset management system needed to service both the franchise operator and TfL's DLR who supervise the franchise contract and administer the penalty/ reward mechanisms for delivery against a complex SLA

Our approach
EAMS Group were engaged to replace SAP with DLR Metro Maximo and provide the foundation for an optimised led operating model for both the incumbent franchisee and DLRL. The Metro Maximo system supports:
- All Asset Groups and Business Units managing their business units via the DLR Metro system
- Fault Reporting Management Centre (FRMC) & Performance
- Integrated HSQE system: Inspections, IRF & Investigations
- Mobile field force delivering 8 apps (Incidents, Investigations, Work Management)

EAMS Group supplied integration to:
- SAP and SAP fault management system (awaiting phase out)
- CBCT integrating the signalling system and network operations view
- Microsoft Dynamics
- GIS

Result
EAMS Group is successfully delivering on time, within budget and delivered
- Linear and Discrete Assets
- Business Intelligence and Reporting
- Optimised Asset information Lifecycle Management
- Optimised Work Management, Planning, Scheduling, Work Delivery, Procurement and Material Management

Additional Reference Resources

Website: eams-group.com
LinkedIn: EAMS Group

Pricing Overview

The EAMS Group Maximo Enterprise Asset Management
as a Service offering is provided in three (3) variants:

Basic

Advanced

World Class

Please refer to the Pricing Document for current pricing.

Contact us

For further information, contact us at:

Email: info@eams-group.com
Phone: +44 (0) 20 3882 8448