Babcock

# Enterprise Application Store
# Government Procurement Service
# G-Cloud 15 Framework

# ENTERPRISE APPS STORE

## SERVICE OVERVIEW

The Enterprise Application Service utilises a web-based Virtual Desktop Infrastructure (VDI) to enable Government and industry partners to securely collaborate. The service provides a central repository for numerous COTS and bespoke project, programme and engineering applications and avoids desktop interoperability issues.

There are two instances of our Enterprise Application Service:

- OFFICIAL-SENSITIVE classification
- SECRET classification.

The Enterprise Application Service currently holds over 60 COTS and bespoke applications. New applications can be tested in a sandpit environment and then added to the service through a robust on-boarding process when required, removing the need to install applications on user's machines. A full list of existing applications is outlined in the table overleaf.

The Babcock Enterprise Apps Store is already utilised by over 5000+ users across UK Government Departments and their industry partners to manage and share data up to and including UK SECRET classification.

## EXAMPLES OF EXISTING APPLICATIONS

## SERVICE FEATURES

The Enterprise Application Service provides the following Customer benefits:

- Enables joint team alliancing, overcomes any local interoperability issues
- Allows access to multiple applications to enable all users all to use the same version of the software
- Allows teams / users to work collaboratively, and securely, from remote geographical locations
- Enables the sharing of information across RLI boundaries without encrypted passwords and secure hard drives
- Allows the management and storage of UK OFFICIAL-SENSITIVE or SECRET data in their respective environments
- Reduces licencing and support costs through re-use of existing procured licenses or sharing licensing with others
- Enables the segregation and management of Export Controlled Information such as ITAR (subject to relevant approvals).

# ENTERPRISE APPS STORE

| APPLICATION | O/S | S |
|---|---|---|
| Adobe Acrobat | * | |
| AIMS | * | |
| ARM | * | |
| Appian | ■ | |
| AutoDesk Suite (AutoCad, Revit, Vault, Inventor, Plant 3D, Navisworks) | ■ | ■ |
| BowTie Incident | * | |
| BowTie Server | * | |
| BowTie XP | * | |
| Cameo | ■ | |
| CAPA | ■ | |
| Crackwise | ■ | |
| Crisp | * | |
| DOORS | ■ | ■ |
| DOORS Rational Publishing Engine | ■ | ■ |
| DOORS System Architect | ■ | ■ |
| Flying Logic | * | |
| Forecast International | * | |
| ICE | ■ | |
| JIRA | ◊ | |
| LEO | ■ | |
| MCWE | ■ | |
| Microsoft Access | ■ | ■ |
| Microsoft Excel | * | ■ |
| Microsoft Lync | ■ | ■ |
| Microsoft Office | | ■ |
| Microsoft PowerPoint | * | ■ |
| Microsoft Project | ■ | |
| Microsoft Visio | ■ | |
| Microsoft Word | * | ■ |
| MOOD | | * |
| ODMS | ■ | |
| Oracle Analytics | * | * |
| Oracle Apex based apps++ | ■ | ■ |
| Oracle AutoVueShared drive | * | * |
| Oracle Business Intelligence | ■ | ■ |

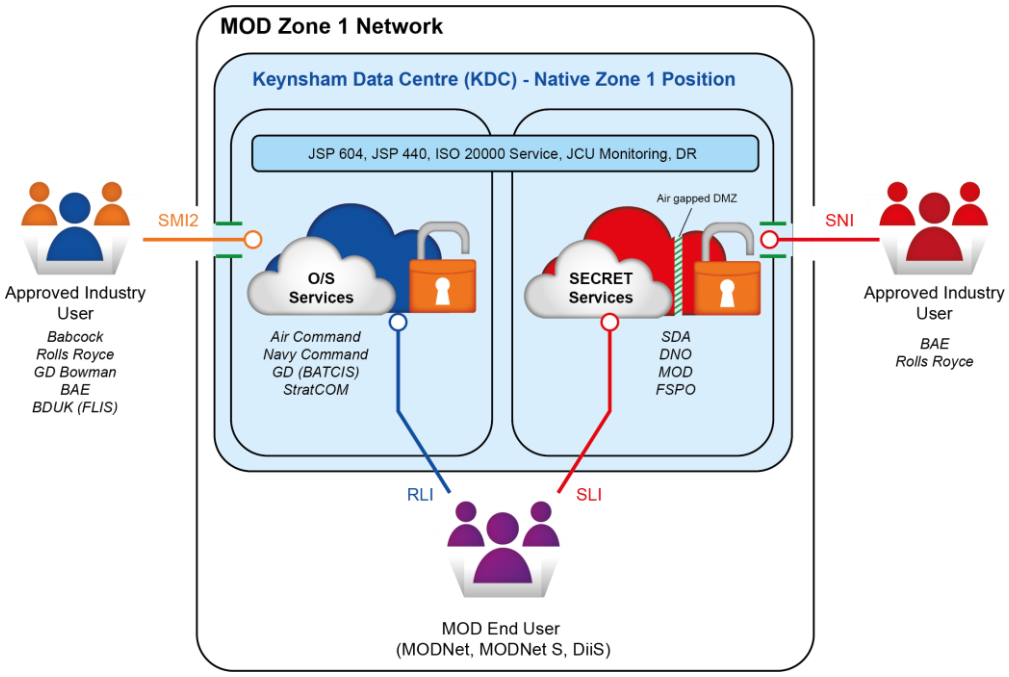
| APPLICATION | O/S | S |
|---|---|---|
| Oracle Gateway++ | ■ | ■ |
| Oracle Primavera P6 | ■ | ■ |
| Oracle Primavera Risk Analysis | ■ | ■ |
| Oracle Primavera Unifier | ■ | ■ |
| Oracle Progress Reporter (Time Reporting) | ■ | ■ |
| Oracle UCM++ | ■ | ■ |
| Oracle Web Services++ | ■ | ■ |
| Oracle WebCentre++ | ■ | ■ |
| Paramarine | | ■ |
| Pertmaster | * | |
| Power BI | ■ | ◊ |
| RAM4 | * | |
| Reliasoft | * | ■ |
| Rhino | | ■ |
| SAEM | * | |
| SCWE | | ■ |
| SEER | * | |
| Shared drive | * | * |
| Sharpcloud | ■ | ■ |
| Skype for business | * | ■ |
| SMARTER | ■ | |
| Sodius DXL Editor | * | |
| Soter | ■ | |
| Sparx EA | ■ | |
| SSMG Applications | ■ | |
| TDMS | ■ | |
| TLM Nexus Approve | ■ | |
| TLM Nexus Insight | ■ | |
| TLM Nexus Resolve | ■ | |
| TrilogiView | ■ | |
| Trueplanning | * | |
| Unity ◊ | ■ | |
| Virtual Bridge | ■ | |
| Web Access | * | |
| Work Bench | * | |

Key: ■ Existing *Previously deployed ++ Currently deployed as middleware as part of other products ◊ Being tested

# ENTERPRISE APPS STORE

## DATA CENTRE

Our IT services are operated from a UK sovereign data-centre which is accredited to hold data up to SECRET Classification. The data centre has a native MOD Zone 1a position which enables the sharing of information across RLI boundaries r Electronic Information Sharing Agreement (EISA) ap- proved industry partners and suppliers.




*SERVICES NETWORK POSITION*

## SECURITY FEATURES

The service provides the following security features:

- High Availability Service with N+1 UPS resilience
- Dual Resilient RLI and SLI connectivity
- JSP 440 and 604 compliant
- SC and DV cleared British Nationals undertaking system administration
- Conformance to at least level 3 of the Information Assurance Maturity Model (IAMM)
- Penetration testing, IT Health Checks and vulnerability assessments (LAN, RLI and SLI networks)
- Robust Business continuity plans in place with regular simulation testing undertaken
- ITAR/EAR agreed and accredited process, enabling the segregation and management of Export Controlled Information such as ITAR (subject to relevant approvals)
- Identify and Access Management capable to receive SAML 2 token and to enable more automated user account access via the MOD IdAM service.

## SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

In line with the Authority's Defence Digital Policy, our services are monitored via a number of performance and availability suites, as well as Security Information and Event Management (SIEM) monitoring and alerting systems to provide an early indication of failure points in the network, to identify service components that are not in an optimal state, or issues of a security-based nature. These systems support the NCSC Principle 11 relating to Data access/ transfer within hosted systems including provision of:

- Cyber threat detection
- Monitoring/logging capability
- Detect/log instances of misuse, malicious attack, unauthorised access and any other threat to its integrity.

# ENTERPRISE APPS STORE

Implementing one of our IT services is straight forward although it is appreciated that each team or community will have differing needs and requirements. Our team will guide you through the process establishing the required set up against the 6 considerations summarised below:

**01 Access to IT Services**

To access one of our IT services, you must have access to the RLI or SLI through either a direct network connection, an SNI/SMI2 connection or an approved Internet access method. This means that access can be achieved directly from your MODNet account or across an Industry SMI2 should you require Enterprise collaboration.

**02 Application On-boarding**

Any requirement for on-boarding of new applications will be assessed for use on the environment, including compatibility with the Government and/or MODNet build and accessibility across the network. The system will need to meet MOD accreditation standards including JSP 604, our highly trained System Support Team will assist with this process but must be sponsored and supported by the Authority appointed System Owner.

**03 System Owner**

"You will need to appoint an Authority-appointed Information Asset Owner (IAO) who will be responsible for all data holding systems. The Contractor will manage a configuration controlled register of data holdings, with data holding items being assessed against National Cyber Security Centre (NCSC) Principles for protecting bulk personal data as part of IAO approval/acceptance of any residual risk associated with operating the service. Data holdings are also assessed for privacy impact (PIA) in accordance with DPA legislation, to ensure that personal data is appropriately managed.

**04 Existing Data**

An assessment of any pre-existing data which needs to be loaded to the system is undertaken to understand any current and/or future security requirements. This can be batch loaded to the system if required.

**05 User On-boarding**

The System Owner will need to describe the business rules for user access and authorise the set-up of new user accounts you will need to provide a list of all users. All users must hold Security Check (SC) Clearance as a minimum; agree to Security Operating Procedures (SyOPs) conformance; have MOD sponsorship; provide proof of identity.

**06 System Acceptance**

We will produce a range of technical documents which may include solution proposals, functional specifications and system test scripts. These will then be used by the system owner to formally accept the proposed solution.

# ENTERPRISE APPS STORE

## ACCREDITATION

All of our IT services must achieve accreditation by the Authority prior to 'go live.'

Our team of IT security experts will support you with the engagement required with the MOD Defence Digital support teams including Network Operating Authority (NOA), release and deployment teams, Portfolio Assurance Technical Coherence Case Officer (PATC CO) and CyDR to ensure alignment with policies and frameworks such as JSP604 and accreditation for all deliveries undertaken. Ensuring that all services attain Authority to Test (ATT) and at least an Interim Authority to Operate (IATO) on way to full Authority to Operate (ATO).

## CONFORMANCE TO JSP 604

The following table provides an overview of our current deployed services against JSP 604 principles as outlined in The Defence Manual for ICT:

| RULE | LINK | STATUS | DESCRIPTION |
|---|---|---|---|
| 00 | Rule 0 | Live | ICT shall be developed against an understood business need |
| 01 | Rule 1 | Live | ICT shall be reused where available |
| 02 | Rule 2 | Live | Projects shall maximise their contribution towards the Single Information Environment (SIE) |
| 03 | Rule 3 | Live | ICT shall be developed with respect to the relevant domain architecture |
| 04 | Rule 4 | Live | ICT shall be compliant with quality of service (QOS) policy |
| 05 | Rule 5 | Live | ICT shall be compliant with domain name system (DNS) policy |
| 06 | Rule 6 | Live | ICT shall be compliant with internet protocol (IP) policy |
| 07 | Rule 7 | Live | ICT shall be compliant with messaging policy |
| 08 | Rule 8 | Live | ICT shall be compliant with electronic directory services policy |
| 09 | Rule 9 | Live | ICT shall be developed using the cross domain solutions approach defined by ISS Des Architecture |
| 10 | Rule 10 | Live | ICT shall be accredited in accordance with current policy |
| 11 | Rule 11 | Live | ICT shall comply with Op AUGITE requirements. |
| 13 | Rule 13 | Live | ICT shall be compliant with information management policy |
| 14 | Rule 14 | Live | ICT shall be developed and its performance demonstrated with respect to the environment in which it will operate |
| 15 | Rule 15 | Live | ICT shall have suitable representative test environments (RTE) available to enable through life testing to be conducted |
| 16 | Rule 16 | Live | ICT capabilities and services shall be designed to provide a high-quality product, meeting the customers' requirements for reliability, maintainability, usability and serviceability thereby permitting holistic service management. |
| 17 | Rule 17 | Live | ICT shall have defined support arrangements |
| 18 | Rule 18 | Live | ICT shall have appropriate software licenses procured and managed through life |
| 19 | Rule 19 | Live | ICT shall comply with spectrum management requirements |
| 20 | Rule 20 | Live | ICT shall comply with electromagnetic integration requirements |
| 21 | Rule 21 | Live | ICT shall be compliant with safety and environmental requirements |
| 22 | Rule 22 | Live | ICT shall be compliant with HMG Information Assurance Policy for the employment of Cryptographic Products |

# ENTERPRISE APPS STORE

Our services are supported by ISO 20000 certified IT Service Management processes to which it has held accreditation since 2009. These processes cover service, risk, incident, problem, change and release management processes to ensure that the best possible levels of service quality and availability are maintained at all times.

All services are supported by an IT Service Desk;. problems and incidents are managed in accordance with ITIL compliant processes. Incidents raised to the Service Desk are assessed against a 'priority matrix' this is derived from the contract Service Level Agreement (SLA) to identify the precedence and remedial actions.

## SERVICE LEVEL AGREEMENT

**CAT A Services:**

- Services will be available from 04:00 to 23:59, 7 days a week, 52 weeks per year (CAT A Service Availability Period);
- During the CAT A Services Availability Period the service will achieve a 95% Service Availability
- Service Response times will be as outlined in the table below:

| CAT | Priority | Definition / Typical Scenario | Response Times | Resolution Times |
|---|---|---|---|---|
| CAT A | Critical (P1) | System capability severely degraded or down.<br>Restricted service available.<br>No work round.<br>Business impact important. | 4hr response time (within service hours) | 72 hours (24x7) from call being received. |
| | Major (P2) | System capability degraded.<br>Some business impact.<br>Short term work round available. | 8hr response time (within service hours) | To be agreed with the Authority providing that the Contractor shall not be required to work to resolve the incident outside of the CAT A Services Availability Period. |
| | Minor (P3) | System capability intact but usability degraded.<br>No business impact.<br>Work round acceptable. | 2 day response time (within service hours) | 5 service days or such other period as is agreed with the Authority |
| | P4 | Service interruption affecting single user. | 2 day response time (within service hours) | 5 service days or such other period as is agreed with the Authority. |
| | P5 | A request for service or information; or update of a user's permissions. | 2 day response time (within service hours) | 5 service days or such other period as is agreed with the Authority. |
| | | Single account creation. | 2 day response and resolution time (within service hours) measured from receipt by the Contractor of authorisation from the Authority. | |
| | | An Expedited Request for service information; or an Expedited Request to update a user's permissions. | 1 day response time (within service hours) measured from receipt by the Contractor of an Expedited Request. | |
| | | An Expedited Request for a single account creation. | | |
| | | Multiple account creation. | Helpdesk Response and resolution within such period as is agreed with the Authority | |
| | | A request for change. | To be processed as agreed in accordance with the Change Procedure. | |

# ENTERPRISE APPS STORE

## SERVICE MANAGEMENT

Our service is constantly monitored and measured for performance. Reports are produced on a daily basis to capture the supply and demand on the service. Metrics and reports can be provided on request, subject to security arrangements, these may include but are not limited to the following: Bandwidth, Capacity, Usage and Processing Speed.

## SCHEDULED MAINTENANCE

The system requires routine and planned maintenance which will result in temporary interruption to the managed service. Babcock will tightly manage the schedule of this work and will provide the client with appropriate notice of any downtime needed. Planned maintenance will normally be performed outside of the Working Day and will have at least 5 working days' notice.

## BACK-UP/RESTORE AND DISASTER RECOVERY

Backups of data are made on a daily, monthly and yearly basis.

Babcock have a robust disaster recovery and Business Continuity process which includes a mobile IT recovery service which is able to deliver and restore replica capability should an unprecedented event occur.

## TRAINING

Training can be provided at a UK site of your choice at the man-day rates as defined in the Skills For the Information Age (SFIA) rate card. Training material is available to all users of the system and includes FAQ's and set-by-step diagrams to walk users through common procedures.

## ORDERING AND INVOICING PROCESS

The Babcock Enterprise Apps Store can be purchased using a Purchase Order or G-Cloud Call off agreement and is invoiced on a 30 day payment terms. Costs quoted are exclusive of VAT and any additional taxes and expenses unless otherwise stated.

## TERMINATION TERMS

Should the customer wish to terminate the service at the end of the agreed period then the notice period as defined in the Supplier Terms will apply.

## DATA RESTORATION / SERVICE MIGRATION

Data will be held on our backup tapes for up to a year after cessation of the contract. After such time we cannot guarantee that the data can be retrieved. Any retrieval of the data held on our systems after a year will be subject to an annual charge which will be priced at point of contact.

## CUSTOMER'S EQUIPMENT

As a minimum use of the service will require the following:

- Access to the Internet, RLI, SMI2, SLI or SNI SECRET Shared Zone, with the appropriate end device to access the different cloud based services.

# ENTERPRISE APPS STORE

## CUSTOMER'S RESPONSIBILITIES

The customer is responsible for the following:

- Adherence to MOD or Government security Policy
- Undertaking the necessary Security Checks for all users to be provided access to the system
- Adherence to SYOPS by their users
- Ensuring that user's access privileges are correctly defined and regularly reviewed
- 'Offline' handling and distribution of All Sensitive information
- Connection and maintenance of their user device to access the cloud-based service (RLI, SLI, SNI SECRET Shared Zone)
- Observance of the fair usage policy
- Control and management of controlled information, including correct labelling of ITAR
- Identification of Information Assurance Owner (IAO)
- All users of the system must meet the following criteria
    - Security Check Clearance
    - Meet Government security criteria including conformance with:
    - Security Operating Procedures (SyOPs)
    - MOD or Government Sponsorship
    - Proof of identity
    - RLI/SLI access is required to access the service either through a direct network connection, SMI2 , ALI or SNI connection or an approved Internet access method.

Each on-boarded application and/or data will be subject to User Acceptance Testing for verification by the Customer and acceptance of the on-boarding process into service

## TRIAL SERVICE

Although no free trial service is available at this time, we have a dedicated Team who are happy to work with our customers to test applications not already hosted to investigate their applicability for the service. This can include interactive user sessions and demonstration of our capability.

## OFF BOARDING

The off-boarding process for the removal from the system is as follows:

- Formal notice is given for the termination of the service (90 days notice)
- Access to the customer specific workspace is removed
- Should you require your data to be extracted at the point of exit a discontinuation fee will be applied, this is subject to the amount of data and security level of data held on the system
- Data will be held on our backup tapes for up to a year after cessation of the contract. After such time we cannot guarantee that the data can be retrieved. Any retrieval of the data will be subject to an annual charge which will be priced at point of contact.

Email: digital.solutions@babcockinternational.com

Babcock