



Enterprise Collaboration Service G-Cloud 15 Framework

ENTERPRISE COLLABORATION SERVICE

SERVICE OVERVIEW

The Babcock Enterprise Collaboration Service is a web based work-space that is hosted within the MOD secure cloud. The service can be used to manage, store and securely distribute information up to and including UK OFFICIAL-SENSITIVE classification in the RLI connected system. The capability provides a single information environment to allow for secure access control management and auditability, whilst supporting Enterprise collaboration.

The Enterprise Collaboration Service is one of the largest Collaborative Working Environment (CWE) in use across the UK Defence sector, with 10,000 users across a range of UK Government Departments and approved Industry Partners.

The Enterprise Collaboration Service can be accessed by Dii (F)/MODNet (R) end-user devices and can also be utilised by Industry Partners with RLI, either via a Secure Managed Interface (SMI2) gateway service or via an approved end user device.

There is also a SECRET Collaborative Working Environment (SCWE) which can be used to manage information up to UK SECRET classification with user access via Dii (FS)/MODNet (S) across the SLI connected system.

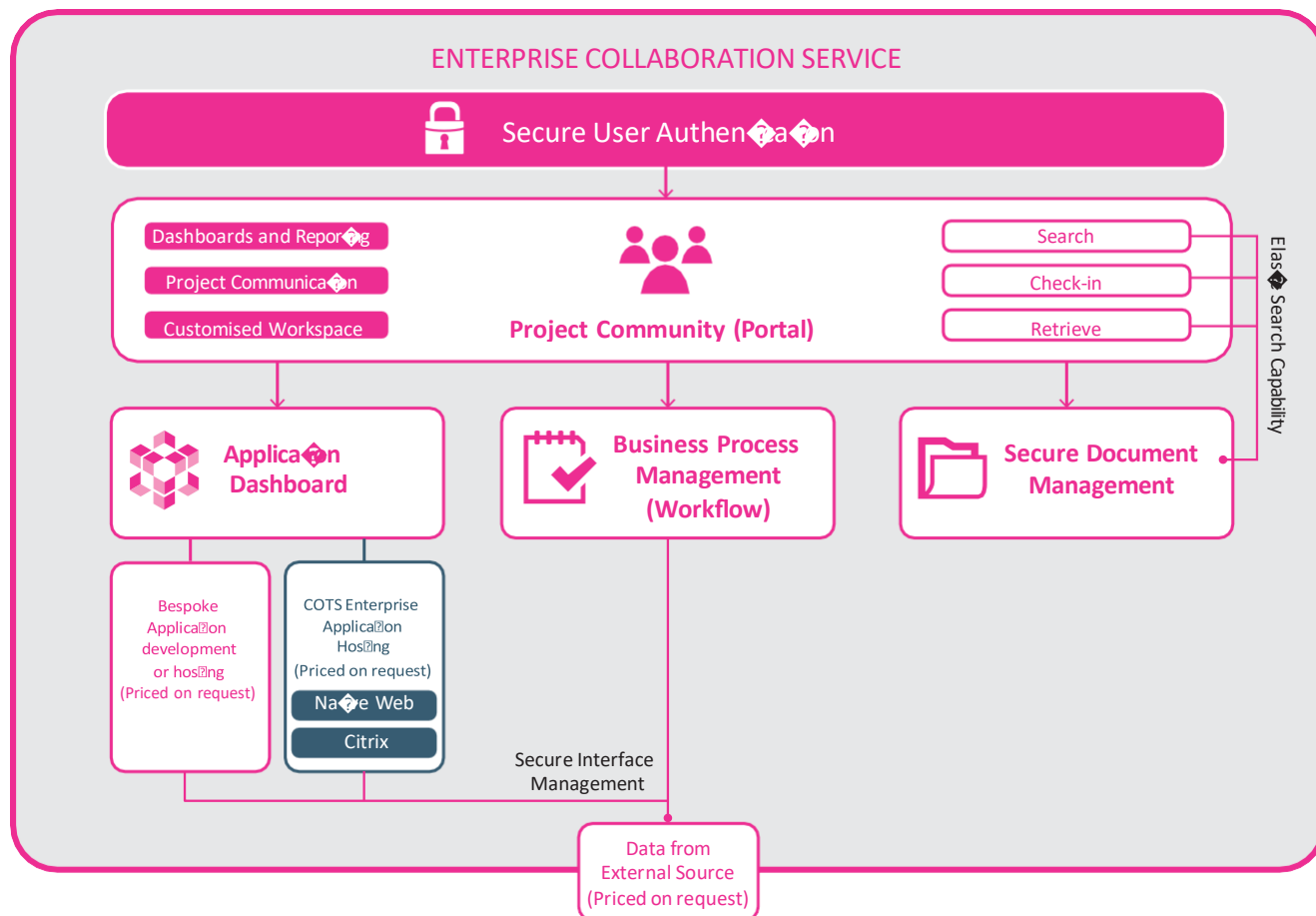
Our service is hosted from our UK based, DAIS approved data centre and conforms to all relevant UK Government standards and policies including JSP440 and JSP604. In addition, our service has an impressive history of operating at 99% availability for the past 10 years; this is supported by our ISO20000:2011 accredited IT Service Management processes to which Babcock has held accreditation since 2009.

Our service can be utilised to manage Assets Subject to Special Controls (ASSC) including; Defence Articles and Technical Data subject to International Traffic in Arms Regulations (ITAR), Export Administration Regulation (EAR), Personal, Financial, IPR and PSA data and can be enhanced to accept Identity and Access Management (IdAM) attributes for additional access control and distribution.

A single information environment enabled by Information and Communications Technology (ICT) to allow for effective and efficient secure access control management and auditability, whilst supporting Enterprise collaboration.



The Enterprise Collaboration Service consists of four main components; Project Community (Portal), Application Dashboard, Workflow and Secure Document Management capability.



SERVICE BENEFITS

The Enterprise Collaboration Service provides the following Customer benefits:

- Enables joint team alliancing and provides Enterprise Business Workflows that can be integrated into other systems
- Allows teams / users to work collaboratively, and securely, from remote geographical locations
- Enables the sharing of information across RLI boundaries without the need for encrypted passwords or, USB Sticks or standalone network drives
- Allows the management and storage of UK OFFICIAL-SENSITIVE or SECRET data in their respective environments and includes caveats such as NNPI, IPR, ITAR/EAR etc

SERVICE FEATURES

- Administration rights to allow end-user customisation of work-spaces to meet team / project needs from a vast array of out-of-the -box functionality features;
- Flexibility to allow specific applications to be developed and deployed within the application;
- Includes a Document Review workflow to enable multi-step document approvals and audit trails;
- Provides secure web-based portal entry with dedicated access controls and authorised permissions lists to enable wide collaboration or “Need to Know” principles.
- Integration with a low code workflow capability to enable complex digital process automation.

- Single sign-on links and an application links portal that allows the user a single place to reach out to other systems
- A powerful content crawler and search facility including full text retrieval service
- Can be further enhanced with data feeds from other systems, Business Intelligence reporting and a Virtual Desktop Infrastructure (VDI)
- Identify and access Management enabled to future proof for Automated Secure Access Management and automated account management processes

USER AUTHENTICATION

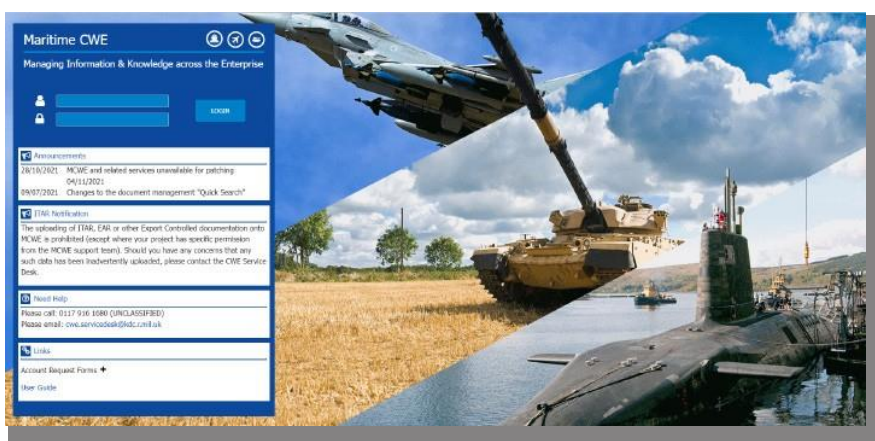
Access to the Enterprise Collaboration Service is managed via a Secure web-based portal entry with dedicated access controls and authorised permissions lists.

PROJECT COMMUNITY HOMEPAGE (PORTALS)

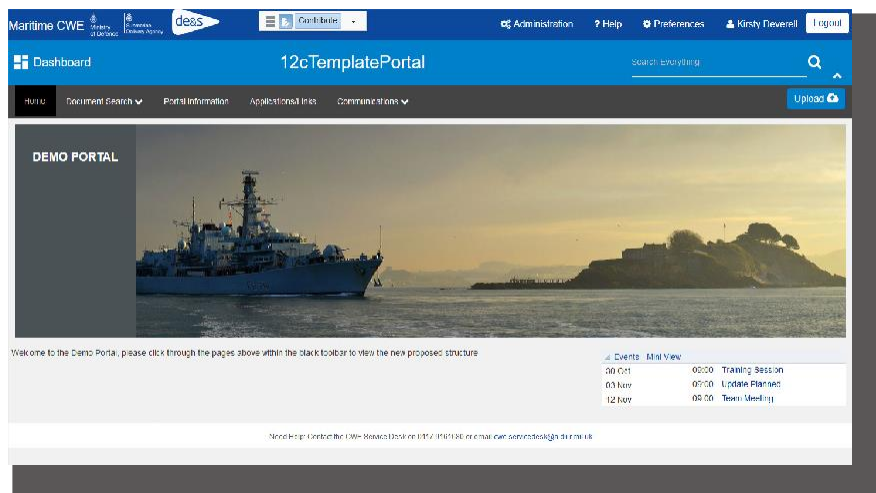
A key feature of application is the ability to create unique workspaces and communities tailored to specific user requirements. Administration rights will be given to selected users to allow customised workspaces to meet team / project needs.

Portal functionality includes:

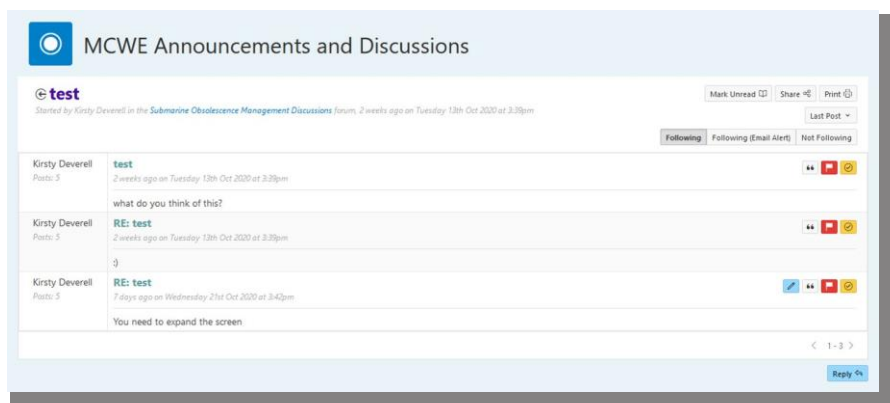
- Personalised Virtual Space, providing personal document storage, scheduling calendar, to do lists and key contact information
- Interactive Community Homepage – with notice areas, discussion boards, address book, key documentation store and simplified customisation toolset
- Social Media - the provision of community Wikis, Blogs and Polls
- Links to the document management system, workflows and Enterprise Applications
- Fully customisable project space to meet customer requirements



SECURE USER AUTHENTICATION



EXAMPLE PORTAL



ANNOUNCEMENTS AND DISCUSSIONS

SECURE DOCUMENT MANAGEMENT

A core component of the Enterprise Collaboration Service capability is the secure document management functionality. This capability delivers an enterprise solution which meets The Authority's Information Assurance (IA) requirements including JSP 440 and 604.

The document management system utilises meta-data sets and Access Control Lists (ACL's); this allows Customers to control who has access to what information based on "Need to Know" principles.

Granular ACLs, supported by a robust on-boarding work instruction, govern access to documentation and records held within applications offered within the bounds of the applications and service products.

ACL's can be tailored to meet specific project or community's requirements using portal and check in profile templates. These templates help to agree all information naming conventions and reference schemes (meta-data tags) and are agreed by The Authority prior to implementation and access to the system being granted.

The document management capability ensures strict version control with 'check-in and check-out' functionality. This is supported by a full audit log which will specify who has updated the content and when the last version was published.

The capability is accredited to hold Assets Subject to Special Control (ASSC) including ITAR information and includes caveats such as NNPI, IPR, ITAR/EAR etc subject to MOD Sponsorship.

GRANULAR SECURITY SETTINGS USED TO MANAGE INFORMATION ON A 'NEED-TO-KNOW' BASIS

ELASTIC SEARCH CAPABILITY FROM PORTAL

BUSINESS PROCESS MANAGEMENT (WORKFLOW)

The capability include access to a powerful intelligent Business Process Management System (iBPMS) to support dynamic case management (DCM) and digital process automation (DPA). Our automated workflows have streamlined and enabled quicker completion of repeatable business tasks. This minimises errors and increases overall efficiency. The extra time gained allows teams to make quicker, smarter decisions and empowers employees to collaborate in a more productive and agile way. Workflows have also helped to:

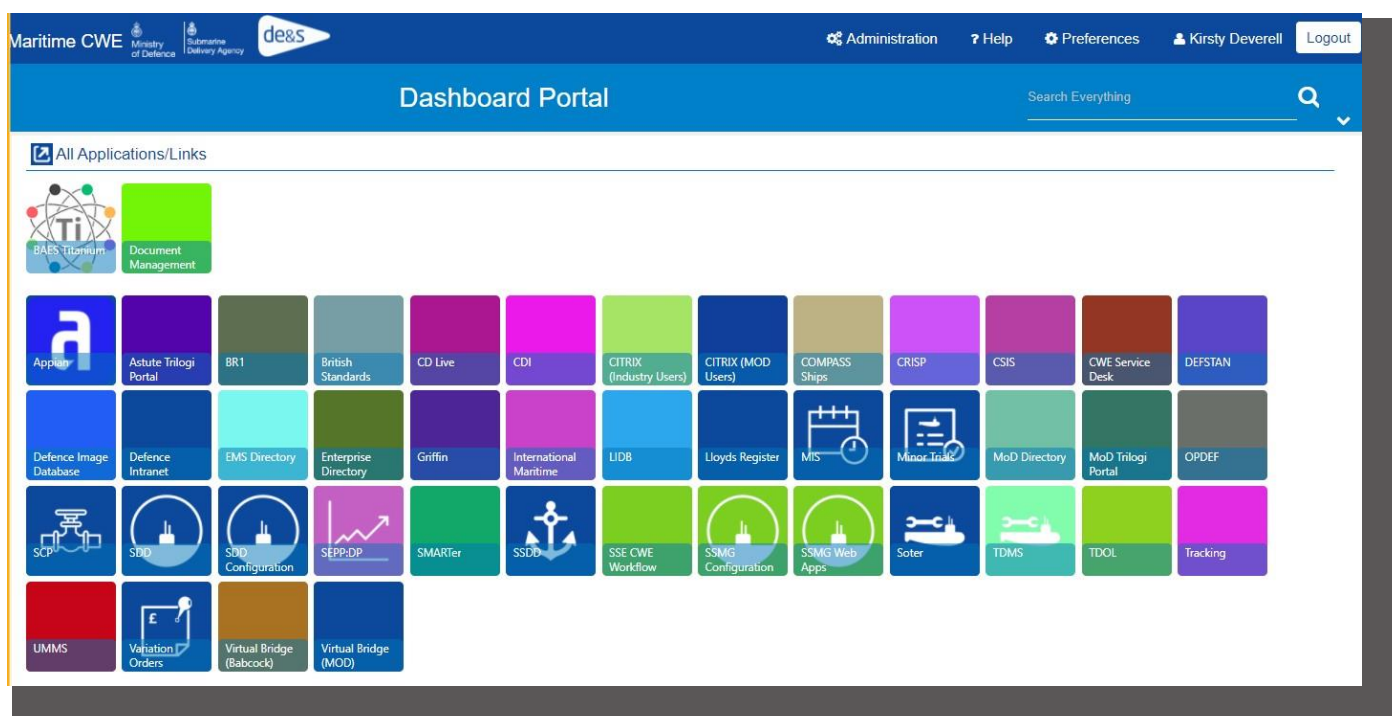
- Identify Redundancies.
- Increase Accountability and Reduce Risk
- Improve communication
- Provide better customer visibility
- Improve the quality of data and safety

Our team of business analysts and application developers can support Customers through capturing, transforming and streamlining existing business process and turning these into real life digital solutions. Workflows are priced on a case-by-case basis.

APPLICATION DASHBOARD

The portal can be configured to hold an application dashboard which links directly to bespoke and COTS applications on requests.

Links to external systems can also be provided; these may require separate log-in but the dashboard provides a user-friendly way for teams to access their chosen project tools from one location. These services are also available via the Digital Marketplace as 'Enterprise Application Store.'



EXAMPLE APPLICATION STORE

SECURITY FEATURES

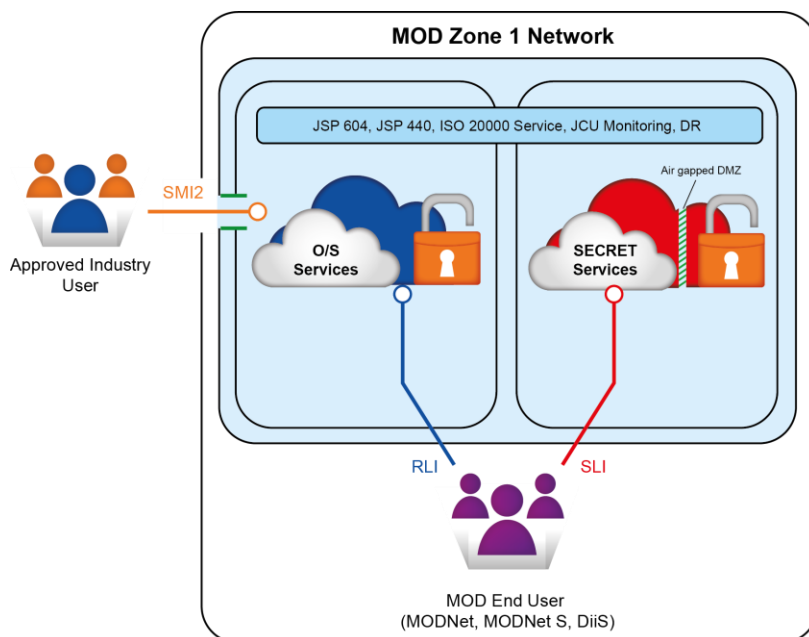
The service is operated from a UK Sovereign datacentre which is accredited to hold data up to SECRET Classification. The datacentre has a native MOD Zone 1a position which enabling the sharing of information across RLI/SLI boundaries with EISA approved industry partners and suppliers via an industry SMI2 or SLI connection.

The service provides the following additional security features:

- High Availability Service with N+1 UPS resilience
- Dual Resilient RLI 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 and vulnerability assessments (LAN, RLI, SMI2 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 capability capable to receive SAML 2 token and to enable more automated user account access via the MOD IdAM service

In line with The Authority's Defence Digital Policy, the service is 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.



CAPABILITY NETWORK POSITION

The screenshot shows the 'Maritime CWE Content Check-In Form for Maritime CWE Profile'. The form is divided into several sections with expandable/collapsible headers. The 'Content Information' section includes fields for Title, Author, Security Group, Security Account, Release Date, Content ID, and Revision. The 'Retention Schedule' section includes fields for Retention Schedule, Expiration Date, and Additional Fields. The 'Additional Fields' section includes fields for Owner, Content Type, External Issue Number, External Issue Ref, External Issue Date, Category, Proprietary Information, Copyright Clearance, Library Ref, and Security Marking. The 'Security Marking' section includes fields for Security Profile, Security Marking, and Security Descriptor. The 'Search Terms' section includes a field for Search Terms. The form is titled 'Content Check-In Form for Maritime CWE Profile' and includes a 'Log In' button in the top right corner.

GRANULAR SECURITY SETTINGS USED TO MANAGE INFORMATION ON A 'NEED-TO-KNOW' BASIS

ACCREDITATION

All 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

SERVICE MANAGEMENT

The Enterprise Collaboration Service is supported by our ISO 20000 certified IT Service Management processes to which it has held accreditation since 2009. Since accreditation, there have been zero non-conformance at any stage of our ISO 20000 periodic assessments. 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.

SERVICE LEVEL ARRANGEMENTS

The Standard support service for the Enterprise Collaboration Service is as follows:

- The System will be available during the hours 04:00 - 23:59, 7 days a week
- 95% Target SLA (Outside Scheduled Downtime)- Infrastructure and Applications may be available at times outside of the target availability hours stated above.
- Manned helpdesk support from our trained operators during the following office hours:
 - Monday to Thursday – 07:30 to 17:00 (excluding weekends, UK bank holidays and Christmas shut-down period) UK time.
 - Friday – 07:30 to 16:00 (excluding weekends, UK bank holidays and Christmas shutdown period) UK time.
- Out of hours support can be arranged at additional cost.

Enhanced services can be provided on request and these will be priced on a case-by-case basis.

In the event of an unexpected occurrence, Babcock will record such occurrence as a separate technical issue. Those technical issues will be reviewed and prioritised in line with the table below to ensure that business critical needs are met as soon as possible:

Priority	Definition / Typical Scenario	CAT A Response Times	CAT A Resolution Times
Critical (P1)	System capability severely degraded or down. Restricted service available. No work round. Business impact important.	4hr response time (within service hours)	72 hours (24x7) from call being received.
Major (P2)	System capability degraded. Some business impact. Short term work round available.	8Hr response time (within service hours)	To be agreed with the Authority
Minor (P3)	System capability intact but usability degraded. No business impact. Work round acceptable.	2 day response time (within service hours)	5 service days or such other period as is agreed with the Authority
Request for System Enhancement (RSE) / Request for Change (RFC) (P4)	A Customer requested change to the agreed scope or design	5 day response time (within service hours)	5 service days or such other period as is agreed with the Authority

CUSTOMER'S RESPONSIBILITIES

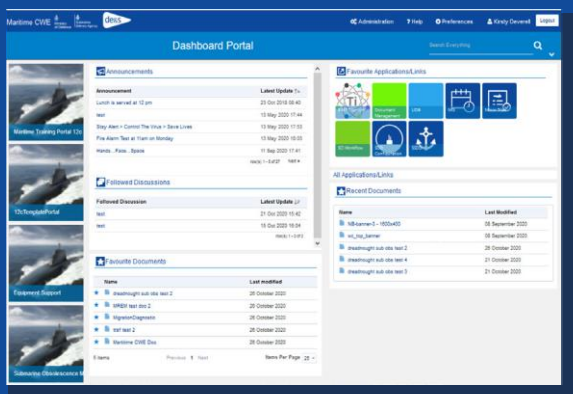
The customer is responsible for the following:

- 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)
- Observance of the fair usage policy;
- Control and management of controlled information, including correct labelling of ITAR;
- Identification of Information Assurance Owner (IAO).

ON BOARDING & OFF-BOARDING

The setting up of a new community and the addition of users will follow defined business implementation processes to ensure the service provided meets the customer requirements:

NEW COMMUNITIES



EXAMPLE NEW COMMUNITY HOMEPAGE

- Each new community is subject to a one off set up fee which is dependent on the amount of data to be loaded to the system and any non-standard functionality which the community requires;
- RLI, SMI2 or SLI access is required and we can help you with the connectivity required;
- All Communities will require a System Information Asset Owner (IAO) who will own the information risk and describe the business rules for user access, authorise the set-up of new user accounts.

NEW USERS

Once the new community is established, a list of new users will need to be provided. All users of the system must meet the following criteria:

- Security Check Clearance;
- Meet Government Security Operating Procedures (SyOPs);
- MOD Sponsorship.

All users of the system will access to the Training community Space which provides a range of training material including process flow summaries, downloadable user guides and animated tutorials.

NEW USER ACCOUNT FORM

SERVICE MANAGEMENT

The Enterprise Collaboration Service is supported by our ISO20000 certified IT Service Management processes to which it has held accreditation since 2009. Since accreditation, there have been zero non-conformance at any stage of our ISO20000 periodic assessments, we have also invested in a world class fully integrated Configuration Management Database to ITIL standards. 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.

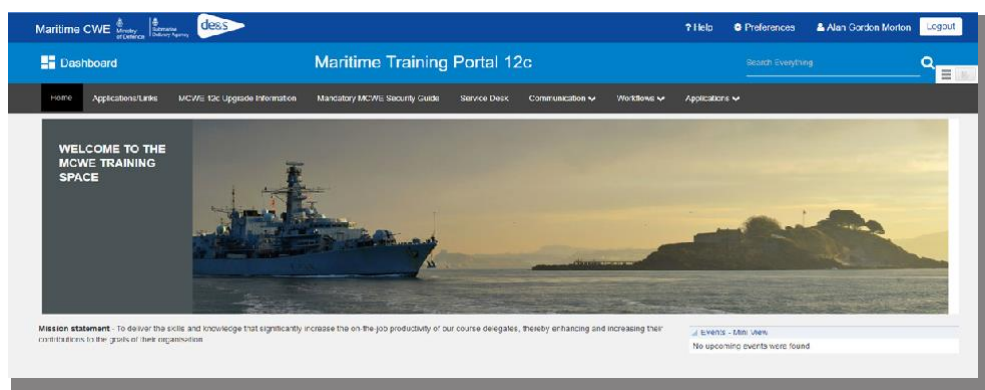
SCHEDULED MAINTENANCE

The system requires routine and planned maintenance which will result in temporary interruption to the managed service. The Service desk 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.

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. Training takes various forms including:

- Floor walking;
- At-desk support – either requested through the service desk, provided ad-hoc or as a result of following up support calls which have been raised on the system;
- Classroom-based training (either on-site or at The Contractor-provided training facilities).



TRAINING PORTAL

Every new user of the system is required to undertake mandatory training; this is provided as e-learning content and requires yearly refresher training to maintain access. Customers have ongoing support readily available in the Training Portal. Modular training is available to a Account Holders, delivered using PPT Shows, User Guides and Desk Top Instructions. Refresher training is also provide to experienced users when there has been a system update or the user is out of practice.

BACK-UP/RESTORE AND DISASTER RECOVERY

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

ORDERING AND INVOICING PROCESS

The Babcock Enterprise Collaboration Service 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 a 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, or SLI with the appropriate end device to access the different cloud based services.

TRIAL SERVICE

Although no free trial service is available at this time, we have a dedicated Capability Team who are happy to provide demonstrations of the Collaboration Service capability. This can include interactive user sessions and demonstration of our capability suite.

SUPPLIER TERMS

Babcock can confirm that it accepts the G-Cloud Framework Agreement. Babcock's supplier terms are included as a separate attachment.

PRINCIPAL LOCATIONS WHERE THE SERVICES ARE BEING PERFORMED

The service can be deployed for Government departments on premise; in a secure Datacentre or within a UK Tier 2 Datacentre across the MOD RLI, SLI or SECRET shared zone (SSZ).

QUALITY STANDARDS

Our Quality Management System is accredited to ISO9001 and TickIT plus which gives an increased emphasis on our process capabilities in order to deliver future service provision improvements. Our service desk is so accredited to ISO20000:2011 for IT service management systems. Babcock also has an embedded assurance culture where Information Assurance and security is part of normal business. Babcock are proud to have been independently assessed as meeting and maintaining Information Assurance Maturity Model (IAMM) level 3 and we are constantly striving to improve and implement strategies and plans to move to the next level, where IA and security are not just an asset to the business, but also business enablers.

TECHNICAL STANDARDS

Babcock, wherever possible, utilises Open standards in their managed service and applications. As such, the service supports a number of Open Standards including:

- HTTP
- HTTPS
- XML
- XLS
- REST
- JSON
- GZIP
- REST
- SOAP

Email: digital.solutions@babcockinternational.com



Babcock