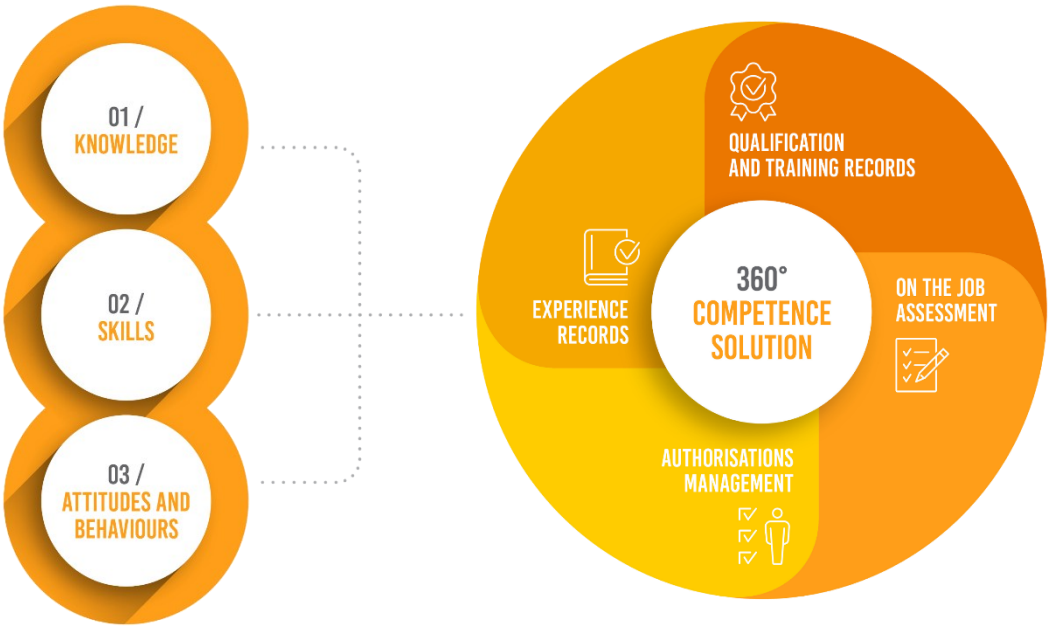
ELMS Competence and Compliance Solution – Service Definition

1. Service Overview

The ELMS Competence and Compliance solution is a multi-tenant Software-as-a-Service (SaaS) platform designed for use by public sector organisations. The service enables customers to manage workforce competence, training, certification, and compliance evidence within a secure, auditable, and centrally managed system. ELMS is explicitly aligned to modern competence frameworks, focusing on the core elements of knowledge, skills, attitudes, and behaviours, ensuring that organisations can demonstrate not only qualification and training status, but also real-world capability and operational readiness.



The service supports regulatory compliance, operational assurance, and risk management through four cornerstone modules that work together to deliver a complete competence lifecycle.

These include the tracking, management, and reporting of personal qualifications and training records; structured competence assessments mapped to role and task requirements; task experience and recency management to evidence ongoing proficiency; and authorisation management with gated, role-based workflows to ensure only suitably competent individuals are permitted to perform controlled activities.

The service is fully managed by the supplier and operated under an Information Security Management System (ISMS) certified to the ISO/IEC 27001:2022 standard.

2. Information Assurance and Security Governance

- The service is operated under a documented ISMS certified to the ISO/IEC 27001:2022 standard.
- Information security risks are identified, assessed, and treated through a formal risk management process.
- Security policies and procedures are reviewed regularly.
- Supplier personnel with access to production systems are subject to appropriate screening and mandatory security awareness training.
- The service is designed to support UK Data Protection and GDPR obligations.

3. Data Backup, Restore, and Disaster Recovery

3.1 Data Backup

- Customer data, configuration data, and uploaded content are backed up automatically at least once every 24 hours.
- Backups are encrypted and stored securely in geographically separate locations (MS Azure UK West and North Europe data centres).
- Backup retention periods are defined, documented, and reviewed.

3.2 Data Restore

- Point-in-time restoration is supported subject to backup availability.
- Restore operations are controlled, authorised, and logged.
- Target objectives:
    - **Recovery Point Objective (RPO):** ≤ 24 hours
    - **Recovery Time Objective (RTO):** ≤ 1 business day for standard incidents

3.3 Business Continuity and Disaster Recovery

- Business Continuity and Disaster Recovery Plans are documented, maintained, and tested periodically.

- The service architecture is designed to reduce single points of failure.
- Major incidents are managed under a formal incident management process with timely customer communication.

4. Onboarding and Offboarding

4.1 Onboarding

Onboarding support includes:

- Secure tenant provisioning
- Configuration of users, roles, permissions, and workflows
- Controlled data import using approved and documented methods
- Administrator training and supporting documentation

Access is provisioned using the principle of least privilege.

4.2 Offboarding

- Customers may request a full export of their data in a commonly used, machine-readable format (e.g. CSV, JSON).
- Data exports are provided securely.
- Following contract termination and any agreed exit period, customer data is securely deleted in line with documented retention and disposal procedures.

5. Service Constraints

5.1 Maintenance Windows

- Planned maintenance is typically carried out outside standard UK public sector business hours.
- Customers are notified in advance of maintenance activities that may affect availability.

5.2 Customisation

- The service supports configuration through standard platform functionality.

- Bespoke development or code-level customisation is not included unless explicitly agreed.
- All changes are subject to formal change and release management controls.

6. Service Levels

6.1 Availability

- Target service availability: **≥ 99.5% per calendar month**, excluding planned maintenance.

6.2 Performance

- The service is designed to support expected concurrent usage with reasonable response times.
- Capacity, performance, and availability are monitored proactively.

6.3 Support Hours

- Standard support hours: Monday to Friday, UK business hours (excluding public holidays).
- Enhanced or extended support options may be available by agreement.

7. After-Sales Support

After-sales support includes:

- Access to a service desk for incident, problem, and service request management
- Ongoing maintenance, bug fixes, and security updates
- Platform updates and enhancements
- Access to user and administrator documentation

Support requests are prioritised and managed based on impact and urgency.

8. Technical Requirements

8.1 Customer Requirements

- Modern, supported web browsers
- Secure internet connectivity
- Customer-managed end-user devices and local networks

8.2 Integration

- Secure APIs may be provided for integration with approved third-party systems.
- API access is authenticated, authorised, rate-limited, and logged.

9. Outage and Maintenance Management

- Service availability and security events are monitored continuously.
- Incidents are logged, assessed, and resolved in line with documented procedures.
- Customers are notified of significant outages or security incidents without undue delay.
- Post-incident reviews are conducted where appropriate.

10. Hosting and Data Location

- The service is hosted on enterprise-grade cloud infrastructure (MS Azure).
- All customer data is hosted within MS Azures UK West and North Europe data centres unless otherwise contractually agreed.
- Logical segregation is enforced between customer tenants.

11. Access to Data Upon Exit

- Customers retain full ownership of their data.
- Data is made available for secure export during an agreed exit period at contract termination.

- Following completion of exit activities, customer data is securely deleted unless legal or regulatory retention obligations apply.

12. Security Controls

12.1 Access Control

- Role-based access control (RBAC)
- Strong authentication mechanisms (MFA)
- Optional integration with single sign-on (SSO)

12.2 Cryptography

- Encryption of data in transit using TLS
- Encryption of data at rest using industry-standard algorithms

12.3 Logging and Monitoring

- Security-relevant events are logged and monitored
- Audit logs are available for administrative and user actions

12.4 Vulnerability Management

- Regular vulnerability scanning and patch management
- Security updates applied based on risk, severity, and impact