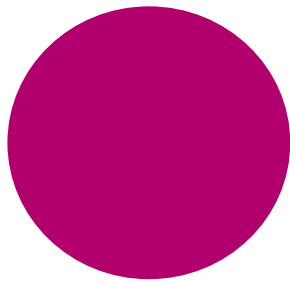

APPROVED TRAINING ORGANISATIONS (ATOs)

E-learning/e-assessment strategy



Sept
2019

CONTENTS



Introduction	1
CITB's aims and objectives	2
Scope	3
Examples	4
E-learning	4
E-assessments	4
Validity and reliability of e-learning and e-assessment	5
Security	6
Data integrity – input and output	7
Operation of systems	8
Integrity of systems	9
Access to e-learning	10
Preventing barriers to entry	11
Business continuity and disaster recovery	12
Automatically generated on-demand tests	13
Test conditions and test environment	14
System familiarisation for trainers, invigilators, moderators and administrators	15
Design, development and delivery of materials	16
Appendix	17
Glossary	17
References	17

Introduction

The increasing use of technology within the vocational education sector for the development, delivery, administration and reporting of e-learning and e-assessment requires a robust and consistent approach that delivers safe and reliable results.

This document sets out CITB's requirements, which address the use of e-learning and e-assessment where it is felt that CITB needs to apply a standardised and consistent approach.

It has been written to support the specific nature of this delivery media. It is intended to support flexibility and encourage innovation.

This document must be used in conjunction with the following documents, where applicable.

- CITB Requirements for Approved Training Organisations.
- CITB Short Duration Standards.
- CITB Scheme Rules (Site Safety Plus).

These documents may change from time to time. Current versions are available at www.citb.co.uk/standards-and-delivering-training/

All Approved Training Organisations (ATOs) and 3rd party organisations are expected to comply with these requirements wherever technology has been used to assist the delivery of a short duration standard, in part or in full, and where the technology enables the assessment of a short duration standard.

Quality assurance of e-learning and e-assessment systems will be incorporated within the approval, self-assessment and monitoring visits. Approved Training Organisations and 3rd party organisations will be required to address any actions highlighted.

Lists of legislation, and best practice and industry standards are included at the end of this document. (*Refer to Appendix on page 17.*)

CITB's aims and objectives

- Use technology that meets an equivalent standard for a traditional classroom-based training course whilst encouraging flexibility and innovation.
- Encourage the uptake of innovative forms of learning and assessment.
- Ensure that Approved Training Organisations and 3rd party organisations have a robust approach to e-learning and e-assessment.
- Ensure the integrity, reliability and validity of e-learning and e-assessment are upheld, and facilitate and support innovative training and assessment practice.
- Ensure that quality assurance of e-learning and e-assessment reviews the following principles.
 - **Relevant.** The course outputs genuinely meet the requirements of the training standard.
 - **Reliable.** The course produces the same results irrespective of the time, location, cohort or context under which the e-learning or e-assessment is delivered.
 - **Efficient.** The system is high quality, easy to use and facilitates the entry of all delegates.
 - **Positive.** The system and course is trusted by delegates and employers and delivers the right outcomes. The experience is open, transparent and accessible.
 - **Learning.** Continuous learning and review is part of a cyclical plan for the approved training provider.

Scope

This document details the requirements for developing and operating e-learning and e-assessment, and their supporting systems for Approved Training Organisations. To become an Approved Training Organisation refer to our website: www.citb.co.uk/standards-and-delivering-training/approved-training-organisations/

E-learning and e-assessment, for the purpose of this document, are defined as the use of electronic systems for the development, operation and delivery of learning materials and assessments that contribute to the achievement of a short duration standard.

In addition, the implications of using electronic means for the generation, delivery and administration of learning and assessment or the calculation of results are included in the scope of what is quality assured.

CITB will examine the extent to which the quality assurance of e-learning and e-assessment is needed through consideration of the course purpose and outcome of the achievement (for example, leads to a competence card or CPD knowledge update).

Examples

E-learning

The term *e-learning* denotes any type of learning that has an electronic component and incorporates one or more of e-learning, e-testing and/or e-assessment. The following examples of e-learning illustrate the potential scope and range of different uses. This list is not exhaustive.

- Learning that is distributed, completed and administered electronically using an intranet or local work stations.
- Learning that is distributed, completed and administered electronically using the internet.

E-assessments

- Assessments comprising a combination of automatic marking or manual marking and that are delivered in either of the two ways above.
- Electronic test delivery, with all marking completed manually on screen.
- A range of multimedia formats for submitting an assessment or test.
- Tests downloaded from the internet by an Approved Training Organisation.
- Delivery of training and assessments and submission of completed assessments by secure email.
- Assessments that are automatically marked and react adaptively to the delegate's performance.

Validity and reliability of e-learning and e-assessment

Approved Training Organisations and owners of standards must carefully consider the principle of how they, together with their technology partner(s), can ensure effective and robust methodologies, including valid and reliable infrastructure and system capabilities, as detailed within this document.

Approved Training Organisations must ensure that assessment and learning, delivered and maintained by electronic media, is fit for purpose and produces a robust, valid and reliable method of **testing** a delegate's knowledge and understanding. The choice of assessment and learning method should be independent of the technology on which it is based.

1. Approved Training Organisations must ensure that e-learning and e-assessment is fit for purpose and does not compromise the assessment methodology or the integrity of what is being taught or assessed. The assessment must only test the knowledge and skills needed to achieve the standard. Technology must not be a barrier to the ability of a delegate to access e-learning or e-assessment.
2. E-learning and e-assessment systems must maintain the integrity and validity of the assessment by following the existing Scheme Rules that support specific short duration standards, CITB products and/or qualifications.

Security

Approved Training Organisations must maintain and review the security of e-learning and e-assessment systems to ensure authentic test outcomes and protect against corruptive influences. Procedures must be in place to assure the security of hardware and software and the integrity of content and data feeds.

3. The data security arrangements for e-learning and e-assessment must comply, where relevant, with current legislation and industry standards. (*Refer to Appendix for a list of current legislation and standards.*)
4. Approved Training Organisations must ensure that the e-learning and e-assessment systems have safeguards in place designed to ensure the security of all aspects of e-learning and e-assessment and their processes, including plagiarism, copying and interference with any test outcomes.
5. E-learning and e-assessment systems must include adequate protection, such as software and/or firewalls that will protect against programmes that allow agents to gain remote access to the computer, as well as viruses and hacking, and monitor and block attempts to corrupt the learning and/or assessment process.
6. Approved Training Organisations must ensure that, through their technology partner, the following areas are addressed in the development of any e-learning system.
 - Developing appropriate authentication processes that include verification of identity.
 - Differentiating users on the basis of permissions and rights of access.
 - Protecting system areas so that only correctly authenticated users are able to access certain parts of the system.
7. E-learning systems must have the functionality to provide accurate audit trails and reports of system use and activity.
8. Approved Training Organisations must give due consideration to the physical security of e-learning hardware (such as servers).
9. Approved Training Organisations must have policies and procedures in place to protect the hardware and software used to deliver e-learning and the network in which it operates.
10. Approved Training Organisations must have procedures in place that will protect the integrity of test data before and after the assessment has taken place and whilst being transmitted to and from the Approved Training Organisation (for example, through encryption or authentication of e-signatures) in line with current relevant legislation and industry standards. (*Refer to Appendix.*)
11. Where an Approved Training Organisation has entered into an agreement or arrangement with any provider, they must have a service level agreement or licence arrangements in place that make clear each party's responsibilities, including security.
12. As good practice the e-learning system must calculate results automatically and securely deliver these to the delegate.

Data integrity – input and output

The Approved Training Organisation must be confident that systems have been thoroughly tested and ensure that they have sufficient capacity to store, retrieve, generate and share all necessary data. This includes, but is not limited to, the ability to exchange data securely with other internal and external systems, as required, without endangering or compromising the integrity of the data.

13. Approved Training Organisations must be confident that there is sufficient capacity to hold all necessary data and that those systems operate successfully. Approved Training Organisations must ensure that effective testing of system capacity has taken place.
14. Approved Training Organisations must put in place systems to monitor, review and correct any anomalies that occur to data input or output and measure the accuracy of the information that is generated. This must be incorporated in to the Approved Training Organisation's quality assurance procedures.
15. Approved Training Organisations must have secure and robust data storage, archiving and retrieval arrangements in place, including effective and secure interfaces with service providers, managed through an effective service level agreement or contract.
16. Approved Training Organisations must ensure, through system testing and regular review, that results, that are automatically calculated and generated by the e-learning system, are accurate and secure.

Operation of systems

E-learning systems must be stable and work reliably to generate valid, trustworthy results. They must be demonstrably consistent with relevant standards of good practice and be easy to navigate.

17. Approved Training Organisations must ensure that e-learning systems are sufficiently robust to support learning, assessments and/or testing.
18. E-assessment systems must incorporate functionality to generate key information including, but not limited to, delegate details, results and statistical performance reporting.
19. The e-learning and e-assessment systems must have a robust method of monitoring and recording delegates' online activity and behaviour whilst they undertake training and testing, including, but not limited to:
 - time taken to complete the course
 - results of exams
 - time taken to complete exams and number of attempts
 - login and logout dates and times
 - attempts to gain control of the system remotely
 - keystrokes or other analytics that assist in the identification of fraud or malpractice
 - delegates' identity.

Integrity of systems

Systems must allow for flexibility in light of technological development. System testing must be thorough and be reviewed at regular intervals once the system is operational. Approved Training Organisations must ensure that suitable support facilities are in place for delegates and that there is a contingency plan should any part of the system fail.

20. Before implementation the Approved Training Organisation must undertake full system testing. Testing should include functionality and capacity for concurrent users and use lessons learnt to make improvements.
21. Approved Training Organisations must have procedures in place to undertake regular system testing for reliability.
22. Approved Training Organisations must ensure that any software developed specifically for the purpose of e-learning and e-assessment is compatible with different operating systems, so as not to disadvantage delegates.
23. Approved Training Organisations must ensure sufficient support is available between the service provider and system users to prevent any delegate being disadvantaged.
24. Approved Training Organisations must have facilities to carry out daily database backups and have in place a robust disaster recovery plan.

Access to e-learning

Approved Training Organisations must ensure that policies and procedures comply with the Equality Act, so as not to discriminate against any delegate on the grounds of accessibility.

25. Approved Training Organisations must consider, early in the development phase of e-learning material, the ways in which they manage and consider delegates that have special assessment requirements. This will include business planning, product design, development, product specification and choice of product. It must also be compliant with the prevailing Equality Act.
26. Approved Training Organisations must have a particular consideration and reasonable adjustment policy that details how modifications will be considered and provided in a consistent manner.
27. Approved Training Organisations must consider, early in the development phase of e-learning, the requirements of delegates with special assessment requirements including, but not limited to, font size, readers and layout in line with recognised guidelines. (*Refer to Appendix.*)
28. E-learning material must be delivered in English or Welsh and the delegate must be competent in English or Welsh at the level required to do the job prior to the commencement of any learning session.

Preventing barriers to entry

Approved Training Organisations must ensure that technology is intuitive and does not create a barrier for any user. Provision must be made for delegates with particular learning and assessment requirements.

29. Approved Training Organisations must make the use of technology available for the benefit of all delegates by providing an intuitive system that promotes learning and assessment from a variety of locations. There should be clear guidance and details of available support facilities.
30. Approved Training Organisations must allow delegates to familiarise themselves with the system prior to using it for live sessions of learning. This could be through a preparatory module or tutorial. The system should not inhibit a delegate's performance.
31. The e-learning system must provide a usable interface and be easy to navigate.
32. The e-learning system must be capable of making adjustments to assessment and/or test times in line with any reasonable adjustment policy.

Business continuity and disaster recovery

Approved Training Organisations must have suitable measures in place to address service availability interruption and the need for disaster recovery for their e-learning and e-assessment services and systems in the event of system failure to ensure business continuity. This should be underpinned by measures to identify potential risks to those services and systems so that they can be managed to minimise disruption.

33. Approved Training Organisations must implement risk management procedures to provide early identification of risks to the operation of e-learning and e-assessment systems and enable action to be taken to minimise the impact of those risks in line with recognised standards of good practice.
34. Approved Training Organisations' service level agreements with service providers for their e-assessment systems must consider how the system will interface with other systems and service providers, as far as reasonably practicable, to enable adaptability in the contracting of services and to help manage risks and dependencies in the event of a system failure.
35. Approved Training Organisations must put in place a disaster recovery programme that sets out how the operation of their e-learning and e-assessment systems and services will restart after a significant failure.
36. Approved Training Organisation disaster recovery plans must demonstrate how the access to alternative, convenient, fully-equipped services and facilities will be provided. This must include, but not be limited to, how service will be resumed in line with the Approved Training Organisation's defined priorities and within timescales after the disaster has occurred.
37. Where e-learning and e-assessment are provided for the Approved Training Organisation by a 3rd party organisation there must be comprehensive reciprocal strategies for backup and contingency scenarios in case of a system failure at the centre.

Automatically generated on-demand tests

Approved Training Organisations must ensure that there is a sufficient volume of assessment items or questions to provide consistently secure, robust, balanced and unique on-demand tests, appropriate to the requirements of the standard.

38. Where Approved Training Organisations use electronic assessment item banks to automatically generate on-demand tests they must ensure, by thorough testing, that there are sufficient assessment items to provide consistently robust, balanced and unique test papers for the assessment and test windows to be accommodated.
39. Where electronic assessment item banks are used to automatically generate individual on-demand tests, Approved Training Organisations must ensure that the scrutiny of assessment items is not compromised by the level of use by ensuring there are sufficient items available to accommodate the expected delegate volumes.
40. Where the electronic assessment item or question banks are used, Approved Training Organisations and 3rd party organisations must ensure that each item, which contributes to measuring the achievement of the standard, is consistent and comparable with others over time for each session.
41. Where delivery of test items or questions is randomised, Approved Training Organisations and 3rd party organisations must have policies and procedures in place to analyse the potential impact of the randomisation on delegates' performance and to ensure that question order does not bias the results.
42. Automatically generated on-demand tests must be appropriately designed to afford delegates with particular assessment requirements and equal opportunities.

Test conditions and test environment

Approved Training Organisations and 3rd party organisations must have policies and procedures in place to ensure there are controls on test conditions in relation to on-demand testing, invigilation, secure test environments and health and safety.

43. Approved Training Organisations must ensure controls on test conditions, in relation to the extent to which on-demand testing is available, to ensure that the security of the assessment is not compromised by the volume of delegates using the tests.
44. Approved Training Organisations and 3rd party organisations must ensure and warrant the management of on-demand testing environments in terms of any additional requirements specific to the use of technology for testing, and that any new skillset or support that could potentially be required by the Approved Training Organisations' invigilators is identified and provided.
45. Approved Training Organisations must ensure that they have policies in place that address the need to manage the secure test environment in relation to the use of technology for assessment (for example, in terms of network security and data integrity) in their test locations.
46. Approved Training Organisations and 3rd party organisations must ensure the test environment and conditions are compatible with health and safety legislation and their obligations under law.

System familiarisation for trainers, invigilators, moderators and administrators

Approved Training Organisations must provide suitable support for system users, such as familiarisation sessions and guidance for all staff involved in e-assessments.

47. Approved Training Organisations must provide trainers, invigilators, moderators and administrators with familiarisation sessions or facilities, so that they have sufficient knowledge and understanding of the testing software. Approved Training Organisations must have clear guidance on the correct support contacts available for all elements of the system.
48. The system must allow for the delegate to practice prior to any test to ensure they have an understanding of how the system and test will proceed under test conditions.

Design, development and delivery of materials

49. Approved Training Organisations and 3rd party organisations can develop electronic training and assessment materials where the short duration standard expressly states the e-learning and/or blended learning (a mix of e-learning and traditional classroom delivery) is a valid method of delivery.
50. The duration of any course designed to be delivered by e-learning must have at least 50% of the total hours stated in the short duration standard for a traditional classroom delivery and meet all of the learning outcomes and assessment criteria.
51. Approved Training Organisations will be required to provide demonstrable evidence that the course will meet the minimum requirements for delivery time, and provide evidence of testing and any due diligence that supports the approach.
52. Any course designed to be delivered by blended learning must be at least 75% of the total hours stated in the standard and cover all of the learning outcomes and assessment criteria.
53. For blended learning courses, where the short duration standard details an exception to the 75% rule, courses can be designed to meet the discrete requirements of the individual short duration standard.
54. The course must be designed so that it prevents the delegate skipping any elements or pages of the course.
55. Where a course is modular, the system must ensure that all elements of the course have been covered prior to completion of any assessment, except where the assessment is at the end of each module.
56. E-learning and e-assessment platforms must include a mechanism for the inclusion of statement of course limitation so that delegates understand how the course can be used in the workplace.
57. CITB's Quality Assurance team will review e-learning and e-assessment material as part of the self-assessment and approval process. Courses that fail to meet the requirements detailed (paragraphs 49 to 56 inclusive) will not receive approval and will not be grant eligible.

Appendix

Glossary

- LMS – Learning management system
- CBT – Computer-based training

References

Legislation

- General Data Protection Regulation.
The **General Data Protection Regulation (GDPR)**, agreed upon by the European Parliament and Council in April 2016, replaced the Data Protection Directive 95/46/EC in Spring **2018** as the primary law regulating how companies protect EU citizens' personal data.
- Equality Act 2010.
- Health and Safety at Work etc. Act 1974.

Best practice and industry standards

- BS 25999: Code of practice for business continuity management.
- RNIB good design guidelines.
- E-learning.
- E-assessment.
- ISO 23988: International code of practice for the use of information technology in the delivery of assessments.