Totara Learn EU Annex 11 Compliance

This page is based on EU Annex 11 document requirements, it is provided to aid partners when answering these requirements. It is important to note that as the software vendor we can only provide information relevant to the core product that we distribute. It is vital the the partner or service provider completes their

Attached downloaded copy:

annex11_01-2011_en.pdf

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities. The application should be validated; IT infrastructure should be qualified. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

Section	Requirement	Totara Learn/Engage/Perform feature
General		
1	**Risk Management** Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	Totara uses a robust development process to manage the quality of the products we produce, and support that we provide. Risks managed throughout this process include security, data integrity, accessibility, privacy, usability, performance and scalability, supported infrastructures and in-product access control. A team of qualified professionals from product, design and development are required to make any change in core, regardless of the size or impact of that change. When required specialists are on hand to review and advise on the above areas.
2	**Personnel** There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	All partners have access to the Totara helpdesk. The helpdesk is run by a dedicated support team who are backed by product, design and development teams to facilitate cooperation with partner in addressing product related issues.
3	**Suppliers and Service Providers**	
3.1	When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous	Totara manages the development of its products and services exclusively in house. In situations where collaboration has occurred, or third parties are brought in to provide service formal agreements are always put in place that clearly state responsibilities, scopes, time frames, levels of access, and terms of operation.
3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Totara provides long term support for its products and has teams of highly skilled teams or professionals who provide support, services, product releases.

3.3	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Products documentation is available at https://help.totaralearning.com/ web site for users review.
3.4	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Information on the development process, including quality practices and processes and security around access control and management is not published publicly but can be made available to partners upon request.
Project phase		
4	**Validation**	
4.1	The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	To be answered by the service provider.
4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	To be answered by the service provider.
4.3	An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.	To be answered by the service provider.
4.4	User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.	To be answered by the service provider.
4.5	The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately	Totara uses a robust development process that requires a team of professionals from all relevant disciplines to sign off on every change made to the system. Internal reviews are conducted for risk areas including security, accessibility, privacy, performance and scalability. Security related penetration testing is outsourced to an external security firm annually. To ensure the ongoing quality of products and services provided by Totara automated quality assurance tools are run continuously to ensure that all unit and acceptance tests pass, that licensing is valid, installation/upgrade processes complete successfully and generate identical outcomes, and that more.
4.6	For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.	Totara internal tracking system and processes include reporting on number and severity of defects found, their fixes, and causes as well as retrospective reviews for significant issues.
4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	Every change to a Totara product is tracked using an internal system and includes acceptance criteria and testing instructions for positive and negative scenarios. In addition, there are strict requirements to provide adequate code coverage where possible using unit testing and acceptance (behavioural) testing. Each change must pass through our continuous Integration system that runs a complex test suite. Every product is additionally put through a barrage of continuous automated tests that include all of the tests conducted on an individual change, as well as additional tests. These are run on a nightly basis.
4.8	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	To be answered by the service provider.
Operational Phase		
5	**Data** Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks	Access to individual actions is controlled via a system of roles and capabilities which get applied to users through hierarchical contexts allowing for management by exception to as little or as much of the application as required. Access control checks ensure that the user performing an action is authorised to do so.

6	**Accuracy Checks** For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	Form validation is used to ensure only valid data is accepted. All incoming data is cleaned when it comes in to ensure it is of the correct type, and sanitised when sent back to the client to ensure it is safe for use. It is up to the organisation to apply any organisation specific validation they require in addition to what Totara products can provide out of the box.
7	**Data Storage**	
7.1	Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.	Totara stores user data primarily in three locations: the database (MySQL, MSSQL, or PostgreSQL), the site data directory, and the caches. It is up to the service provider to ensure that the data storage of all three is properly secured and managed at an infrastructure level. Access control checks within the product ensure that the user performing an action is authorised to do so. The user may only access information they are permitted to access through the product. It is strongly recommended that encryption in transit is used for all over the network infrastructure components. It must either be transparent to Totara, e.g. SSL offloaded by the web server, or supported natively by Totara functionality e.g. MySQL supports SSL through connection properties. Encryption at rest is supported in providing it is transparent to Totara.
7.2	Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	While Totara provides some facility for backup and restore of content such as courses, both manually and automatically, it is strongly recommended that the service provider implement their own site wide back and restore process. Instructions for managing a Totara site during backup processes can be found online in our help documentation.
8	**Printouts**	
8.1	It should be possible to obtain clear printed copies of electronically stored data.	Totara provides extensive reporting capabilities to view, filter and export data in a variety of formats. In particular each user has a Record of Learning which provides a full transcript of learning in web accessible and downloadable formats. Additionally, it is possible for a user who has been given permission to export all of the stored user data about them, and that they have generated. This export is in a mechanical format (JSON) as it is an export of the exact data stored about a user. It does not get localised or translated during export.
8.2	For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	Totara Learn records the user's unique id and date/time of an event. Specific records and associated reports include last modified dates as wells as more complex records such as completion provides history of each change, user and time of event.
9	**Audit Trails** Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	The system includes an integrated logging system which records in-product events to a database table or external log store. The Totara TXP system log is an append only log with no functionality to edit or update records via the interface. Therefore once an event has been recorded it cannot be deleted or modified. In addition Configuration changes report provide records with details on user, time, original and new values of site configuration changes.
10	**Change and Configuration Management** Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Access to individual actions is controlled via a system of roles and assignments, including hierarchical contexts allowing for management by exception to a sub-section of the hierarchy. Access control checks ensure that the user performing an action is authorised to do so. Actions occurring within the product are logged either to the database or to a configured log store. Changes occurring outside of the in-product experience must be managed by the service provider.
11	**Periodic evaluation** Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Totara provides releases on a monthly basis that include bug fixes and improvements. Totara Platform has Server upgrade history report with records of time, components, versions and results of upgrades as well as Security overview page that provides details on specific server configuration and environment requirements are met. For the infrastructure, and any third party plugins and code customisations this is the responsibility of the service provider.

12	**Security**	
12.1	Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	In-product user authentication is controlled by the configured authentication methods, and can include manual (username and password) authentication as well as a range of enterprise level authentication solutions such as OAuth and LDAP. Access outside of the in-product experience must be managed by the service provider.
12.2	The extent of security controls depends on the criticality of the computerised system.	Totara role-based authorisation system allows granular access management.
12.3	Creation, change, and cancellation of access authorisations should be recorded.	Each action on user profile, including user creation, suspension, deletion, role assignment and unassignment including on user performing this action, time of action and details are recorded in system log and can be viewed in Site Logs report.
12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Totara records the user's unique id, date/time of an event, action performed, text description, and change specific metadata such as component or item id being changed.
13	**Incident Management** All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Best answered by the service provider.
14	**Electronic Signature** Electronic records may be signed electronically. Electronic signatures are expected to: • a. have the same impact as hand-written signatures within the boundaries of the company, • b. be permanently linked to their respective record, • c. include the time and date that they were applied	Totara Learn records the user's unique id and date/time of an approval event. The meaning associated with the signature is captured as an "action" in the system log and as a "role" in the record storing the action. The user ids associated with system users are generated during user creation and cannot be adjusted subsequently. Once a specific user id is recorded it will reference that user for ever and will not be reassigned or reused.
15	**Batch release** When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	Access control checks allow to ensure that only users with specific role in a system can create and export reports. All report actions including creation, viewing, changing, and deletion as well as user performed action, date/time of the event are stored in system log and available via Site Logs report.
16	**Business Continuity** For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Totara can be horizontally scaled on several separate application servers using load balancing, database replication and shared file systems.
17	**Archiving** Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	Best answered by the service provider.

Glossary

Application: Software installed on a defined platform/hardware providing specific functionality

Bespoke/Customized computerised system: A computerised system individually designed to suit a specific business process

Commercial of the shelf software: Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users.

IT Infrastructure: The hardware and software such as networking software and operation systems, which makes it possible for the application to function.

Life cycle: All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.

Process owner: The person responsible for the business process.

System owner: The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.

Third Party: Parties not directly managed by the holder of the manufacturing and/or import authorisation.