The Role of the LMS in 21 CFR Part 11 Compliance

Co-author: Dr. Bob McDowall, Director
R.D. McDowall Limited

ABSTRACT

The purpose of this white paper is to describe how NetDimensions Learning addresses the technical requirements of the U.S. Food and Drug Administration's 21 CFR Part 11 Electronic Records; Electronic Signatures. This document explains the requirements of the validation process for 21 CFR Part 11 and how NetDimensions conducted a validation with a client.

Contents

The Role of the LMS in 21 CFR Part 11 Compliance

INTRODUCTION

Your industry demands compliance. Your people need training and certification. NetDimensions has an immediate solution to help your organization manage learning and development in compliance with 21 CFR Part 11 of the Code of Federal Regulations. Because 21 CFR Part 11 is a very rigorous regulation governed by the U.S. Food & Drug Administration (FDA), only a few suppliers of Learning Management Systems can actually meet the requirements for organizations to be able to conform to the standard. NetDimensions offers one of the most unique, reliable, and accepted systems when it comes to 21 CFR Part 11 compliance.

The pharmaceutical and associated industries have been undergoing change since introduction of the FDA's program on GMPs for the 21st Century. One of the outcomes of this was ICH Q10 which set out the requirements for Pharmaceutical Quality Systems (PQS) based on the principles of ISO 9000. One of the foundations of the PQS is resource management which links with the training regulations of the individual GXP (GLP, GMP or GCP) regulations that require firms to demonstrate that staffs have the appropriate combination of education, training and experience to do their assigned jobs. As a core element of a PQS, training records are nearly always reviewed during an inspection. Many companies training records are paper based and may not be up-to-date, making them an easy target during an inspection. Multinational companies have the problem of having to deal with different regulations and different regulators.

NetDimensions is qualified to address multiple global regulators, so your organization can be confident about ensuring regulatory compliance. NetDimensions allows companies to meet Good Laboratory Practice (GLP), Good Manufacturing Practice (GMP), and Good Clinical Practice (GCP) requirements for training records in highly regulated industries.

Other regulations that apply to the management of training records are:

21 CFR Part 820 – GMP for Medical Devices (Quality System Regulation)

21 CFR Part 58 - GLP for Non-Clinical Studies

21 CFR Part 211 – Current GMP for finished pharmaceutical products

Are Your Training Records Inspection Ready?

Training records have always been part of an inspection of the quality system by regulatory authorities.

Typically, when a facility or pre-approval inspection is due, members of staff will prepare for the visit by the Inspectorate. As training records are reviewed in almost all inspections, significant time will be spent checking that records are current and agree with the applicable SOPs.

The time and effort spent checking the records is wasted and non-productive work that can be better spent on more value-added activities within a regulated organization.

However, organizations can fail to have current training records as evidenced by the citation in Earlham College warning letter from 2002:

> "Failure to document training of the only laboratory person involved in drug testing as to specific methodology, instruments used, and the Current Good Manufacturing Practices (cGMP) relevant to laboratory operation as required by 21 CFR 211.25."

The corrective actions to remediate this problem are far more expensive than getting it right the first time.

However, the regulatory climate has changed since the issue of this warning letter as the responses from 483 observations now have to be delivered to the FDA within 15 working days of the end of the inspection. Therefore training records must be inspection ready whether they are held as paper or electronic records. Are your training records inspection ready?

For organizations that are not directly governed by the FDA, 21 CFR Part 11 is still an approved standard for government organizations and private businesses for electronic signatures, auditing, and record keeping. It may not be necessary to conduct a full computer validation and each organization can make that determination. Companies typically find that using electronic record keeping and electronic signatures provides many cost and time saving benefits as well as better risk management in both regulated and non-regulated industries.

A regulatory inspection could be detrimental if your organization is not in compliance with applicable regulatory requirements. It could mean a publically posted warning letter, the loss of proper certification or licensing to conduct business and compliance could become very costly with fines or loss of business. It is critical that organizations are prepared and are using proven systems that provide the required functionality to meet required audits and regulatory compliance needs on an ongoing basis.

ABOUT THIS DOCUMENT

This document is divided into three parts – Part I describes how NetDimensions Learning, the NetDimensions Learning Management System (LMS), supports 21 CFR Part 11 requirements, Part II highlights a successful validation that was conducted with a client, and Part III provides a complete review of all the clauses in the 21 CFR Part 11 regulation as they relate to NetDimensions Learning.

Part I - NetDimensions Learning Support of 21 CFR Part 11

INTERPRETING REQUIREMENTS FOR TRAINING RECORDS

Predicate Rules

The FDA requires that records that are to be maintained under applicable GXP regulations called predicate rules can pertain to both electronic and paper formats. If persons choose to use records in electronic format in place of paper format then Part 11 would apply too. Training records covered by predicate rules must comply with GXP - Good Manufacturing (GMP), Good Clinical (GCP), and Good Laboratory Practices (GLP). The most critical training records are course versions, course completions, and exam completions. Training records are used to verify compliance requirements, develop employee talent, and make key operational decisions within the organization. Therefore, this data must be secured and protected and this applies to creating, modifying, and archiving courses. These functions must identify the person(s) who affected any of these. There are specific purposes for e-signatures in order to record, audit, and validate authenticity.

21 CFR Part 11 further defines the requirements that regulated companies must adhere to in order for the companies' electronic records (including training records) to be accepted as trustworthy and reliable by the FDA. These electronic records must be "trustworthy, reliable and generally equivalent to paper records and handwritten signatures" according to the regulation. The requirements provide that electronic records and signatures will be acceptable in place of paper records, handwritten signatures or other physical records. The Part 11 regulation requires that the computer systems meet the technical aspect of the guideline such as application security, audit trails, electronic signatures, and reporting. It should be noted that, as with many Federal Regulations, specific details and interpretation of scope and applicability of any given section or subsection is left to individual organizations.

Learning Management Systems that maintain training records, such as NetDimensions Learning, can be configured to enable meeting the requirements of Part 11. With an electronic system, training records are always up-to-date and inspection-ready. You won't need to waste time to gather and check if your training records are up-to-date. An electronic system assures that everything is in order and easily accessed.

Regulatory Requirements for Training Records

The GXP regulations stipulate that personnel involved with regulatory activities must have the appropriate combination of education, training and experience to perform their assigned duties.

To illustrate this, the table below shows the applicable sections from three regulations. These three regulations are 21 CFR 11 (Electronic Records; Electronic Signatures final rule), 21 CFR 211 (GMP for finished pharmaceutical products) and 21 CFR 820 (GMP for Medical devices) and the requirements for training records are highlighted in **bold** text.

Regulation	Regulatory Text
11.10(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the **education, training, and experience to perform their assigned tasks**
§211.25 Personnel qualifications	(a) **Each person** engaged in the manufacture, processing, packing, or holding of a drug product shall have **education, training, and experience**, or any combination thereof, to enable that person **to perform the assigned functions**. **Training shall be in the particular operations that the employee performs and in current good manufacturing practice** (including the current good manufacturing practice regulations in this chapter and written procedures required by these regulations) as they relate to the employee's functions. **Training in current good manufacturing practice shall be conducted by qualified individuals on a continuing basis and with sufficient frequency** to assure that employees remain familiar with CGMP requirements applicable to them.
	(b) **Each person** responsible for **supervising** the manufacture, processing, packing, or holding of a drug product shall have the **education, training, and experience**, or any combination thereof, to **perform assigned functions** in such a manner as to provide assurance that the drug product has the safety, identity, strength, quality, and purity that it purports or is represented to possess.
§211.34 Consultants	**Consultants** advising on the manufacture, processing, packing, or holding of drug products shall have **sufficient education, training, and experience**, or any combination thereof, to advise on the subject for which they are retained. **Records shall be maintained** stating the name, address, and qualifications of any consultants and the type of service they provide.
§820.25 Personnel	(c) General. Each manufacturer shall have sufficient **personnel** with the necessary **education, background, training, and experience** to assure that all activities required by this part are correctly performed.
	(d) Training. Each manufacturer shall establish **procedures for identifying training needs and ensure that all personnel are trained to adequately perform their assigned re**sponsibilities. **Training shall be documented**. 1) As part of their training, **personnel shall be made aware of device defects** which may occur from the improper performance of their specific jobs. 2) **Personnel** who perform verification and validation activities shall be **made aware of defects and errors** that may be encountered as part of their job functions.

Standard Operating Procedures (SOPs) and Training Records

Also in the regulations is the requirement for personnel to work according to written procedures, written instructions or standard operating procedures. The intention being that for a regular and repeatable activity, there needs to be a set of instructions that define the tasks to be done and what has to be documented to demonstrate that the activity was actually performed. If any deviations to the procedure are made, they have to be documented at the time of the deviation and not later.

Training plays an important part when implementing a new or updated SOP since it's the training that is teaching employees how to conduct the procedures. This is where the LMS plays a vital role in being able to schedule and track the training of individuals on the SOP's. It is critical that organizations are able to keep accurate records of individuals and their training plans. NetDimensions can provide an easy to use and secure system to keep track of all the companies training records.

TRAINING RECORDS – ELECTRONIC VERSUS PAPER

There is no regulatory requirement that dictates whether organizations must use paper or electronic media to document their personnel training records; it is left to individual firms to make that decision. The flowchart in Figure 1 illustrates some of the differences between electronic records and paper based records.

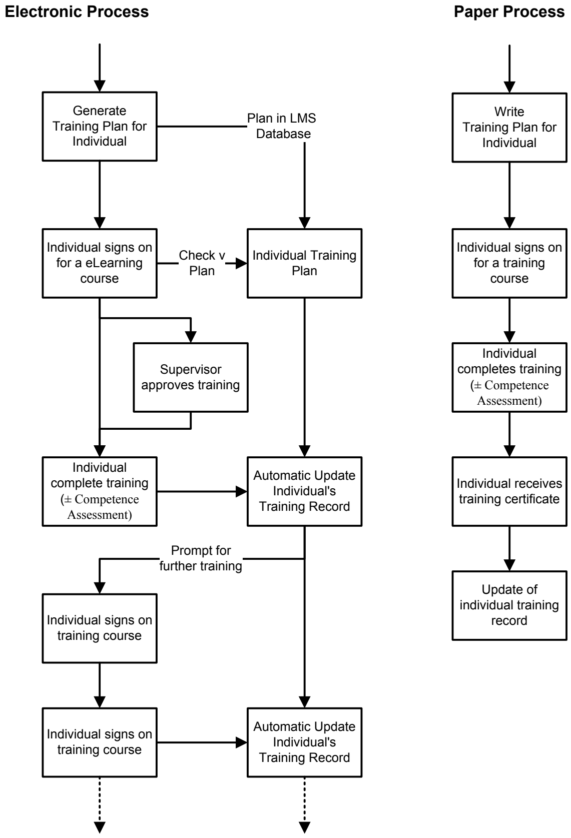

Electronic Process
Paper Process
Generate Training Plan for Individual
Plan in LMS Database
Individual signs on for a eLearning course
Check v Plan
Individual Training Plan
Supervisor approves training
Individual complete training (± Competence Assessment)
Automatic Update Individual's Training Record
Prompt for further training
Individual signs on training course
Individual signs on training course
Automatic Update Individual's Training Record
Write Training Plan for Individual
Individual signs on for a training course
Individual completes training (± Competence Assessment)
Individual receives training certificate
Update of individual training record

Figure 1: Training records - electronic versus paper based workflows.

The major differences between the two media are:

- A Training Plan is electronically generated in the LMS versus a manually written one.
- An electronic training plan is stored and easily accessible to all appropriate personnel versus a physically filed document, which requires the physical presence of the person to read the document.

- When an individual signs on to a training class, the LMS records the fact in the database versus the manual process of updating a record. When the individual completes training, the fact is recorded automatically in the database.
- To review a learner's records you can easily view on line or print a report versus gathering course completion certificates.
- The electronic system is always current compared to a manual process that is always updated some time after the training is completed.
- A clearer view of the organizations compliance to regulations can be easily reported.

Organizations can use either paper or electronic records; however the ability to have easy accessibility to data that is secure speaks for itself. It can take a lot of time if an organization needs to prepare for an audit and gather all the required records. If they are paper records, it is an enormous task. On the other hand, electronic records are quick and easy to access and organize, thus allowing an organization to be inspection-ready regarding training records. However, if training records are held electronically then the organization must consider both computer validation and compliance with 21 CFR 11 regulatory requirements.

21 CFR PART 11 BACKGROUND

Published in 20th March 1997 and effective on 20th August 1997, the Electronic Records; Electronic Signature final rule (21 CFR 11) has had the greatest impact on computerized systems than any other regulation. The basic requirement of the legislation is to ensure that any computerized system used for regulatory purposes produces electronic records that have the integrity and reliability and electronic signatures are trustworthy and equivalent to handwritten signatures executed on paper records.

21 CFR 11 only contains the requirements for ensuring that electronic records and electronic signatures are trustworthy and reliable but does not state which records need to be generated or signed. This is the role of the predicate rules which are the underlying FDA GXP regulations. The applicable predicate rule or rules that an organization must follow will define the records to be generated and retained and which ones need to be signed. Care needs to be taken when interpreting the predicate rules for electronic signature use. For example, there are only six direct references to initials or signatures in 21 CFR 211, however there are many references to items being reviewed, approved etc., which also implies that a signature is required to demonstrate compliance with the regulation. Therefore, only when Part 11 is interpreted with the applicable predicate rules does an effective and complete understanding of what is required fall into place.

In 2003, the FDA's Guidance for Industry on Part 11 Scope and Application was written to manage concerns that Part 11 was being over-interpreted. This document narrowed the scope of Part 11 to that defined in the applicable predicate rules and allowed enforcement discretion for legacy systems, validation, audit trail, copies of records and retention of records.

UNDERSTANDING THE PART 11 CONTROLS

There are different types of control required by 21 CFR 11 which fall into three categories as shown in Figure 2 and discussed below.

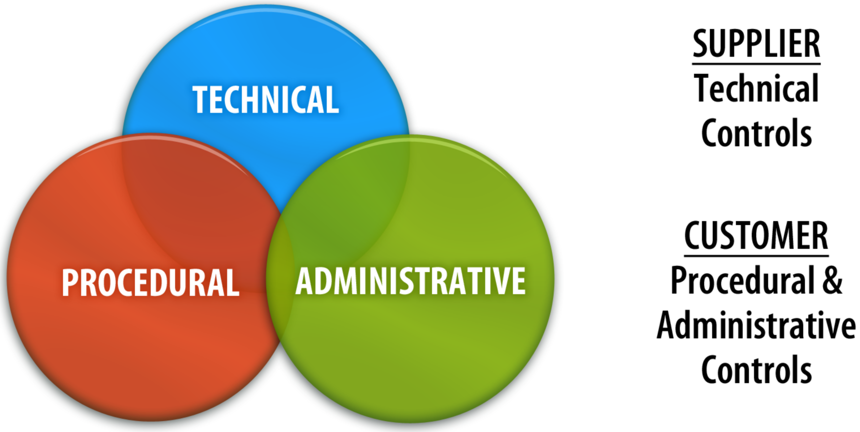


Figure 2: A 21 CFR 11 compliant system requires 3 controls: one from the supplier and two from the customer

1. **Technical** – Configuring the system to meet the requirements of Part 11 such as e-signatures and auditing reports. The technical requirements address how the system is configured to assure that the system operates as intended by the client.
2. **Procedural** – Creating standard operating procedures (SOPs) for how the system will be operated. This includes system settings, processes, password protection, authenticity procedures, and adherence to procedures. This requirement is up to the customer to create these procedures. Part 11 compliance includes procedural controls as well as system intrinsic capabilities.
3. **Administrative** – Each organization has the responsibility to verify the identity of the individuals before they can sanction an electronic signature. It is also the responsibility of the company to assure that the system is secure and adherence to written policies is being followed. Individuals must be held accountable and responsible for actions initiated under their electronic signatures to prevent record and signature falsification.

Please note that you cannot purchase a 21 CFR 11 compliant application.

There are applications that can be designed to be compliant with 21 CFR 11 technical controls, but it is the user that is responsible for providing policies and procedures to ensure the systems are fully compliant with the regulations and the applicable predicate rule. This is shown in Figure 1 and illustrates the importance of an integrated approach to 21 CFR 11 compliance and why there are no 21 CFR 11 compliant applications.

The following assumptions and exclusions are applicable in this white paper:

- **Closed System** - NetDimensions Learning is implemented as a “closed” system (whether installed in a customer’s own data center or hosted via Secure SaaS) as access to the system is under the control of the customer. Therefore there will be no discussion of open systems.
- **Biometrics** - NetDimensions does not provide any biometrics functionality in the system for user authenticity. Integration with a third party system will be required.
- **Tokens** – NetDimensions does not provide any functionality via tokens.

ABOUT NETDIMENSIONS LEARNING

NetDimensions provides companies, government agencies and other organizations with talent management solutions to personalize learning, share knowledge, enhance performance, foster collaboration, and manage compliance programs for employees, customers, partners and suppliers. NetDimensions has been serving over 900 clients and 9 million users worldwide. NetDimensions Learning is an award winning Learning Management System used in corporate training, compliance, and knowledge assessment solutions. NetDimensions Learning complies with 21 CFR Part 11 requirements via specific features for e-signatures, auditing, and reporting of electronic training records, and provides a secure environment for both on-premise and dedicated hosted deployments.

NetDimensions Learning allows you to:

- Manage courses, sessions, classrooms, instructors and learners.
- Pre-assign learning content to particular groups.
- Track individual certifications.
- Deliver audit reports.
- Maintain a repository of documents and knowledge assets.
- Date and Time Stamp training records and audit data fields.
- For a list of all the data fields that can be audited click here to see the list in the Appendix.

OVERVIEW OF 21 CFR PART 11 REQUIREMENTS FOR NETDIMENSIONS LEARNING

As discussed earlier, FDA’s 21 CFR Part 11 covers compliance requirements for organizations in health-care, pharmaceutical, life-science, biotechnology, medical- manufacturing, medical-device, and other FDA-regulated industries as well as most government agencies. 21 CFR Part 11 requires companies to implement controls such as system validation, protection of electronic records, audit trails, electronic signatures, and documentation for software and systems that are involved in processing many forms of data as part of their business practices and product development.

21 CFR Part 11 particularly aims for trustworthy and reliable electronic signatures and electronic records so that no one can alter information without an electronic audit trail in place. The regulation also covers requirements for unique identifiers for individuals, such as unique identification codes for electronic signatures. This allows companies to go to a “paperless” system of record keeping.

Approaching Part 11 from a software implementation and validation standpoint, this means that any software system should provide organizations with the ability to go through a successful validation process or audit with the FDA by ensuring it supports the necessary functionality, quality processes, and reporting for the organization to become compliant.

The key 21 CFR Part 11 support features of NetDimensions Learning are:

E-Signatures

Versioning

Auditing

Reporting

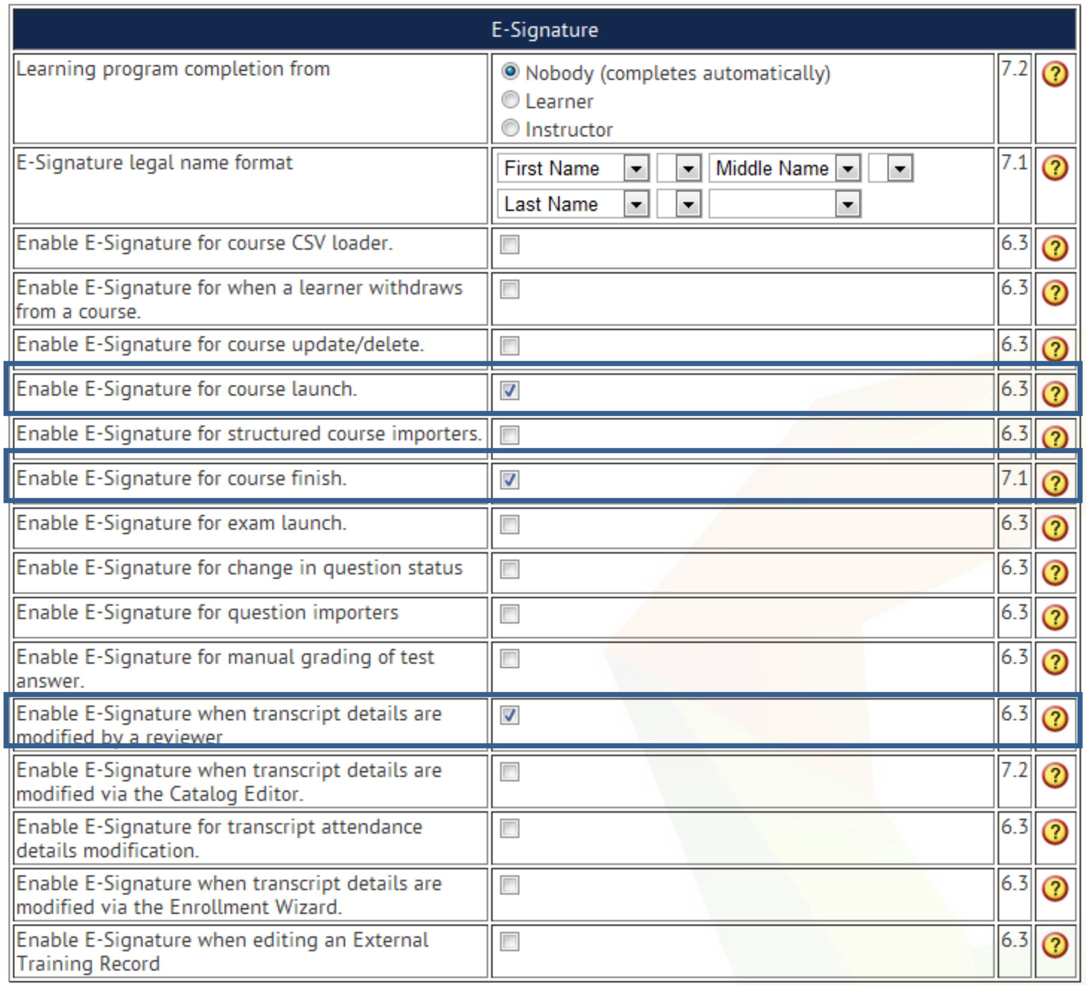
These features are described below in more detail.

ELECTRONIC SIGNATURES

Before every important operation in NetDimensions Learning, an electronic signature or e-signature prompt appears asking for the user ID, password, and update meaning. These three parameters collectively form an e-signature. The user ID and password must be correct for the current user before the requested operation can be carried out.

A critical part of any system is the ease of which the system can be configured instead of customized. There are many options to configure e-signature parameters in NetDimensions Learning, making it easy for administrators to configure the system simply by selecting the required options. These configuration options mean that organizations don't have to customize the system, only configure it. The figure below shows the system configuration options in NetDimensions Learning for managing e-signatures. The three items checked are:

1 Enable e-signature for course launch.
2 Enable e-signature for course finish.
3 Enable e-signature when transcript details are modified by a reviewer.

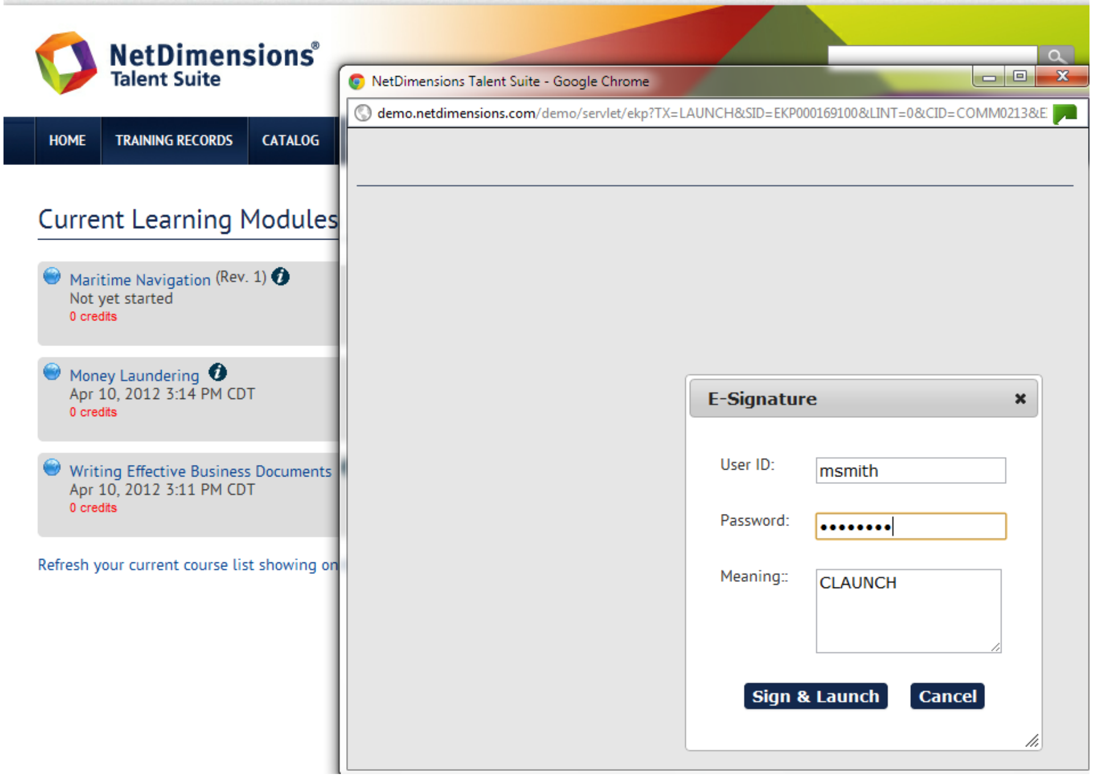


E-Signature			
Learning program completion from	● Nobody (completes automatically) ○ Learner ○ Instructor	7.2	?
E-Signature legal name format	First Name ▾ ▾ Middle Name ▾ ▾ Last Name ▾ ▾ ▾	7.1	?
Enable E-Signature for course CSV loader.	☐	6.3	?
Enable E-Signature for when a learner withdraws from a course.	☐	6.3	?
Enable E-Signature for course update/delete.	☐	6.3	?
Enable E-Signature for course launch.	☑	6.3	?
Enable E-Signature for structured course importers.	☐	6.3	?
Enable E-Signature for course finish.	☑	7.1	?
Enable E-Signature for exam launch.	☐	6.3	?
Enable E-Signature for change in question status	☐	6.3	?
Enable E-Signature for question importers	☐	6.3	?
Enable E-Signature for manual grading of test answer.	☐	6.3	?
Enable E-Signature when transcript details are modified by a reviewer	☑	6.3	?
Enable E-Signature when transcript details are modified via the Catalog Editor.	☐	7.2	?
Enable E-Signature for transcript attendance details modification.	☐	6.3	?
Enable E-Signature when transcript details are modified via the Enrollment Wizard.	☐	6.3	?
Enable E-Signature when editing an External Training Record	☐	6.3	?

Any time any of these actions occur, the e-signature input box will appear and require the user ID, password and meaning.

For example, from the above settings, an e-signature will be prompted based on the configuration settings: 1) when a user tries to launch a course 2) when a user finishes a course, and 3) when transcript details are modified by a reviewer.

Example of the e-signature prompt when launching a course looks like the screen shown below.


NetDimensions Talent Suite
HOME
TRAINING RECORDS
CATALOG
NetDimensions Talent Suite - Google Chrome
E-Signature
Sign & Launch
Cancel

demo.netdimensions.com/demo/servlet/ekp?TX=LAUNCH&SID=EKP000169100&LINT=0&CID=COMM0213&E

Current Learning Modules

Maritime Navigation (Rev. 1)
Not yet started
0 credits

Money Laundering
Apr 10, 2012 3:14 PM CDT
0 credits

Writing Effective Business Documents
Apr 10, 2012 3:11 PM CDT
0 credits

Refresh your current course list showing on

User ID: msmith

Password: ••••••••

Meaning:: CLAUNCH

The screen shows that a user has tried to launch a course and the e-signature frame popped up so that the user needs to provide their user ID, password and meaning text. The system can be set up to either automatically provide the meaning text based on the action or for the user to select from a drop-down menu. Clicking "Sign & Launch" will validate the user ID and password if it is correct, and the course will be launched.

VERSIONING OF COURSES

NetDimensions Learning allows administrators to control the versions of courses. Organizations typically have the most current courses available for review during an audit. However, it may be the case that many employees have completed a *prior* version of a course. NetDimensions Learning automatically keeps track of all revisions of content. If you are asked to present the actual training taken by an individual, online transcripts provide that information so you are sure to present the actual version of the course which the individual completed.

AUDITING

All changes made to sensitive data are audited in the database along with information on the type of change, who made the change and when. Types of changes include any creation, update and deletion of sensitive data. Following are the list of entities that are audited categorized by their functional area.

There are five major areas for auditing over 100 entities within the system. The list below shows each major area and the number of entities that can be audited for each.

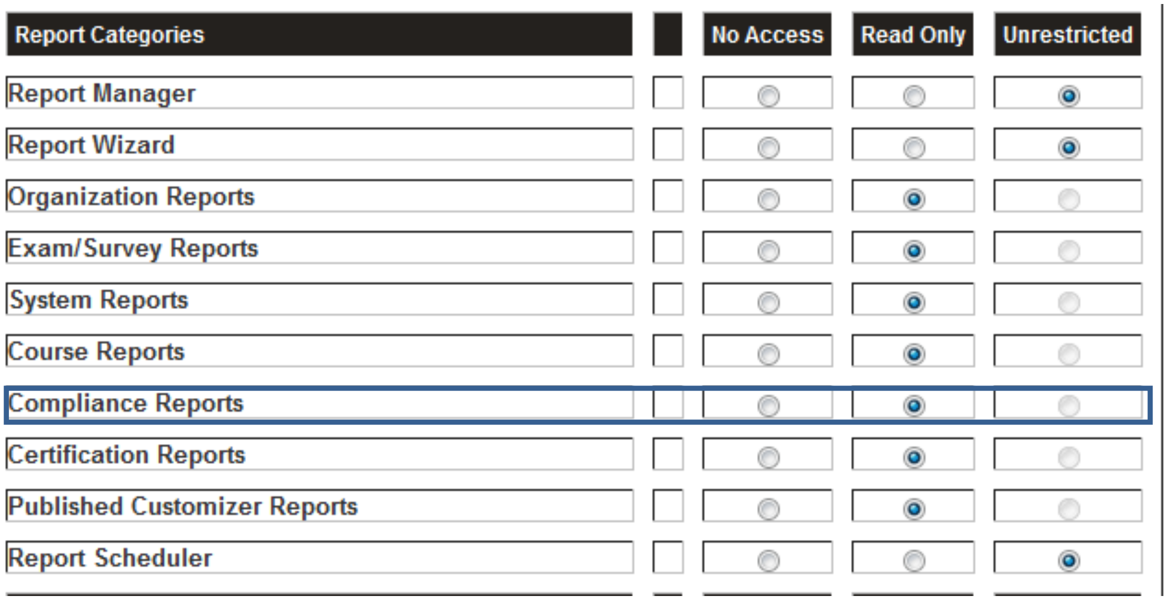
- ***Courses, Sessions and Modules – 40 entities***
- ***Questions – 17 entities***
- ***Enrollments, Transcripts and Records – 9 entities***
- ***Exams – 17 entities***
- ***Courseware – 18 entities***

All audit trails can be viewed using the Compliance Reports described in the following section.

A complete listing of all the auditable fields that can be reported on is included in the **Appendix** section at the end of this document.

REPORTING

As discussed earlier, all audited data is conveniently presented as standard NetDimensions Learning reports. This means users can view this audited information in various electronic formats like HTML, CSV, PDF and Excel as with other standard NetDimensions Learning reports. A user's role must have access to the Compliance Reports section of system’s Report Manager in order to access the audit-related reports.



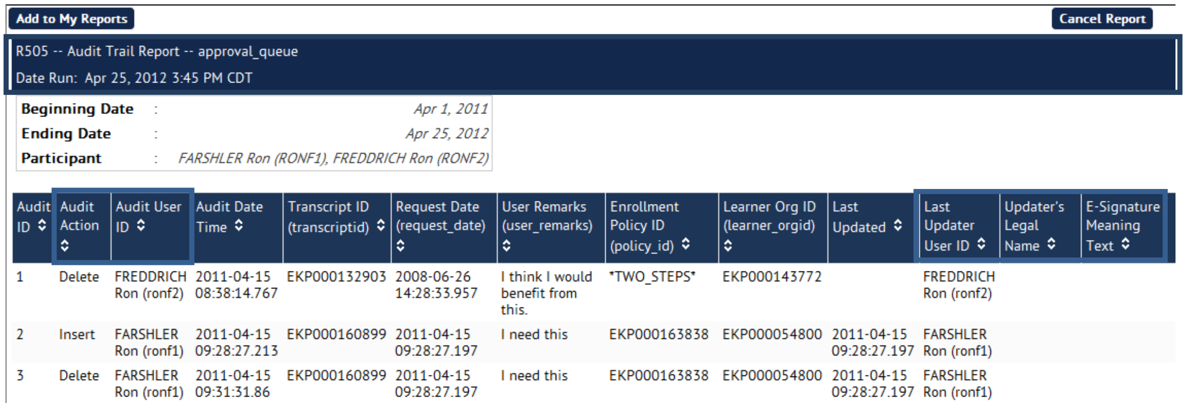
Report Categories		No Access	Read Only	Unrestricted
Report Manager	□	○	○	●
Report Wizard	□	○	○	●
Organization Reports	□	○	●	○
Exam/Survey Reports	□	○	●	○
System Reports	□	○	●	○
Course Reports	□	○	●	○
Compliance Reports	□	○	●	○
Certification Reports	□	○	●	○
Published Customizer Reports	□	○	●	○
Report Scheduler	□	○	○	●

Users with this role access can now navigate to the **Compliance Reports** section of Report Manager. There are four reports relevant to auditing in this section:

- ***Audit Trail Report (R505)***
- ***Audit Trail User Action Report (R506)***
- ***Learning Module Audit Report (R507)***
- ***User Transcript Audit Report (R508)***

Audit Trail Report (R505)

This report displays the audit trail for the selected audit item within the specified date range. The audit trail is displayed in chronological order of audit date. Apart from the date range, a list of users whose updates have caused auditing (audit users) can also be selected.



R505 -- Audit Trail Report -- approval_queue

Date Run: Apr 25, 2012 3:45 PM CDT

Beginning Date	:	*Apr 1, 2011*
Ending Date	:	*Apr 25, 2012*
Participant	:	*FARSHLER Ron (RONF1), FREDDRICH Ron (RONF2)*

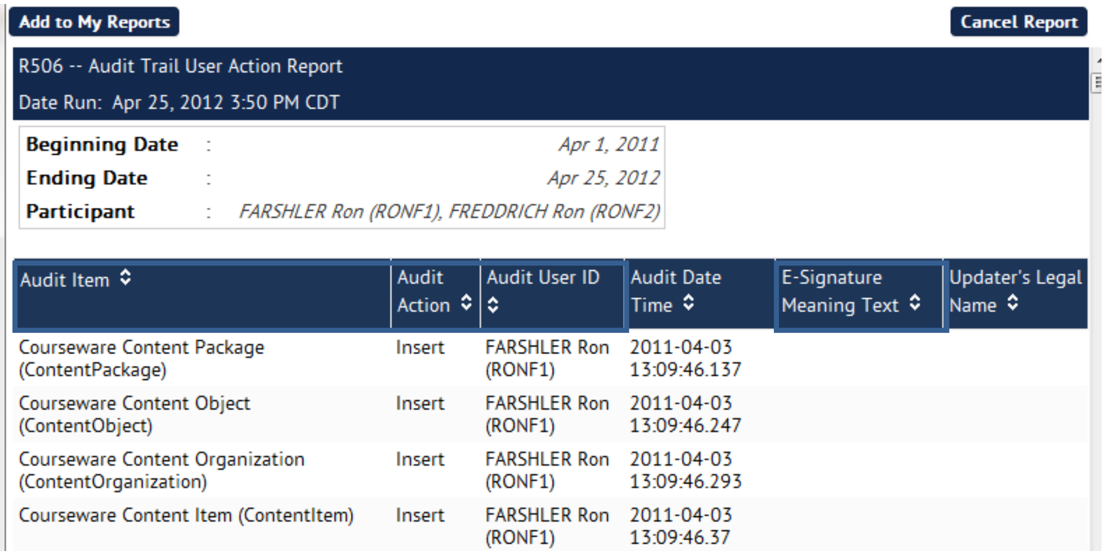
Audit ID ⇕	Audit Action ⇕	Audit User ID ⇕	Audit Date Time ⇕	Transcript ID (transcriptid) ⇕	Request Date (request_date) ⇕	User Remarks (user_remarks) ⇕	Enrollment Policy ID (policy_id) ⇕	Learner Org ID (learner_orgid) ⇕	Last Updated ⇕	Last Updater User ID ⇕	Updater's Legal Name ⇕	E-Signature Meaning Text ⇕
1	Delete	FREDDRICH Ron (ronf2)	2011-04-15 08:38:14.767	EKP000132903	2008-06-26 14:28:33.957	I think I would benefit from this.	*TWO_STEPS*	EKP000143772		FREDDRICH Ron (ronf2)		
2	Insert	FARSHLER Ron (ronf1)	2011-04-15 09:28:27.213	EKP000160899	2011-04-15 09:28:27.197	I need this	EKP000163838	EKP000054800	2011-04-15 09:28:27.197	FARSHLER Ron (ronf1)		
3	Delete	FARSHLER Ron (ronf1)	2011-04-15 09:31:31.86	EKP000160899	2011-04-15 09:28:27.197	I need this	EKP000163838	EKP000054800	2011-04-15 09:28:27.197	FARSHLER Ron (ronf1)		

Important fields are:

- Audit Action indicates what sort of action has been performed on the Audit Item, e.g. Update, Delete or Insert.
- Audit User ID indicates who has performed the action.
- The remaining columns indicate the data newly inserted, or the new data if an update has occurred, or the data prior to the deletion if a deletion has occurred.

Audit Trail User Action Report (R506)

This report is similar to R505 and displays the audit trail for a given set of users within the specified date range.



R506 -- Audit Trail User Action Report

Date Run: Apr 25, 2012 3:50 PM CDT

Beginning Date	:	*Apr 1, 2011*
Ending Date	:	*Apr 25, 2012*
Participant	:	*FARSHLER Ron (RONF1), FREDDRICH Ron (RONF2)*

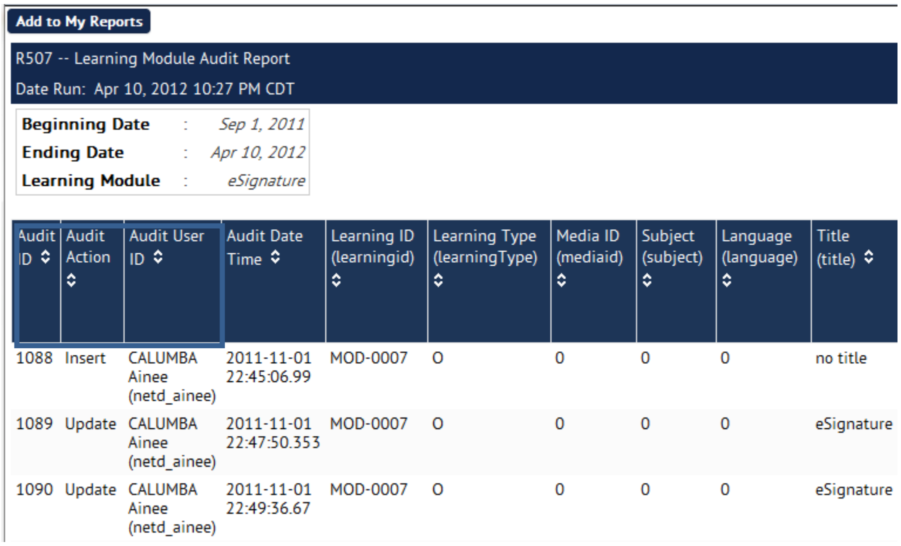
Audit Item	Audit Action	Audit User ID	Audit Date Time	E-Signature Meaning Text	Updater's Legal Name
Courseware Content Package (ContentPackage)	Insert	FARSHLER Ron (RONF1)	2011-04-03 13:09:46.137		
Courseware Content Object (ContentObject)	Insert	FARSHLER Ron (RONF1)	2011-04-03 13:09:46.247		
Courseware Content Organization (ContentOrganization)	Insert	FARSHLER Ron (RONF1)	2011-04-03 13:09:46.293		
Courseware Content Item (ContentItem)	Insert	FARSHLER Ron (RONF1)	2011-04-03 13:09:46.37		

Important fields are:

- Audit Item indicates which item is being reported on.
- Audit Action indicates what the action was.
- Audit User ID indicates who performed the action.
- E-Signature Meaning Text indicates what meaning was selected.

Learning Module Audit Report (R507)

This report shows the audit trail for any additions, changes or deletions to a Learning Module. Notice under the Audit Action column the actions that are shown. In this case "Insert" and "Update".



R507 -- Learning Module Audit Report

Date Run: Apr 10, 2012 10:27 PM CDT

Beginning Date	:	*Sep 1, 2011*
Ending Date	:	*Apr 10, 2012*
Learning Module	:	*eSignature*

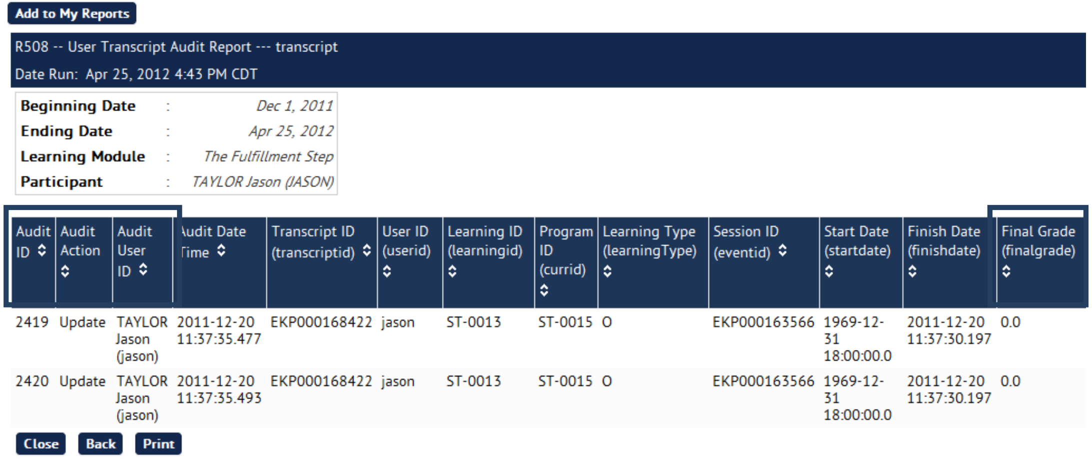
Audit ID	Audit Action	Audit User ID	Audit Date Time	Learning ID (learningid)	Learning Type (learningType)	Media ID (mediaid)	Subject (subject)	Language (language)	Title (title)
1088	Insert	CALUMBA Ainee (netd_ainee)	2011-11-01 22:45:06.99	MOD-0007	O	0	0	0	no title
1089	Update	CALUMBA Ainee (netd_ainee)	2011-11-01 22:47:50.353	MOD-0007	O	0	0	0	eSignature
1090	Update	CALUMBA Ainee (netd_ainee)	2011-11-01 22:49:36.67	MOD-0007	O	0	0	0	eSignature

Important fields are:

- Audit ID.
- Audit Action.
- Audit User ID.

User Transcript Audit Report (R508)

This report shows the Transcript Audit for individuals and courses they are enrolled in.



R508 -- User Transcript Audit Report --- transcript

Date Run: Apr 25, 2012 4:43 PM CDT

Beginning Date	:	*Dec 1, 2011*
Ending Date	:	*Apr 25, 2012*
Learning Module	:	*The Fulfillment Step*
Participant	:	*TAYLOR Jason (JASON)*

Audit ID	Audit Action	Audit User ID	Audit Date Time	Transcript ID (transcriptid)	User ID (userid)	Learning ID (learningid)	Program ID (currid)	Learning Type (learningType)	Session ID (eventid)	Start Date (startdate)	Finish Date (finishdate)	Final Grade (finalgrade)
2419	Update	TAYLOR Jason (jason)	2011-12-20 11:37:35.477	EKP000168422	jason	ST-0013	ST-0015	O	EKP000163566	1969-12-31 18:00:00.0	2011-12-20 11:37:30.197	0.0
2420	Update	TAYLOR Jason (jason)	2011-12-20 11:37:35.493	EKP000168422	jason	ST-0013	ST-0015	O	EKP000163566	1969-12-31 18:00:00.0	2011-12-20 11:37:30.197	0.0

Important fields are:

- Audit ID.
- Audit Action.
- Audit User ID.
- Final Grade.

Part II Computerised System Validation Case Study

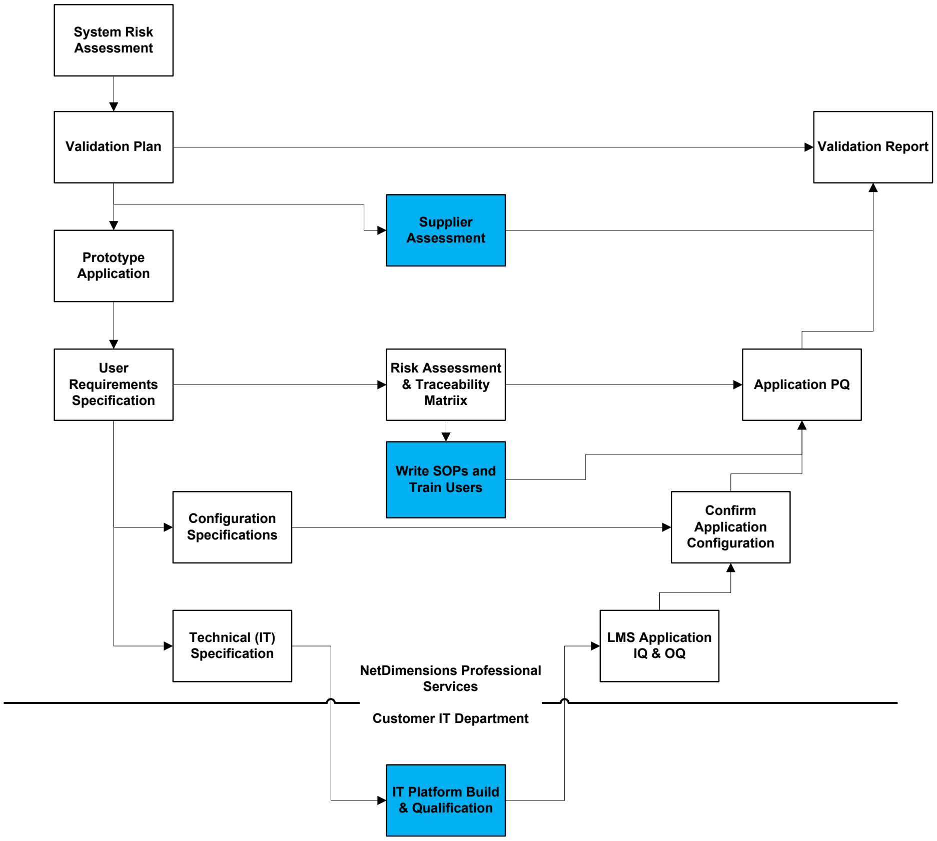
A case study of the validation of the NetDimensions Learning LMS is presented and discussed in this section.

NetDimensions have partnered with an experienced third party Dr Bob McDowall of R.D.McDowall Limited to deliver validation services in conjunction with our Professional Services group. The regulated healthcare company had purchased the LMS for 30,000 users and it was being rolled-out to over 40 countries. The validation was therefore required to comply with medical device regulations (21 CFR 820), pharmaceutical GMPs from the USA and European Union (21 CFR 211 and EU GMP Part 1 including Annex 11 for computerised systems) and the Electronic Records and Electronic Signatures (21 CFR 11).

The system presented in this case study was installed on the customer's site and operated by their own IT department. However, the principles described in this case study can be applied to a single hosted SaaS (Software as a Solution) LMS solution from NetDimensions.

SYSTEM LIFE CYCLE

As the current regulations and guidance for computerised system validation require a life cycle approach, this is presented in the Figure below. The rationale for selecting this life cycle model is that the LMS is a GAMP category 4 (commercial configurable product) and therefore instead of writing functional and design specifications, the focus is on documenting the configuration of the software.


System Risk Assessment
Validation Plan
Validation Report
Supplier Assessment
Prototype Application
User Requirements Specification
Risk Assessment & Traceability Matriix
Application PQ
Write SOPs and Train Users
Configuration Specifications
Confirm Application Configuration
Technical (IT) Specification
LMS Application IQ & OQ
NetDimensions Professional Services
Customer IT Department
IT Platform Build & Qualification

Note this in this figure, the documents highlighted in blue are presented for completeness of the system life cycle but were the responsibility of the customer.

- Supplier assessment: quality management system, product development and hosting services
- Installation of the IT platform by the IT Department
- Writing SOPs to use the system
- Execution of Performance Qualification (PQ) or User Acceptance Test (UAT) test scripts

Documents for the validation were drafted by the NetDimensions validation team for review and comment by the customer's project team.

DO I NEED TO VALIDATE THE SYSTEM?

To determine if the LMS needs to be validated and the extent of the work required is documented by the system level risk assessment. This consists of two parts, the first is a questionnaire to determine if the system requires validation and the second identifies the GAMP software category and the impact of the records and signatures maintained by the system. The outcome of this risk assessment was that the system required validation by a life cycle approach rather than a simplified approach.

Deliverable: System risk assessment

CONTROLLING THE VALIDATION

Any validation project needs to be controlled via a validation plan which defines the roles and responsibilities of the people involved in the project, the life cycle to be followed together with the anticipated documented evidence to be written.

In addition planned changes to the validation plan can be accommodated by issuing approved amendments that justify the changes to the original plan.

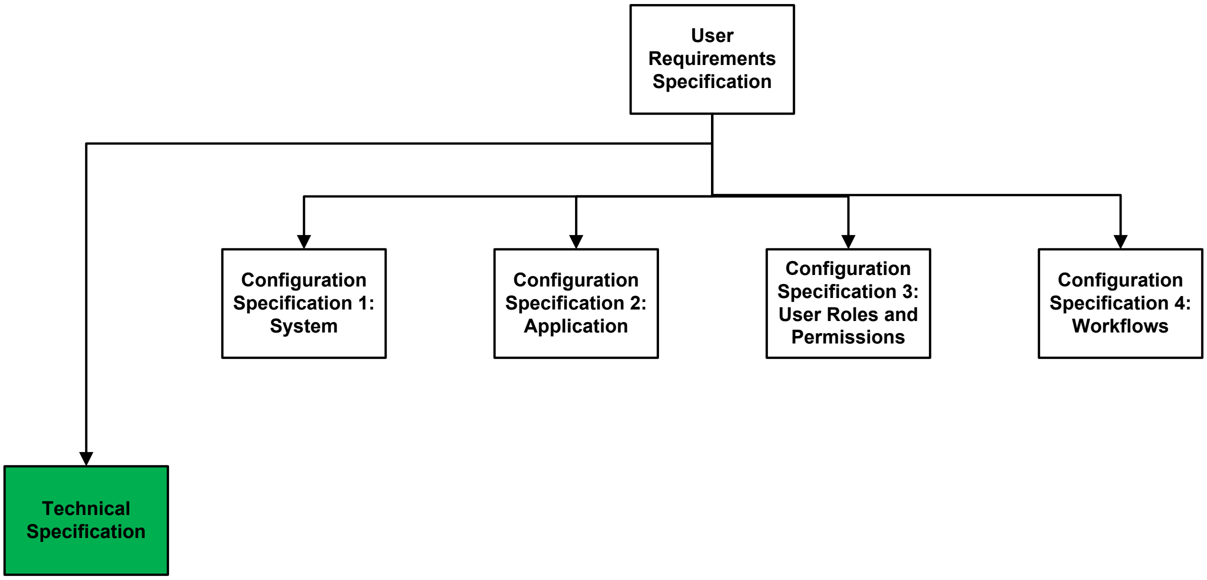
Deliverable: Validation Plan and any formal amendments to the plan

HOW IS THE SYSTEM SPECIFIED?

Rather than a single specification document for the validation, there are several documents that will specify the whole system and the documents produced can be seen in the accompanying Figure below.

User Requirements Specification (URS)

The key document in any validation is the user requirements specification (URS) contains a comprehensive listing of all requirements (in excess of 500 requirements) for the LMS including computing requirements, system sizing, regulatory compliance, functional requirements, IT support, interfaces and any data migration needs. Requirements are uniquely numbered for traceability throughout the rest of the system life cycle and are prioritised.


User Requirements Specification
Configuration Specification 1: System
Configuration Specification 2: Application
Configuration Specification 3: User Roles and Permissions
Configuration Specification 4: Workflows
Technical Specification

Application Configuration Specifications

Configuration of the LMS to match a client's business process is documented in four configuration specifications:

- Configuration Specification 1: System
- Configuration Specification 2: Application
- Configuration Specification 3: User Roles and Permissions
- Configuration Specification 4: Workflows

Requirements in the URS point to each of the configuration specifications and there is traceability back from each specification to the URS.

Technical Specification

The technical specification, **for an on-premise installation**, defines the IT platform for the system and takes into consideration the minimum specification recommended by NetDimensions with the customer's corporate computing requirements to document the actual server platform ordered. Each instance, physical or virtual will be documented here with traceability back to the URS. From the technical specification the platform for each instance will be qualified by the customer's IT department. This document could be written by either the customer's own IT department or by NetDimensions validation team.

Deliverables:

- User Requirements Specification
- Four configuration Specifications
- Technical Specification

RISK ASSESSMENT AND TRACEABILITY MATRIX

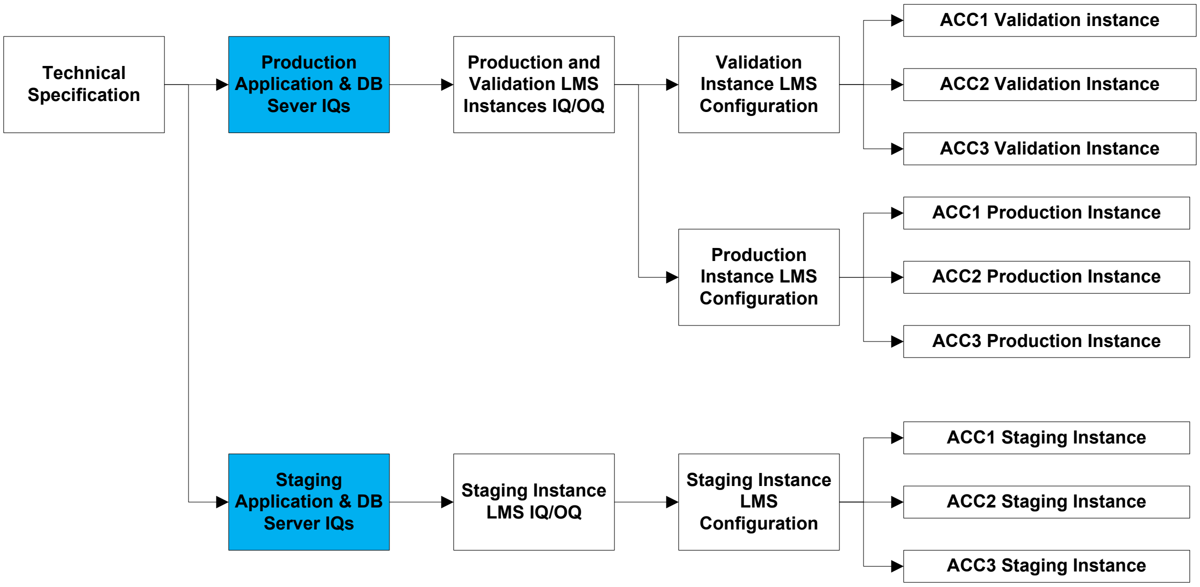
Following the completion of the URS, a risk assessment and traceability matrix (RATM) was written that assessed each prioritised requirement from the perspective of business and / or regulatory risk. This allows high priority / high risk requirements only to be determined if they will be tested or verified (e.g. installation of components, writing an SOP etc).

One advantage of writing the RATM early in the project is that a list of requirements that trace to SOPs can allow a customer to assess if existing procedures need to be updated, retired or new ones need to be written. This applies for both users and IT support.

Deliverable: Risk assessment and traceability matrix

BUILD AND CONFIGURE THE SYSTEM

This phase of the work consists of three main parts as shown in the Figure below, please note that the blue tasks in the figure are the responsibility of the customer.


Technical Specification
Production Application & DB Server IQs
Production and Validation LMS Instances IQ/OQ
Validation Instance LMS Configuration
ACC1 Validation instance
ACC2 Validation Instance
ACC3 Validation Instance
Production Instance LMS Configuration
ACC1 Production Instance
ACC2 Production Instance
ACC3 Production Instance
Staging Application & DB Server IQs
Staging Instance LMS IQ/OQ
Staging Instance LMS Configuration
ACC1 Staging Instance
ACC2 Staging Instance
ACC3 Staging Instance

Build the IT Platform

Based on input from the technical specification, the IT platform to run the LMS is ordered, installed and qualified by the customer’s IT department. In this case study, there were two identical servers ordered and installed on each server together with customer’s selected database.

Deliverable: IQ documents for each server

Is the Software Installed Correctly and Does the System Work?

The NetDimensions combined IQ and OQ documents that the LMS software and associated utilities have been correctly installed and work as expected. The main focus is on the installation qualification (IQ) phase and a short operational qualification (OQ) phase. The rationale for this is that many OQ protocols are executed on an unconfigured application which is then configured by the customer. Therefore the NetDimensions' approach is to focus on the IQ rather than the OQ due to the fact that the software will be configured after the initial IQ/OQ execution.

As shown in the figure above the case study had two instances of the LMS installed on the production server: one for production and one for validation. The rationale for this approach was to ensure that validation data as kept separate and the production instance would be clean.

Deliverable: NetDimensions combined IQ / OQ for each server

Application Configuration Confirmation Documents

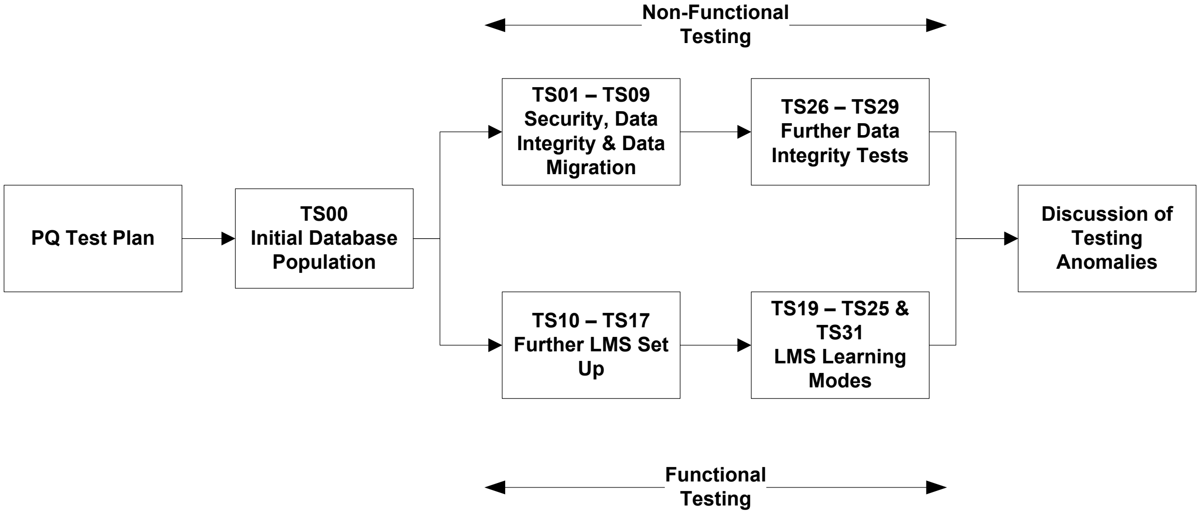
After the combined application IQ and OQ has been performed, the system is configured according to configuration specifications CS1, CS2 and CS3. The application configuration conformation documents confirm that the correct configuration that has taken place and this was performed on each instance of the LMS. The whole system was now placed under change control and any further changes to the configuration results in a new version of the configuration specification being released.

Deliverables:

- System configuration conformation for each instance
- Application configuration conformation for each instance
- User roles and permissions configuration conformation for each instance

PERFORMANCE QUALIFICATION (PQ) TEST PLAN AND TEST SCRIPTS

The Performance Qualification (PQ) or User Acceptance Testing is carried out according to the prioritised requirements in the user requirements specification and linked configuration specifications.


Non-Functional Testing
PQ Test Plan
TS00 Initial Database Population
TS01 – TS09 Security, Data Integrity & Data Migration
TS26 – TS29 Further Data Integrity Tests
TS10 – TS17 Further LMS Set Up
TS19 – TS25 & TS31 LMS Learning Modes
Discussion of Testing Anomalies
Functional Testing

PQ Test Plan

To control this work there is an overall PQ test plan that defines the environment(s) where testing will take place, the design of the overall test suite, details of each test script and the requirements that will be tested and the assumptions exclusions and limitations of the testing.

There is requirements traceability to the individual test script and back to the user requirements specification in both the PQ test plan and each PQ test script.

PQ Test Suite

Under the umbrella of the PQ test plan there is a suite of PQ test scripts for functional tests e.g. learning modes and workflows and non-functional tests e.g. security, data integrity, audit trail etc plus an SOP for test script execution which can be incorporated into a customer quality system.

The test scripts were executed by the customer's project team members and reviewed by the NetDimensions validation team. Results were summarised in the PQ section of the validation summary report.

Deliverables:

- PQ test plan
- PQ test scripts
- Documented evidence
- Test execution notes and anomaly reports

ADDITIONAL COMPLIANCE DOCUMENTS

Two additional documents were written for the customer validation that are not shown on the overall life cycle figure.

Definition of Electronic Records / Raw Data

To comply with FDA's Part 11 scope and application guidance for definition electronic records and EU GMP Chapter 4 on documentation for raw data, this document is provides definition of electronic records and raw data held by the system.

System Description

The system description is written to meet the requirements of EU GMP Annex 11 and outlines the overall system. It provides sufficient detail of the system but also cross references key validation documentation where further information about the system resides.

Deliverables:

- System description
- Definition of electronic

REPORTING THE VALIDATION

At the end of the project, the validation summary report documents what actually happened together with a discussion any amendments to the plan and deviations during the testing. The validation summary report contains a release statement for the system.

Deliverable: Validation summary report

TIME SCHEDULE

The validation project described here was completed in nine weeks within the agreed timeframe for the project. This is an extremely tight time scale and to achieve this requires a high degree of commitment and the availability of staff on the project.

Part III – Analysis of 21 CFR 11 Clauses for NetDimensions Learning

DIVISION OF RESPONSIBILITIES FOR 21 CFR PART 11 COMPLIANCE

In an earlier section the three types of Part 11 controls were explained as technical, procedural and administrative and for a system to be Part 11 compliant all three types of controls must be in place. In this section we will discuss the applicable clauses from 21 CFR 11 sub part B (electronic records) and sub part C (electronic signatures) to highlight the responsibilities of NetDimensions to deliver appropriate technical controls in the LMS system as well as the customer to provide the procedural and administrative controls. As you read this section you will discover that although there is a division of the regulation into a sub part dealing with electronic records and another one covering electronic signatures, there are requirements for electronic signatures in the sub part on electronic records and vice versa. It is important to understand that Part 11 is an integrated regulation.

In this section we will only consider sub parts B and C with the omission of §11.30 for open systems as the NetDimensions system is a closed system.

21 CFR 11 Requirement	NetDimensions Responsibilities	Customer Responsibilities
§ 11.10 Controls for Closed Systems		
11.10(a) Validation of the systems to ensure accuracy, reliability, consistent intended performance and the ability to discern altered and invalid records.	▪ Follow Quality Management System guidelines in development of our product. ▪ Provide an application that has been developed under a quality management system to enable the system that can be validated. ▪ Changes to database records will trigger the audit trail. ▪ Data entries are checked to see that they fit with verification rules.	▪ Responsible for the initial validation of the LMS system. ▪ Maintain the validation status of the system. ▪ Operate the change control procedure. ▪ Write and update the system SOPs.
11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by the agency.	▪ Provide a comprehensive set of standard, audit and compliance reports. ▪ Provide that report outputs can be printed or viewed on screen. ▪ Provide ability so reports can be exported in HTML, CSV, Excel and PDF formats. ▪ Comprehensive set of standard, audit and compliance reports. ▪ Report output can be printed or viewed on screen.	▪ Configure the network and the LMS software to prevent deletion or unauthorized copying of files through the operating system. ▪ Control the date and time settings on the workstation.
11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	▪ Provide recommendations for database backup. ▪ If LMS is hosted, data is secured through SSL. ▪ Provide a secure and compliant hosting service. Hosting service is ISO 27001 compliant. ▪ Provide recommendations for database backup. ▪ If LMS hosted, data is secured through SSL.	▪ Define record retention period. ▪ Write SOPs for backup, recovery, archive and restore. ▪ Define and qualify any additional software utilities necessary for backup and recovery.
11.10(d): Limiting system access to authorized individuals.	▪ Access controlled by user identity and password. ▪ Access privileges to different functions achieved by configuring Permissions and Roles settings. ▪ Inactivity lockout and limiting logon attempts. ▪ Access is controlled by user identity and password. ▪ Access privileges to different functions achieved by configuring Permissions and Roles settings.	▪ SOP on System Security and Access Control must cover the proper configuration and maintenance of User IDs and passwords. ▪ List of current and historical users with access privileges. ▪ Configure LMS security features as defined in the SOP for System security and Access Control. ▪ Implement inactivity lockout.

21 CFR 11 Requirement	NetDimensions Responsibilities	Customer Responsibilities
11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	▪ Secure database provides for a date/time stamped audit trail including user logon and logoff. ▪ Date and Time stamp any additions, deletions or modifications made to training records or users status, learning transcript records, job role, competencies, and learning event records. ▪ Any additions, deletions or modifications made to training records or users status, learning transcript records, job role, competencies, and learning event records. ▪ Modifications to records cannot be overwritten. ▪ Whenever an insert, update or deletion is carried out on one of the audited database tables, an entry is automatically created in the corresponding audit history table, recording a copy of the new data, the current date and time, and who carried out the change. ▪ The audit history data is only ever added to and never updated or deleted, it is always possible to see previously recorded information.	▪ Enable audit trail on installation. ▪ SOPs to reflect the retention of records including the corresponding audit trails. ▪ SOP for regular review of audit trails.
11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	▪ Configurable software that provides mechanisms within the system to enforce specific workflows. ▪ Configurable software provides mechanisms within the system to enforce specific workflows. ▪ Configurations can be applied to sequence courses, pre-requisites, exams, programs, competencies and other functions.	▪ Define and document workflows for specific processes in the organization.
11.10(g) Use of authority checks to ensure that only authorized individuals can use the system electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	▪ Allows for user roles to be set up each having its own set of access controls. ▪ Permit particular users to use certain functions. ▪ Limit other users from using them. ▪ Allow electronic signatures for various options such as updating courses.	▪ SOP on System Security and Access Control. ▪ Configure and maintain user access to specific areas within the LMS or via LDAP. ▪ Enable electronic signature features as required.
11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	▪ Not applicable for the LMS.	▪ Not applicable for the LMS.
11.10(i): Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	▪ Quality System documents the education, experience and training of NetDimensions staff.	▪ Vendor audit or checklist. ▪ Training records for system users and maintenance staff.

21 CFR 11 Requirement	NetDimensions Responsibilities	Customer Responsibilities
11.10(j): The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	▪ Not applicable.	▪ SOP on non-repudiation of electronic signatures.
11.10(k): Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	▪ Version controls are documented. ▪ Access to documentation is limited to user logon and password.	▪ SOP on Change Control. ▪ Retention of procedures dealing with system maintenance as defined under predicate rules for equipment maintenance. ▪ SOP on System Security and Access Control. ▪ Version control of all regulated documents.
§11.50 Signature Manifestations		
11.50(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	▪ Provide configurable electronic signature. ▪ The system tracks and audits the following: ▪ Printed Name of the signer, both first name, last name and user ID. ▪ The Date/Time signature was executed in the system. ▪ Meaning associated with the signature. ▪ Meanings (meanings can be customized in the system and are automatically applied to the appropriate action such as a course launch or course finish.	▪ SOPs governing user account setup include Input of the person's full name. ▪ List of full names to ensure that name is not duplicated (especially in larger companies). ▪ Configure and document the allowable meanings of signatures in the dropdown option.
11.50(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	▪ Technical controls in §11.10 as discussed above.	▪ Applicable sections of §11.10 apply to electronic signatures e.g. authorization, training, etc.

21 CFR 11 Requirement	NetDimensions Responsibilities	Customer Responsibilities
§11.70 Signature/Record Linking		
11.70 Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	▪ The link between an electronic signature and its executor's user ID cannot be broken. ▪ Provide encryption capability for secure electronic signatures. ▪ A user cannot be deleted in a CFR-enabled instance of NetDimensions Learning, and the user ID cannot be changed. ▪ Provide encryption capability for secure electronic signatures; the link between an electronic signature and its executor's user ID cannot be broken. ▪ A user cannot be deleted in a CFR-enabled instance of NetDimensions Learning, and the user ID cannot be changed.	▪ SOP for signing electronic records. ▪ Handwritten signatures on electronic records must be cross-referenced to the records signed. ▪ Applicable audit trail manifestations of electronic signatures and history of the specific record may need to be printed.
§11.100 General Requirements		
11.100(a): Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	▪ User IDs in the system are unique and a second identity of the same name cannot be created. ▪ Our guidelines recommend that you disable deletion of user accounts and learning modules if you want a CFR-compliant installation. That prevents reuse of the IDs.	▪ SOP on System Security and Access Control. ▪ Proper configuration of user accounts under. ▪ List of User IDs to prevent reissue or reuse of user ID. ▪ No group logon permitted.
11.100(b): Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	▪ Not applicable.	▪ SOP for verifying an individual's identity.
11.100(c): Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	▪ Not applicable.	▪ Pharmaceutical company or CRO sends a letter to the FDA. ▪ SOP on FDA Inspections.

21 CFR 11 Requirement	NetDimensions Responsibilities	Customer Responsibilities
§11.200 Electronic Signature Components and Controls		
11.200(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. Be used only by their genuine owners; and Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	▪ NetDimensions operations on a discontinuous identification control, therefore both signature components are required for each electronic signing.	▪ Interpret regulations for which records to sign in the LMS. ▪ Configure electronic signature options in the LMS application.
11.200(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	▪ Not applicable as biometrics not used.	▪ Not applicable.
§11.300 Controls for Identification Codes/Passwords		
11.300(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	▪ Since every user in the system has a unique user ID, this guarantees the uniqueness of user ID and password combinations. ▪ Our guidelines recommend that you disable deletion of user accounts and learning modules if you want a CFR-compliant installation. That prevents reuse of the IDs.	▪ Ensure user identities are never reused. ▪ Maintain historical list of User IDs and User Names from Windows® Security. ▪ Maintain history of security changes or Windows settings. ▪ Maintain list of application security changes.
11.300(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password ageing).	▪ The system can force the user to change their password periodically. The password change interval is configurable by the system administrator.	▪ Enable automatic password expiry. ▪ SOP on System Security and Access Control: check the list of users. ▪ SOP for the periodic review of system access logs against list of users.

21 CFR 11 Requirement	NetDimensions Responsibilities	Customer Responsibilities
11.300(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	▪ Functionality exists within the system to allow a user's password to be reset and a temporary password to be sent to the user's registered email address.	▪ SOP on System Security and Access Control.
11.300(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	▪ When the number of consecutive failed login attempts reaches a specified limit, the user's account becomes suspended to prevent further login attempts. ▪ The system administrator is notified before the user's account can be made active again.	▪ Enable inactivity lockout. ▪ Configure application for number of attempts to access system and automatic account lockout if permitted number of failed attempts is exceeded. ▪ Security Violations report lists unsuccessful log on attempts.
1.300(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	▪ Not applicable as tokens are not used.	▪ Not applicable.

Appendix

Auditable data fields.

Courses, Sessions and Modules

- Learning Object
- Course Contact List
- Course Access Level
- Course Download
- Course Schedule
- Course Evaluation
- Instructor Comment
- Course Revision
- Optional Paid Item Refund Deduction
- Course Owner
- Enrollment Policy
- Learning Object Attribute
- getAbstract Launch Properties
- Generic Virtual Classroom Launch Properties
- Course Audience
- Course Details
- Course Access User
- Course Session Cost
- Course Session Schedule
- Program Session
- Knowledge Center Options
- Course Optional Paid Items
- Course Objective
- Course Prerequisite
- Enrollment Policy Step
- Virtual Classroom Session Details
- GlobalEnglish Launch Properties
- WebEx Launch Properties
- Course Auto-enroll
- Course Access Level
- Course Content Server
- Course Test
- Program Courses
- Homework File
- Course Cost
- Custom Course Enrollment Policy
- Course Misc. Details
- Program
- Course Instructor
- Automatic E-mail Set-up
- Safari Books Launch Properties
- NETg Proxied Authentication

Questions

- Question Attributes
- True or False Question
- Fill in the Blank Question
- Multiple Choice Question
- Drag and Drop Question Draggable
- Hotspot Properties
- Question Properties
- Matching Question
- Rating Question
- Triple Rating Question
- Audio Capture Question
- Question Approval
- Single Choice Question
- Essay Question
- Triple Rating Question Item
- Drag and Drop Question
- Hotspot Question

Courseware

- Courseware Launch Options
- SCORM Sequencing
- SCORM Objective
- SCORM Objective Map
- Courseware Vendor
- CMI Assignable Unit
- Courseware Content Object
- SCORM Sequencing Rule
- SCORM Rollup Rule
- Courseware Content Organization
- Courseware Content Package
- CMI Descriptor
- Courseware Content Item
- SCORM Sequencing Rule Condition
- SCORM Rollup Condition
- Courseware Content Organization Node
- Courseware Content Organization Objective
- Courseware Content Organization Node Objective

Enrolments, Transcripts, Records

- Transcript
- Approval Queue
- Purchased Optional Paid Items
- Course Withdrawal Reason
- Approval Queue Step
- Learners Withdrawn from Course
- External Training
- Payment Details
- Course Withdrawal Refund Deduction

Exams		
Exam Question Properties	Exam Section Properties	Exam Properties
Exam Attempt	Exam Answer Attempt	Matching Question Attempt
Essay Question Attempt	Fill in the Blank Question Attempt	Rating Question Attempt
Audio Capture Question Attempt	Exam Attempt Section	Exam Random Section
Hotspot Answer	Drag and Drop Answer	Exam Comment
Triple Rating Question Attempt	Exam Print Properties	

About the Co-Author

Dr. Bob McDowall is a leading world expert in computer validation. He has 40 years experience as an analytical chemist including over 25 years computer validation experience. His areas of validation expertise include Chromatography Data Systems, Laboratory Information Management Systems, Adverse Event, Clinical Data Management Systems, Enterprise Resource Planning Systems and IT network and infrastructure qualification.

Dr. McDowall has published extensively on 21 CFR 11, computer validation and network infrastructure qualification. Dr. McDowall is on the editorial boards of Quality Assurance Journal, Spectroscopy, LC-GC North America and LC-GC Europe magazines and is currently the author of the columns entitled 'Questions of Quality' in LC-GC Europe and Focus on Quality in Spectroscopy. He is the recipient of the LIMS Award (1997) and the Association of Laboratory Automation (ALA) / Society of Laboratory Automation and Screening (SLAS) Long Service Instructor Awards in 2003 and 2011. He is also a trained auditor.

NetDimensions®
www.NetDimensions.com

North and South America

NetDimensions Inc.
1111 Cromwell Ave., Suite 302
Rocky Hill, CT 06067
Tel: +1 (860) 436 3898
Fax: +1 (860) 436 3896
E-mail: netd-americas@netdimensions.com

Europe, Middle East & Africa

NetDimensions (UK) Limited
Sandford House
Catteshall Lane
Godalming, Surrey
GU7 1LG, United Kingdom
Tel: 0870 042 7443 (within the UK)
Tel: +44 179 551 8016 (outside the UK)
Fax: +44 207 681 1485
E-mail: netd-emea@netdimensions.com

Asia Pacific & Rest of the World

NetDimensions Limited
17/F, Siu On Centre
188 Lockhart Road
Wan Chai, Hong Kong SAR
Tel: +852 2122 4500
Fax: +852 2869 8760
E-mail: info@netdimensions.com

NetDimensions Software (Shanghai) Co., Ltd.
Block 1, 457 North Shan Xi Road
Jing An District
Shanghai 200040
Tel: +86 21 6141 8480
Fax: +86 21 6141 8485

6/F, Tower 2, Prosper Centre
5 Guanghua Road, Chaoyang District
Beijing, China 100020
Tel: +86 1 8573 1030
E-mail: netd-cn@netdimensions.com

NetDimensions Services Asia Limited
Unit 1904, The Orient Square Building
Emerald Avenue, Ortigas Center
Pasig City, Philippines 1605
Tel: +632 914 1882 or 83
Fax: +632 470 2546
E-mail: info@netdimensions.com