



# NAVIGATING THE (EVER-CHANGING) COMPLIANCE LANDSCAPE

A Guide for Using Learning Management  
Systems to Meet Regulatory Compliance

Written by K.M. Lowe

Brought to you by GeoMetrix Data Systems Inc.

## Contents

The Road So Far .....	3
Electronic Record Management Systems .....	7
Agencies & Regulations .....	11
Regulatory Compliance for Electronic Systems.....	22
Open vs. Closed System.....	24
System Access: Profiles & Passwords .....	24
Verification & Validation .....	30
Revision Controls.....	32
Reporting & Generating Copies .....	34
System and Operational Checks .....	36
Product Documentation.....	37
Additional features .....	38
The Road Ahead .....	40
More Information .....	44
Abbreviations & Acronyms .....	47

## Materials Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of GeoMetrix Data Systems Inc. (GeoMetrix). These materials may be out of date, and GeoMetrix makes no commitment to update the materials. In no event will GeoMetrix, its suppliers or other third parties mentioned be liable for any damages whatsoever arising out of the use of this material or information contained therein.

This material is copyrighted to GeoMetrix Data Systems Inc. and any unauthorized use of it may violate copyright, trademark, and other laws.

# The Road So Far



A compliance survey carried out by the Brandon Hall Group a few years ago showed that demonstrating learning compliance to an external agency was important for 90% of the respondents. About 50% of all the organizations surveyed said it was actually critically important to their business. And in specific industries, the number

that said it was critical was much higher — more than 70% for “high consequence” industries.

High consequence is a term that has been used to describe those industries where compliance is essential. High consequence equals highly regulated, and for good reason. As the name suggests, errors in the activities of these organizations have severe consequences. Typically, these are industries where human life or quality of life is at stake, but not always. High consequence might relate to financial or intellectual property security. Examples of high consequence industries include food production, biotech, healthcare, aviation, nuclear power, and law enforcement.

For organizations in the high consequence category, an LMS may not be optional. These organizations may need their LMS — and all their other enterprise systems for that matter — to help them prove compliance to whatever rules are applied to their road.

But even for organizations in low or medium consequence industries, regulations still apply. No one in today’s business world

operates without rules. In fact, today's business environment is an increasingly complex maze of rules and regulations.

Legislation and standards are in place or being proposed for almost all aspects of business and industry. Throughout the world, regulations govern the manufacturing and handling of a variety of products for health and safety reasons. Other policies are designed to provide privacy and security or prevent fraud. These regulations are administered by government agencies, international organizations and industry associations, and compliance is sometimes voluntary but often mandatory.

Many of these laws and guidelines focus on the maintenance, security and auditing of records, and most were originally designed for printed documents. But with electronic data replacing printed documentation, new strategies are needed for dealing with regulatory compliance.

Some legislation has specified that requirements apply to all records regardless of their physical form. According to the U.S.

Food & Drug Administration (FDA), an electronic record can be “any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.”

Certain compliance standards, however, still require printed records, and for many organizations this means keeping both electronic and printed copies of data. For those regulations that permit the use of electronic data for compliance, strict guidelines are in place to ensure the security, confidentiality and authentication of those electronic records.



# Electronic Record Management Systems



Of course, the electronic records themselves are only part of what is necessary for compliance with legislation or standards. The internal policies and procedures that surround those electronic records form an important piece of the compliance puzzle. For example, most regulations require that an organization ensure the security of its electronic records.

Since a computer record is only as secure as the system that holds it, the organization must therefore make certain that the hardware and software comprising that system is secure as well. Technically, this also means securing the physical location of any servers or back-up copies of data and so on. No electronic record or system can meet such requirements — only an internal security policy and its associated procedures can.

While compliance with regulations is dependent on internal policies and procedures, the computer systems and the software that runs on them must provide the means to carry out those policies and procedures. An electronic records management system must therefore offer certain functionality to authenticate and validate the integrity of its records.

Records management procedures published by the U.S. Occupational Safety and Health Administration (OSHA) state that electronic records “require strict controls on their identification, maintenance, retrieval, use and disposition.” The U.S. FDA has regulations designed to ensure the integrity, trustworthiness,



reliability, traceability, and accountability of records management for organizations that produce or work with certain products. The policies of most regulatory bodies include language directed at ensuring the security of electronic records and the systems that support them. These systems must let organizations create, implement and verify security and auditing related to regulatory compliance.

Although a learning management system (LMS) or any of its components (learning management system; performance management system) is not involved in the manufacture of products normally covered by legislation or standards, it may manage the training of those who do. These systems often play an important role in the training and certification of individuals who operate equipment or carry out processes that are regulated.

A learning management system (LMS), for example, may carry records related to courses and learning activities that are critical to compliance. As a result, an LMS employed in an organization that is

subject to regulatory compliance must provide the same controls as any other electronic records management system.

Because computer systems have vastly different functions and architectures, the standards governing their use for regulatory compliance are often vague and open to interpretation. Regulations frequently do not offer hard-and-fast rules on how to comply. Instead they provide guidelines or an end-result, and each organization must determine the best way to accomplish that result. Regulated organizations are ultimately responsible for the computer systems in their facilities and for ensuring that those systems meet any regulations set out for them. However, since these organizations seldom design the systems they use, it falls to hardware and software vendors to interpret the standards and ensure that appropriate features and functions are available to meet them.

# Agencies & Regulations



There are a variety of regulatory bodies issuing rules that could apply to the records in a learning management system — and in

some cases, more than one agency will be applying rules. In some cases, agency jurisdiction intersects and even overlaps.

Established in 1947, the International Organization for Standardization (ISO) is the largest developer of standards in the world. ISO is a network of the national standards institutes of more than 150 different countries that publishes a range of standards for business and industry. When it comes to quality management standards, ISO 9000 is the most influential. The ISO Technical Committee 176 is responsible for developing these standards, which were originally inspired in the 1970s by the Canadian Standards Association's CSA Z299 series for quality and business management. Today, the secretariat of ISO/TC 176 is held by the Standards Council of Canada and administered by the CSA: [www.csagroup.org](http://www.csagroup.org).

ISO has also developed a code of practice for information security management. As with most other standards, ISO/IEC (International Electrotechnical Commission) 17799 is not a how-to guide, but instead provides guidelines and addresses topics in terms of policies and best practices. For more information on ISO/IEC 17799 visit

[www.iso.org](http://www.iso.org), or read the FAQ document published by the U.S. National Institute of Standards and Technology's Information Technology Laboratory at [www.csrc.nist.gov/publications](http://www.csrc.nist.gov/publications).

The British Standards Institute (BSI) takes the information security management code of practice one step further by providing actual specifications with guidance for use in its BS 799. The first part of this standard covers the code of practice, and the second part specifies requirements for establishing, implementing and documenting information security management systems and forms the basis for an assessment of the system. For more information about BS 799 visit the BSI website at [www.bsi-global.com](http://www.bsi-global.com).

In Europe, the DLM (Document Lifecycle Management) Forum, a constitutional organization of the European Union, provides appropriate guidelines, among other things, for public and private electronic records management. Back in 1999, a document titled “DLM-Message to the ICT industry,” the Information and Communication Technologies Industry (ICT) was asked to provide easily applicable and cost-effective records management and digital



archival solutions. In the year 2000, the European ICT industry responded with a publication on electronic document and records management with guidelines for authenticity, accessibility, privacy, security, user differentiation and more. These have evolved over time. To view the DLM guidelines visit <http://dlmforum.eu>





The U.S. FDA regulates food, drugs, medical devices, biologics, animal feed and drugs, cosmetics and radiation-emitting products such as cell phones for the U.S.A. The FDA 's rules for manufacturing and distribution are designed to protect consumers and promote public health. In the U.S. Code of Federal Regulations (CFR), Title 21 deals with Food & Drugs. Until recently, the regulations in this title required paper records with handwritten signatures.

In 1997, part 11 of 21 CFR was enacted to cover the use of electronic records and electronic signatures. Commonly known as 21 CFR 11, this part defines the criteria “under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.” For a complete list of the requirements of 21 CFR 11 visit: [www.gpo.gov](http://www.gpo.gov).

The Canadian Food Inspection Agency delivers all federal inspection services related to food, animal health and plant protection in Canada. The CFIA's Quality Management Program has a similar

record keeping requirement to that of the FDA that specifically lists personnel training records and can be viewed at [www.inspection.gc.ca](http://www.inspection.gc.ca).

The agency's "Facilities Inspection Manual" stipulates that when "microprocessor technology is used, specific controls must be developed to control the creation and maintenance of electronic records and electronic signatures," noting in an appendix that complying organizations "must develop and implement additional controls to demonstrate the reliability of the electronic records."

New Zealand's Food Safety Authority has a "Risk Management Programme" for animal products that requires record keeping procedures for records held in electronic or other form ([www.nzfsa.govt.nz/animalproducts](http://www.nzfsa.govt.nz/animalproducts)). Most countries have similar record management requirements for food and drug industries.

The U.S. Department of Labor's OSHA Records Management Program provides "records management procedures on OSHA records, nonrecords and personal papers, regardless of media." Available at



[www.osha.gov](http://www.osha.gov), Chapter V of this document covers the use of electronic records to comply with health and safety regulations. The U.S. Environmental Protection Agency has proposed the establishment of electronic reporting to satisfy certain document submission requirements in EPA's regulations ([www.epa.gov](http://www.epa.gov)). Title 14 of the U.S. CFR covers the acceptability of electronic recordkeeping systems for the U.S. Department of Transportation's Federal Aviation Administration. An Advisory Circular lists the records required and specifically mentions training records: [www.airweb.faa.gov](http://www.airweb.faa.gov).

Some standards organizations are not actually involved in the development of standards but simply administer the standards created by others. Many national standards organizations participate in a larger entity, such as ISO or IEC.




These agencies develop standards by participating on international committees rather than working on their own. For example, the International Committee for Information Technology Standards (INCITS) is the primary U.S. focus of standardization in the field of information and communications technologies. As such it serves as the American National Standards Institute's Technical Advisory Group for ISO/IEC. INCITS has a policy of adopting standards that

were developed internationally with the Joint Technical Committee 1 of ISO/IEC.

Standards Australia is Australia's representative on the International Organization for Standardization, the International Electrotechnical Commission, and the Pacific Area Standards Congress. Australia has adopted ISO's Records Management standards, which "sets out the records management processes of registering, classifying, indexing and tracking an organization's records to identify them uniquely in a recordkeeping system and to enable them to be retrieved effectively and accurately. The published standards are distributed by SAI Global under contract to Standards Australia: [www.standards.com.au](http://www.standards.com.au).

And most public agencies themselves are subject to record management standards. For example, the Australian government is subject to the "Territories Record Act" available through [www.territoryrecords.act.gov.au](http://www.territoryrecords.act.gov.au). Government departments in Canada are ruled the "National Archives of Canada Act" and "Canada's Access to Information Act." U.S. agencies are governed





by the “Federal Records Act” and “National Archives and Records Administration” (NARA) regulations 36 CFR Chapter 121 for electronic records management. The U.S. Department of Energy (DOE) publication “Electronic Records Management Guide” provides guidance for the department on managing electronic records. This guide combines DOE guidelines with those of NARA, the General Services Administration and the Office of Management and Budget: [www.directives.doe.gov](http://www.directives.doe.gov).

The standards and policies published by or for most agencies include language directed at ensuring the security of the electronic system or the content of the information presented, and usually both. Most of these agencies have regulations for electronic records as an option. Regulations do not normally mandate, but rather permit, the use of electronic records for compliance. FDA's 21 CFR 11 states that “... persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.” Organizations that do not wish to, or are not



prepared to, use electronic records can often continue to use traditional documents with hand-written signatures.

And it is also important to remember that standards for electronic records are evolving as the systems that support them evolve and, therefore, should be reviewed regularly. For some organizations, this means dealing with evolving regulations from multiple agencies at the same time. Record holders should consider a strategy of systems and procedures that provides an ideal combination of short-term compliance with long-term sustainability.

If your organization is one of those that is subject to regulations from more than one agency, you should take some comfort in the fact that the rules are similar, if not identical, when it comes to electronic records management. And, as noted earlier, instead of strict rules, they provide guidelines or an end-result. Chances are, as long as you meet the guidelines of one agency, you will meet another. The safest policy then would be to meet the most stringent set of rules and in the process meet all the lesser ones as well.

# Regulatory Compliance for Electronic Systems



Essentially, the concerns about using electronic records are that records can be lost in a system crash, the data can become corrupt or modifications can be made without proper authorization. In addition, since printed documents with hand-written signatures are recognized as legally binding on the signatories, the agencies are looking for ways to make electronic records similarly binding on

their owners. The regulations have been proposed to ensure that whenever an organization replaces printed documents with electronic data, there are checks and balances in place to ensure integrity of the electronic records so that they can be legally equivalent to printed records.

Since staff training, performance management and certifications are critical to ensuring quality standards for any regulated products, facilities may be required to submit worker records, authenticate those records and validate the systems that support them.

To help customers fulfill requirements, learning management systems and all their components should include a range of features for security, authentication, validation and auditing. Since the FDA's 21 CFR 11 covers similar provisions to most standards for electronic records, we will use its requirements as reference points.

## Open vs. Closed System

Many standards distinguish between open systems and closed systems. The FDA defines an open system as one in which system access is not controlled by persons who are responsible for the content of electronic records and a closed system as one in which system access is controlled by persons who are responsible for the content of electronic records. Learning management systems usually fall into the latter category, and therefore, would need to comply with the regulations set out for closed systems. If operational control of the system is outside the regulated organization (a Web-based portal service from an application service provider, for example), it may be considered an open system, which can require additional safeguards.

## System Access: Profiles & Passwords

A significant component of most standards is controlled access to electronic records. Regulatory bodies want assurances that only authorized users can access and make changes to records. Most

regulations stipulate that access be controlled by two distinct identification components. This is satisfied in most systems by a user code and password. Access to the LMS should be through a unique username and password. The unique combination of username and password creates a digital signature for that user.

Attached to each digital signature is a user profile that controls that individual's rights and privileges while in the system. Only system administrators should have access to user profiles in the LMS satisfying 21 CFR 11's requirements for "transaction safeguards to prevent unauthorized use of passwords and/or identification codes." Also, certain reports and customization options should only be accessible by the system administrator. For security purposes, we recommend only one or two individuals in an organization be given system administrator status and be responsible for user profiles.

By means of individual profiles, a user is assigned specific rights on an item-by-item basis that creates a unique outline specific to that individual. Using group profiles, individuals are assigned to a group

and receive the security rights designated for that group. For each item listed in a profile, there should be several access levels from which to choose from low security to high.

Access to reports should also be provided by multiple security level, since they pull information from the database. Only reports with the same or lower security level as that assigned to the user profile should be visible to that individual. If a report has a security level of 4 and a user only has a security level of 3, the report should not be listed when that user is logged on. To offer further control, an organization should have the option to disable users' ability to create, modify or delete reports – essentially giving that user 'read' access only.

This kind of user profile system lets an organization selectively limit the areas of the program that users can enter. Thus, a training registrar might have full access to worker information, but may not have the ability to edit or delete courses or instructors; whereas a person in charge of scheduling might have full access rights to



courses, instructors and scheduling, but no access to worker records and enrolment information.

Security settings as described above comply with 21 CFR 11's requirement that the system “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.”

Most regulatory standards also require systems to re-authorize users after a set period of inactivity. This is designed to prevent someone else accessing a work station when the logged-in user walks away from it. The system should be set to shut-down after a specified period of time — forcing users to restart the application and log on again to regain access. The requirement in 21 CFR 11 states, “Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.”

To satisfy such a requirement, the system should be set to terminate the application after a set amount of inactivity. This

prevents unauthorized users from accessing the application when the authorized user is not present

An LMS should of course have specific rules for password creation to help ensure that passwords cannot be guessed easily. The system should require that passwords contain at least six characters, have at least three alphabetical characters, must begin and end with alphabetical characters, do not contain month or weekday names or abbreviations, and are not previously used passwords.

Regulatory standards typically also require that passwords be changed on a regular basis to increase system security as in 21 CFR 11's requirements to ensure "that identification code and password issuances are periodically checked, recalled, or revised..." The LMS should have settings to force users to change their passwords on a regular basis. The system should have options to require passwords to be changed every set number of days (typically 60, 90, or 120 days).

If your organization has single-sign on for all enterprise systems, the users should be required to change that one password within the time period mandated by the highest security guideline. Since there are rules in high consequence regulations that require daily password changes, single sign-on may not be practical for all systems. Luckily, most are not that stringent, but that should be a consideration when reviewing single sign-on.

FDA 21 CFR 11 requires “maintaining the uniqueness of each digital signature “such that no two individuals have the same combination of identification code and password.” The system's user naming system should reject duplicates of user names that are already in the system at the creation or edit point. Since only system administrators should have access to user profiles, it is easy to enforce a policy that either prevents deleting user names or re-issuing user names that have been deleted. This should satisfy the requirement that each electronic signature “shall not be reused by, or reassigned to, anyone else.”

Another requirement of 21 CFR 11 is that the system 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.”

Encrypting user passwords can prevents users with the ability to access the database outside of the application from determining user passwords.

## Verification & Validation

Most regulatory standards also require that audit trails of key information be maintained. “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” is a requirement of 21 CFR 11.

Again, deciding on which information is key within the system will depend upon internal policies and procedures and how specific data is used, but the LMS should maintain certain logs. A translation log provides a list of records that have been changed, when they were

changed and which user changed them. A field changes log can be used to track individual changes made to specified fields.

Regulatory bodies typically require that key record changes be verified, i.e., an individual accepts responsibility (and 'signs') for the fact that the record change has been reviewed. For example, 21 CFR 11 states, “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.”

Once key records have been identified, the system should allow you to require a digitally verified signature on change of those records. This forces users to 'sign' for the fact that they have altered the record by providing a digital signature to proceed with the change. The LMS should allow for verification to be placed on any of the core data tables within the system. When a record is verified, users must re-enter a valid username and password (even though they

have logged on) to accept the change. Record validation is also logged to the system transaction log for that user.

## Revision Controls

Some regulations require revision controls for electronic records to ensure that “record changes shall not obscure previously recorded information” (21 CFR 11). This is also used to ensure that those 'reading' a document are informed of changes to the information. Within a regulated industry, it is important to be able to maintain previous versions of documents.

Essentially, standards specify that once key records are 'published,' they cannot be altered. Instead another version of the document must be created. A LMS should support versioning for courses, programs and job roles, since these are most commonly considered 'documents' or key records within regulated industries.

The system should preserve versioning information throughout related records, so that it is possible to tell what version of a course



was taken by a specific worker. This information should be kept indefinitely to satisfy a requirement such as 21 CFR 11's "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."

Course upgrades can work in conjunction with versioning to fill in learning gaps between different course versions. If a new version of a course has been created due to a change in content, you can update the skills of workers who have taken previous versions using an upgrade course. Workers are presented with new or changed materials without having to re-take the entire course. Using the upgrade feature, completion of the upgrade course will automatically credit the worker to the new version.

A course equivalency feature can make one course provide the equivalent completion to another for purposes of prerequisite checking or degree programs and certifications. Equivalencies should work in one direction only to prevent workers receiving credit for more advanced learning than what was taken. Versioning,

upgrading and equivalencies give you comprehensive administration and tracking of courses to help you accelerate learning, while controlling data and easing the challenges of change.

For documents other than courses, programs and job roles, another document control option is a document library that can store different versions of documents in a global repository. Thus, it is possible to see exactly which version of a document was used with an individual or group at a particular time – and to access the document itself to view its contents.

## Reporting & Generating Copies

Generating printed copies of records or data is often critical to compliance with industry standards or legislation. In 21 CFR 11 it states that to be compliant the system must have 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.”

You should be able to print critical data directly from the application and standard reports should be available for particular business process and for regulatory compliance verification.

For specific requirements, the system should allow custom reports to be created. Reports should have options that allow filtering by date, groups, course, facility, equipment, instructor, organization, student, class and more. Administrative users should be able to quickly and easily modify columns, sorting, grouping, fonts, column titles and other properties, saving the new version of the report as needed. Administrative users should be able to create fields in the database, customize dialogs for data entry/manipulation and show customized fields within any report. The LMS should allow reports to be exported directly (as HTML, RTF, PDF, Text or ASCII) to Word or Excel and printed or incorporated into other documents as necessary.

## System and Operational Checks

Standards and regulations often require specific operational and security checks. A requirement in 21 CFR 11 states that a system should “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.” This can be accomplished differently for different organizations and is dependent on how the system is used. In some cases, the operating system will supply this security feature. For others, the database will have its own security features. In some cases a customization in the system at the appropriate point using a macro will meet the requirement.

Another section of 21 CFR 11 requires the “Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.” Again, how this is accomplished will depend on the particular operation or sequence of steps. Certain operations in the LMS should already be limited to a specific sequence. For others, a system administrator should be able to set up 'scheduled actions'

within the LMS to be executed automatically. And in some cases a custom macro may be appropriate. Regardless of the need, the system should be able to accommodate the operational system check that is required.

## Product Documentation

To help organizations with any requirements to document their systems and procedures, the vendor should provide a comprehensive set of software guides for the learning management system, in addition to a searchable help system.

However, regulations sometimes require the use of appropriate controls over system documentation, “Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance” (21 CFR 11). In this case, a solution is to have only one set of printed product documentation held by a system administrator. Electronic versions can be removed from the product if they are normally included.

## Additional features

Standards usually require that an electronic records management system maintain a directory and sub-directory structure similar to a paper document filing system. An OSHA requirement for filing electronic records is that the “directory and sub-directory structure used to file documents should be similar to the file system contained in OSHA Instruction ADM 12-0.1 used to file paper documents” (V-B-1). The LMS should offer a directory/sub-directory structure to organize files. The system should allow for multiple levels of parent and child folders to arrange information.

In addition to ensuring unique names for users, organizations should be able to set the system to allow only unique codes for any item in the system. This option can satisfy regulations for data integrity by ensuring there are no duplicates of any key records.

Organizations that are subject to regulatory compliance may have specific data tracking or usage requirements. To accommodate



these, the LMS should provide customization options, such as a form editor and/or macroing language.

The LMS should provide the option to hide fields that contain sensitive data or are not applicable to users – or reposition commonly used or required fields to make them more easily accessible. The system should allow renaming of labels to match industry standards or regulatory terminology and the creation of custom fields to track information specific to an operation or regulation.

Records must be stored and maintained for specific lengths of time for validation purposes. Back-up strategies are necessary to cover problems that may occur throughout the life of a system from mistakenly deleting files to a large disaster.

To assist organizations with securing data integrity and longevity, the vendor should provide written recommendations for back-up and recovery strategies that outlines considerations, requirements and a suggested plan.

# The Road Ahead



The upcoming compliance road for some industries may be signposted with more stringent rules, while others may see signs come down through deregulation. We don't know for sure what lies ahead

through the tunnel that leads to the future. But it's best to err on the side of caution and assume that the world will become more regulated rather than less.

The one thing we can be fairly certain of is that electronic record keeping is not going away and will likely play an even bigger part in meeting regulatory compliance. But regardless of whether an organization chooses to use electronic records in lieu of printed records for compliance, standard operating procedures for most activities are required by regulated organizations. Organizations that choose to comply using printed records must still have sufficient security and processes to ensure the authenticity of records and signatures.

For those organizations that decide to comply using electronic records, a learning management system needs to provide the means to verify and validate electronic records related to training and certification. Used as an operational tool, an LMS and components can help an organization meet quality management standards by

tracking the training, performance and certification of individuals carrying out regulated activities.

The road to compliance may at times seem to be all up hill with speed bumps and hairpin curves. But in fact, it's fairly straight and follows a logical route. The signposts may sometimes be vague and act as guidelines rather than strict laws, but that's to give organizations flexibility in how they achieve the end result. Overall, the compliance landscape is navigable by those who read the regulations and apply good practices to their processes and procedures.



For information on how the GeoTalent Learning Management System can help you navigate compliance, please visit [www.geotalent.com](http://www.geotalent.com), call 1-800-616-5409 or email [sales@geotalent.com](mailto:sales@geotalent.com).

## More Information

The following resources can provide more information on electronic records management and the standards that govern them.

American National Standards Institute (formerly the National Standards Systems Network or NSSN) provides a comprehensive data network on national and international standards and regulatory documents. Searchers can use document numbers, key words and organizations to find specific standards. The results provide an overview of the standard or document, which organization published it, and where to find or purchase a copy: [www.ansi.org](http://www.ansi.org) .

The Association of Records Management Administrators International offers invaluable resources such as legislative and regulatory updates; standards and best practices; technology trends and applications; live and Web-based education; marketplace news and analysis; and books and videos: [www.arma.org](http://www.arma.org).



Since the secretariat of ISO/TC 176, which is responsible for ISO 9000 is held by the Standards Council of Canada and administered by the CSA, the CSA publishes a wide range of documents and checklists designed to help organizations in their quest for ISO 9000 compliance: [www.csagroup.org](http://www.csagroup.org).

The National Institute of Standards and Technology's Computer Security Division provides a variety of publications and resources related to computer security on its website: [www.csrc.nist.gov/publications/index.html](http://www.csrc.nist.gov/publications/index.html).

The State of California publishes an excellent handbook that includes comprehensive information on electronic records management along with a glossary. The Electronic Records Management Handbook is available at [www.dgs.ca.gov](http://www.dgs.ca.gov).

The Government of South Australia publishes the Glossary of Records Management Terms, which should be available at [www.archives.sa.gov.au](http://www.archives.sa.gov.au)



# Abbreviations & Acronyms

ADL	Advanced Distributed Learning	U.S.A.	<a href="http://www.adlnet.org">www.adlnet.org</a>
AICC	Aviation Industry CBT Committee	International	See SCORM
ANSI	American National Standards Institute	U.S.A.	<a href="http://www.ansi.org">www.ansi.org</a>
ARMA	Association of Records Managers and Administrators	International	<a href="http://www.arma.org">www.arma.org</a>
BSI	British Standards Institute	United Kingdom	<a href="http://www.bsi-global.com">www.bsi-global.com</a>
CFIA	Canadian Food Inspection Agency	Canada	<a href="http://www.inspection.gc.ca">www.inspection.gc.ca</a>
CFR	Code of Federal Regulations	U.S.A.	<a href="http://www.gpo.gov">www.gpo.gov</a>
CSA	Canadian Standards Association	Canada	<a href="http://www.csagroup.org">www.csagroup.org</a>
DOE	Department of Energy	U.S.A.	<a href="http://www.energy.gov">www.energy.gov</a>
EC	European Community	Europe	<a href="http://www.europa.eu">www.europa.eu</a>
EEC	European Economic Community	Europe	<a href="http://www.europa.eu">www.europa.eu</a>
EPA	Environmental Protection Agency	U.S.A.	<a href="http://www.epa.gov">www.epa.gov</a>
EU	European Union	Europe	<a href="http://www.europa.eu">www.europa.eu</a>
FAA	Federal Aviation Administration	U.S.A.	<a href="http://www.faa.gov">www.faa.gov</a>
FDA	Food & Drug Administration	U.S.A.	<a href="http://www.fda.gov">www.fda.gov</a>
FRA	Federal Records Act	U.S.A.	<a href="http://www.usa.gov">www.usa.gov</a>
GSA	General Services Administration	U.S.A.	<a href="http://www.gsa.gov">www.gsa.gov</a>
IEC	International Electrotechnical Commission	International	<a href="http://www.iec.ch">www.iec.ch</a>
INCITS	International Committee for IT Standards	U.S.A.	<a href="http://www.ncits.org">www.ncits.org</a>
ISO	International Organization for Standards	International	<a href="http://www.iso.org">www.iso.org</a>
NARA	National Archives and Records Administration	U.S.A.	<a href="http://www.archives.gov">www.archives.gov</a>
NIST	National Institute of Standards and Technology	U.S.A.	<a href="http://www.nist.gov">www.nist.gov</a>
NZFSA	New Zealand Food Safety Authority	New Zealand	<a href="http://www.nzfsa.govt.nz">www.nzfsa.govt.nz</a>
OSHA	Occupational Safety & Health Administration	U.S.A.	<a href="http://www.osha.gov">www.osha.gov</a>
PASC	Pacific Area Standards Congress	Asia-pacific	<a href="http://www.pascnet.org">www.pascnet.org</a>
SA	Standards Australia	Australia	<a href="http://www.standards.org.au">www.standards.org.au</a>
SCC	Standards Council of Canada	Canada	<a href="http://www.scc.ca">www.scc.ca</a>
SCORM	Sharable Content Object Reference Model	International	<a href="http://www.adlnet.org">www.adlnet.org</a>
TC	Technical Committee (ISO TC)	International	<a href="http://www.iso.org">www.iso.org</a>
TRA	Territories Record Act	Australia	<a href="http://www.territoryrecords.act.gov.au">www.territoryrecords.act.gov.au</a>

## About GeoTalent

GeoTalent is a unified Learning and Talent Management System that incorporates our TrainingPartner LMS. This cost-effective alternative to high-priced enterprise systems offers the customizability that GeoTalent customers have come to know.

1-800-616-5409  
250-361-9300  
[sales@geotalent.com](mailto:sales@geotalent.com)  
[www.geotalent.com](http://www.geotalent.com)

