Standardization Efforts to Secure Security in E-learning

Dragan Zlatkovic[1], Nebojsa Denic[2], Milos Ilic[3], Milena Petrovic[4]
[1, 3]Alfa BK University in Belgrade
3 Palimira Toljatija, Belgrade 11070, Serbia
{dragan.zlatkovic@sbb.rs, milos.ilic@alfa.edu.rs}

[2, 4]University of Pristina, 29 Ivo Lola Ribara
Kosovska Mitrovica 38220 Serbia
{nebojsa.denic@pr.ac.rs, milena.petrovic@pr.ac.rs}

ABSTRACT: *Standardization with information security is required to optimum use of e-learning process. We in this work have evolved framework for quality assurance and used the security as well as learning parameters as input. We in this process have used the PDCA cycle and enhanced the system with a good LTSA architecture.*

Keywords: E-learning, Standards, Security, PDCA Cycle, LTSA

Received: 18 April 2020, Revised 4 August 2020, Accepted 12 August 2020

DOI: 10.6025/jism/2020/10/4/103-110

1. Introduction

Quality assurance in e-learning is a natural continuation of education quality in general. Thanks to the specificities of this type of teaching/learning, special procedures and schemes for quality assurance have been developed at different levels: at the level of educational software, at the level of the individual course institution, at the level of the study program or institution. Because quality of e-learning is associated with security, these schemes also address security issues through their criteria.

Regardless of the purposes of the information system used, there are general safety recommendations and standards that are defined by specific documents. ISO International Standardization Organization has provided best practices for information security management through its set of ISO 27K standards [1].

When creating any model, it is necessary to take into account the standards that deal with the given area in general (in this case, the information security), as well as standards dealing with security in a specific field (e-learning), as part of a specific form of regulation. In this paper is a brief overview of standardization in security and relevant standardization in e-learning.

2. Standardisation of Security

Official standardization is presented through a set of ISO/IEC 27K family documents [2]. Some of the essential standards related to "information technology - security techniques" are:

• ISO/IEC 27000 – Information security management systems — Overview and vocabulary;

• ISO/IEC 27001 - Information technology - Security Techniques - Information security management systems-Requirements;

• ISO/IEC 27002 – Code of practice for information security controls - virtually a detailed catalog of information security controls that might be managed through the ISMS, etc.

The security management philosophy in the 2005 standard version relied on the PDCA methodology, Fig. 1, while in the new version (2013), this approach is placed in the other plan, with an emphasis on the quality of organization's security and compatibility with different standards, especially with ISO 9000.

Entry to this circle is the requirements and expectations of interested parties-stakeholders, and the exit is security management.

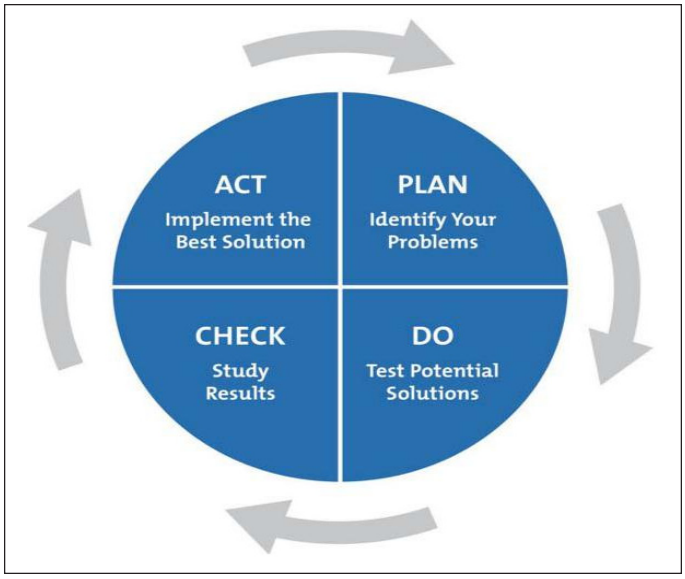

Figure 1. The Plan–Do–Check–Act (PDCA) Quality Cycle

The standard ISO/IEC 27002 (2015) presents a particular set of good practice recommendations, which can be applied in a wide range of information systems, including an e-learning system [1].

The first step is the risk assessment, which establishes, quantifies and prioritizes the risks to the given criteria for accepting risks and goals that are important for the organization itself. The results should serve as a guide to further management actions and prioritization in managing security risks and implementing security measures [3].

The risk can be assessed at the level of the whole organization, its parts, specific system components or even at the level of the service. After carrying out a risk assessment, it is necessary to define the appropriate risk management mode [4]:

- Apply the appropriate protection measure; accept risk;
- Avoid risk by not carrying out activities that would lead to it;
- Transfer risk to another (suppliers, insurance company).

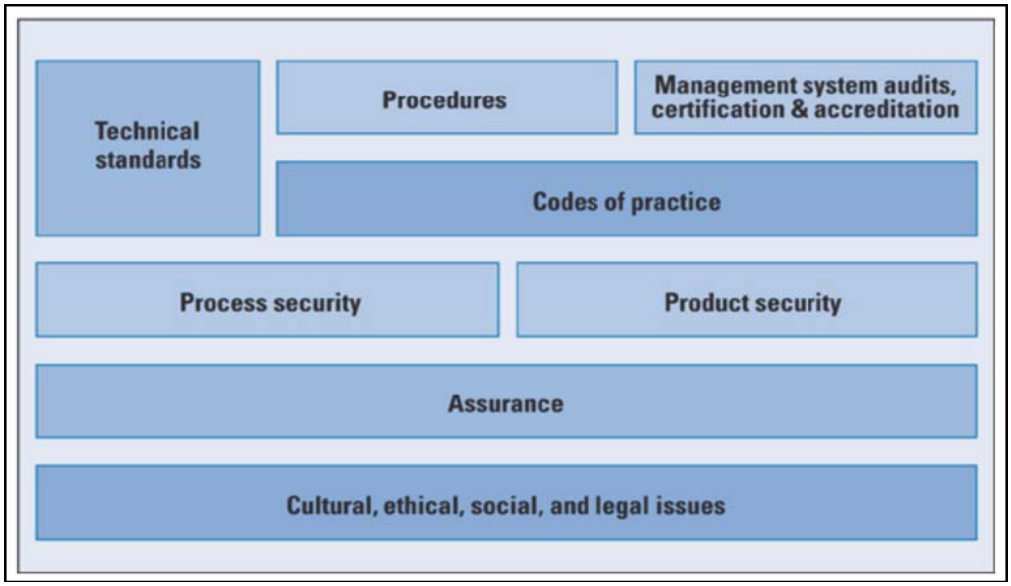

Figure 2. Information Security Management Elements (according to ISO Standard)

Through eleven classes of protection measures, many safety-relevant categories have been defined, such as, for example, "Information security awareness, education, and training," and given is the goal of the protection measure and one or more protection measures applied to achieve the goal. ISO "protection measure" is called a control [5].

Guidelines for auditors on information security controls provide instructions to auditors to review the implementation and the correctness of the protection measures, including verifying the technical compatibility of these measures and the established standards of the organization. If the protection process covers the e-learning system, these recommendations can be further exploited precisely to verify that system or its protection measures [4].

3. Information Security within E-learning Standards

Some organizations deal with the creation of standards and recommendations in the field of e-learning. Among the most important are the Learning Technology Standardization Committee (LTSC), the IMS Global Learning Consortium, the Aviation Industry CBT Committee (AICC) and the U.S. Department of Defense Advanced Distributed Learning (ADL).

The e-learning standards generally consist of several parts [6]. The first describes the data model and provides norms and content abstracts, the other is a formal description (mainly through XML), and the third represents the API, an interface for collaboration with other systems.

A very detailed overview of e-learning standards is given in [7].

3.1. IEEE 1484

The most famous and most detailed standard is IEEE 1484[8]. Within the segment 1484.1-2003 of the IEEE Standard for Learning Technology - Learning Technology Systems Architecture (LTSA), a high-level e-learning model is also given. The task of this architecture is to provide a high-level framework for the development of various e-learning systems and facilitate their evaluation and comparison.

In addition to the IEEE 1484 working group, LTSA was developed through the activities of various other organizations [8]:

- DoD Advanced Distributed Learning (ADL)
- Aviation Industry Computer-Based Training (CBT) Committee (AICC)

• American National Standards Institute, Information Infrastructure Standards Panel (ANSI IISP)

• Architecture Abstraction Hierarchy Reference Model, by Frank Belz, Dan Suthers, Tom Wheeler.

• Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE)

• Tool/Agent Communication, by Steven Ritter - Carnegie Mellon University (CMU)

• Common Object Request Broker Architecture of Object Management Group (OMG), Medical Informatics (CORBAMED)

• Apple Computer's Educational Object Economy (EOE)

• Educom's Instructional Management Systems Project (IMS)

• International Standards Organization - International Electrotechnical Committee, Joint Technical Committee 1 - Information Technology, Business Team on Electronic Commerce (ISO-IEC JTC1 BT-EC)

• Global Information Infrastructure - Standards Roadmap: a catalog and analysis of GII standards (ISO-IEC JTC1 GII)

• Cultural Adaptability Workshop (ISO-IEC JTC1 CAW)

• Standards Operations Roundtable (ISO-IEC JTC1 SORT).

LTSA Components are [8]:

• **Processes:** Learner, Evaluation, System Coach, Delivery process;

• **Flows:** Behavior, Assessment, Performance, Query Index, Content Index, Locator Index, Learning Content, Multimedia, Learning Style;

• **Data Storage:** Records Database, Knowledge Library.

The "Learner Process" is an abstraction of students and can represent an individual student, a group of learners who learn individually, a group that determines collaboratively, and so on.

The student receives a multimedia setting, and his behavior is watched. At this level of abstraction, multimedia and observed behavior are shown separately. However, real implementations usually combine these elements into one or more interface modules, such as window systems, presentation in a web browser, specialized applications, etc.

The learning style is established in cooperation with the System Instructor.

The process of behavior represents the student's coded behavior, from the student to the evaluation process. In this process, practice is embedded in an appropriate context by matching learning content with a specific range of behavioral responses.

Encoding behavior is how behavior information is organized, for example, key press, mouse click, voice command, etc. Coding represents the student's behavior independent of the content of learning [3].

The evaluation process results in the evaluation information and sends the evaluation details to the System Instructor. The evaluation process creates information about achievement, which is stored in the Records Database.

The evaluation process uses the learning content object to provide a context student's behavior and determine the appropriate evaluation.

The evaluation process sends out information about achievement and keeps the database (for example, "question 12, answered correctly – student spent 57 seconds") [5].

The knowledge library keeps different data (tutorials, tools, experiments ...). Related material is provided based on the Context Index (metadata). Based on these metadata, the delivery process supplies Content [9].

The delivery process transforms content acquired from the knowledge library into the appropriate multimedia form.

LTSA Implementation in Online Learning

As already stated, LTSA is a generic architecture. In the concrete implementation (for example, in e-learning), mapping of individual components into appropriate representations of the electronic learning system is achieved. Fig. 3, shows that the user - the learner is mapped into the LTSA learner component and a database of courses in the knowledge library.

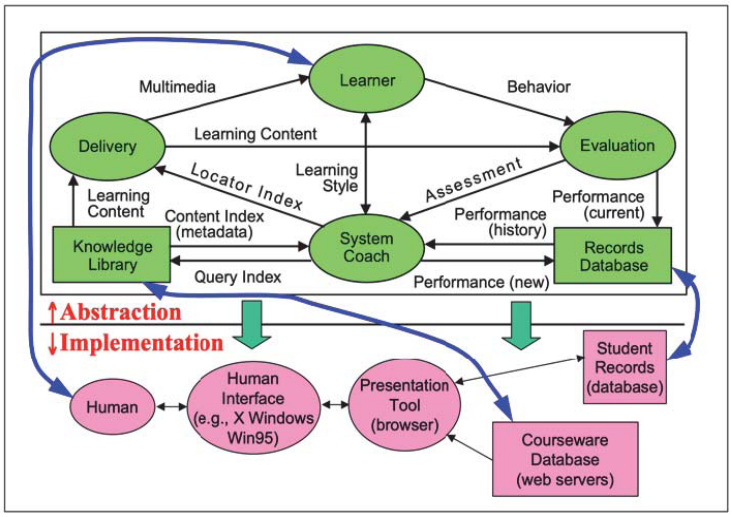

Figure 3. Mapping the LTSA components of the online learning scenario [8]

Security elements in IEEE 1484.

Table 1 briefly shows the security related features of IEEE 1484 standard [10].

Model	Specification	Model	Specification
Session – View Security	D	Non-Repudiation	I
Security Parameter Negotiation	D	Repudiation	I
Security Extension	D	Privacy	N
Access Control	D	Confidentiality	N
Identification	I	Encryption	N
Authentication	O	Data Integrity	N
De-identification	O	Validation of Certificates	N
Authorization	I	Digital Signature	N
Delegation	I		

Table 1. Security Features Defined In Ieep P1848

D – Defined: The model and/or requirements are defined or provided.

I – Implementation-dependent: The detailed methods are depended on detail implementations.

O – Outside the Scope: The methods are outside the standard.

N – Non-specified: The standard doesn't specify the model and requirements.

Within the LTSA standard, a particular part - Public and Private Information (PAPI) deals with the student himself, that is, the syntax and semantics of his information and forms of access. The elements deal with skills, abilities, contact information, learning style, performance, personal portfolio, security parameters. The standard provides different types of information review, according to the appropriate roles: teacher, student, parent, employer [11].

PAPI specifically addresses the issue of access to external repositories and provides for the creation of the so-called the surrogate of the identifier, by which the student registers to the external service, thereby eliminating the possibility of its monitoring [7].

3.2. IMS Global Learning Consortium LIP

IMS Global Learning Consortium is an organization that develops open e-learning recommendations, addressing key issues and challenges in distributed learning environments across a range of specifications, including metadata, enterprise specifications, learning package specifications, tests and questions [12]. Among other things, the IMS specification Learner Information Package (IMS LIP) addresses the interoperability of the student's information system with other learning systems [13]. Student data is designed as a collection of student data and typically contains a record of the level of education, a learning diary, a lifelong learning diary, and so on.

IMS LOM deals with privacy issues in Version 1.0, and in this segment attaches great importance. There are two mechanisms proposed [13]:

Support for the inclusion of data describing the level of privacy, access rights, and data integrity. These data are defined through a special meta-structure.

Support for user data that would be used to secure data transfer. This information is defined as a student's security key (learner security key).

Security keys constitute a structure that keeps different keys providing communication between learners and systems and e-learning services.

Unlike PAPI, IMS besides data also provides a model or metadata that supports modeling. Also, this model itself is extremely flexible.

3.3. Educause-Internet2 Eduperson

EduPerson's specifications came from the Internet2 Initiative and EduCause [14]. It represents an attempt to model of typical student information, as well as other entities in the institution, as part of the Lightweight Directory Access Protocol Scheme (LDAP), which would facilitate the creation of institutional directories by providing appropriate templates.

EduPerson is not broad as PAPI, and since it covers a more whole class of users than students (employees, alumni), it provides less specific information: name, nickname, organization, contact information, photo, preferred language, etc.

Necessary attributes related to security are userCertificate and userSMIMECertificate. They define the X.509 student certificate or the certificate for Multipurpose Internet Mail Extensions (MIME) e-mail applications.

Other standards related to e-learning are mainly dealing with content and do not treat security issues. For example [15]:

The AICC focuses on practical aspects, providing recommendations for platforms for e-learning, peripherals, audio devices,

and similar implementation details.

The ARIADNE deals mainly with metadata to share and reuse materials.

The ADL-SCORM is oriented towards methods of aggregation, description, and sequencing of learning objects.

4. Conclusion

Despite the existence of different standards and their detailed specification, the issue of their implementation remains open. In many modern e-learning environments, support for standards was not included at the start, either because they were not developed at that time, either because of the lack of attachment of crucial importance to standards (assessing that implementation is unprofitable). Therefore, for systems already in operation, it is not easy to add support for standards, because in some segments it would require complete reengineering.

Specific general international standards are dealing with information security and which can be used to design a security information system or an appropriate module in any environment. These options relate to the design methodology, but also specific practices (according to ISO 27002). PDCA is recognized as a methodology suitable for designing modules.

There are a large number of non-compliant e-learning standards, and the security of information considers a number of these standards. In practice, these elements are not implemented on a broader scale. The reasons for this can be sought in the complexity of the proposed solutions. On the other hand, the standards are relatively flexible so that they can be expanded and adapted to a particular need.

References

[1] Standard SRPS ISO/IEC 27001R Institute for Standardization of Serbia, Belgrade, 2015.

[2] ISO 27000,R 2013. [Online]. Available: http://www.27000.org. [Accessed: 02 Apr-2019].

[3] Zlatkovic, D., Denic, N., Petrovic, M., Ilic, M. (2019). An Qualitative Analysis of the Effects of E-learning on Students Intristic MotivationR, ITOP'19, Conference Proceedings, p 185-193, Cacak, Serbia, 2019.

[4] Nikolic, V., Petkovic, D., Denic, N., Milovancevic, M. (2019). Appraisal and review of e-learning and ICT systems in teaching processR, *Physica A: Statistical Mechanics and its Applications*, Vol. 513, p 456-464, 2019. https://doi.org/10.1016/j.physa.2018.09.003.

[5] Milosevic, M. (2016). Development and Implementation of the Security Moduls and its Impact on the Quality of E-learning R, Cacak, FTN.

[6] Anido-Rifon, L. E., Fernandez-Iglesias, M. J., Caeiro-RodrMguez, M., Santos-Gago, J. M., Llamas-Nistal, M., Alvarez Sabucedo, L., MMguez Perez, R. (2014). Standardization in computer-based education, R *Computer Standards & Interfaces*, 36 (3), p 604–625.

[7] Jerman-Blazic, B., Klobucar, T. (2005). Privacy provision in e-learning standardized systems: status and improvements, R *Computer Standards & Interfaces*, 27 (6), p 561–578.

[8] Farance, F., Tonkel, J. (2001). IEEE P1484.1/D9, 2001-1130 Draft Standard for Learning Technology - *Learning Technology Systems Architecture (LTSA)*, R *p* 1–120, 2001.

[9] Denic, N., Zlatkovic, D. (2017). A Study of the Potentials of the Distance Learning SystemR, IConSE'17, Conference Proceedings, 8 p. 30-39.

[10] El-Khatib, K., Korba, L., Xu, Y., Yee, G. (2003). Privacy and Security in E-learningR, *International Journal of Distance Education Technologies*. 1 (4), p 1-19.

[11] Weippl, E. R. (2005). *Security in e-learning*, New York, Springer, 2005.

[12] Smythe, C. (2005). *IMS Learner Information Package Summary of Changes*, *IMS Global Learning Consortium*.

[13] Smythe, C., Tansey, F., Robson, R. (2001). *IMS learner information package information model specification*, *IMS Global Learning Consortium*, 2001.

[14] eduPerson Object Class Specification (201602)R, Internet2 Middleware Architecture Committee for Education, Directory Working Group, 2016.

[15] Shih, T. K., Hung, J. C. (2007). *Future directions in distance learning and communications technologies*. Hershey, PA: Idea Group Pub.