International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 17 (2025) pp. 746-764

https://doi.org/10.70917/ijcisim-2025-0045
Article

Implementation and Evaluation of A Proposed Framework for Auditing Learning Management Systems in An Egyptian University

Mohammed Alsaid Abdelkader *, Sherif A. Mazen, and Iman M. A. Helal

Information Systems Department, Faculty of Computers and Artificial Intelligence, Cairo University, Giza 12613, Egypt; s.mazen@fci-cu.edu.eg (S.A.M.); i.helal@fci-cu.edu.eg (I.M.A.H.)
* Correspondence author: moh_alsaid_fci@yahoo.com

Received date: 7 May 2025; Accepted date: 21 October 2025; Published online: 31 December 2025

Abstract: The COVID-19 pandemic accelerated hybrid education, increasing reliance on learning management systems (LMS). While essential for course delivery, their growing use underscores the need for systematic auditing to ensure quality, security, and institutional trust. This paper presents a streamlined LMS auditing framework covering performance, security, user roles, support, and feedback. Unlike existing models that are fragmented or limited to technical checks, the framework unifies risk analysis, user experience, and policy evaluation, simplifying the process while broadening its scope. Developed through a review of literature, metrics, and policies combined with risk assessment strategies, the framework provides a structured approach to reduce complexity, identify vulnerabilities, and establish effective controls. Its application in a higher education case study demonstrates practical value in assessing LMS performance and informing strategic planning. The contribution presents a concise and adaptable model that enables institutions to safeguard digital assets and enhance hybrid learning environments.

Keywords: learning management system; e-learning; hybrid education; auditing; risk analysis

1. Introduction

As the world rapidly evolves, educational institutions are embracing e-learning as the primary alternative to traditional learning, particularly in the wake of the COVID-19 crisis. The rise in e-learning has become a symbol of opportunity, driven by the swift progress in information technologies. This shift has been fueled by numerous factors, including population growth, urban traffic challenges, the growing importance of time management, the need to meet diverse learning demands in limited physical spaces, the increasing trend of remote work, the pursuit of democratizing education, and the growing accessibility of information. These exciting developments have given rise to innovative learning management systems that play a crucial role in facilitating the e-learning process [1]. The learning management system (LMS) is a software application that helps with the management of digital training content. It can also be defined as the educational platform within institutions that offers an integrated platform to send, collaborate, and share teaching materials among teachers, learners, and the management of institutions [2]. Another definition of LMS is a web-based software platform that provides an interactive online learning environment and automates the administration, organization, delivery, and reporting of educational content and learner outcomes [3], LMS has five components, which are: computer hardware, computer software, human resources, databases, and computer networks.

LMSs can be categorized into two types, which are: proprietary and open source. One of the earliest proprietary LMSs was WebCT, before the name was phased out in favor of Blackboard [4]. The other category is open source, which has been created to enable universities and colleges to readily download

the source code, adapt it to their circumstances, and build their own LMS solutions. A prominent example of an open-source LMS is Moodle [5]. Whether LMS is proprietary or open source, there are some features that each LMS should be able to introduce to satisfy user needs.

The stakeholders include learners, instructors, instructional designers, system administrators, support teams, and the organization, each playing a distinct role within the LMS. It is important to define the responsibilities of each user group. Each stakeholder has specific expectations from the LMS based on their unique needs and objectives. Therefore, the features and capabilities of the LMS should be designed to align with these needs and goals.

- ✓ **Learners** are the most critical group of users within the LMS. Their primary goal is to efficiently access learning content and activities.
- ✓ **Instructors** represent user groups; they specialize in delivering aspects of a course. They upload content, create activities and quizzes, grade submissions, and access the system frequently.
- ✓ **Instructional designers** play a vital role in the LMS in how to maximize the benefits of LMS tools and activities because they are responsible for designing the user experience in the context of learning.
- ✓ **Systems Administrators,** who can be someone in the organization or a designated contact person if a vendor manages the LMS. They play a vital role in the LMS to ensure that the LMS is running, secure, and updated.
- ✓ **LMS / IT Support** can support all types of users in the organization.
- ✓ **The organization** representative can represent the organization's interests and speak on its behalf.

During usage, stakeholders may face several challenges, such as compatibility with old and new mobile devices, lack of ease-of-customization, not necessarily user-friendly, lack of administration features support, limited protection from security attacks, limited reports and analytics, and difficulty in system upgrades. So, there is a need to audit the LMS system to assess the LMS and give recommendations to measure and improve its value for the business. Our motivation for this research is to survey LMS threats and risks, as most educational institutions are moving towards e-learning after the COVID-19 crisis.

The remainder of this paper is organized as follows: Section 0 covers background concepts and the literature research concerned with LMS challenges, risks, and threats. The information systems auditing process will be discussed in Section 0. Then, In Section 0 and Section 0 we assess the most important frameworks and standards to audit LMS, in Section 0 We discuss the roadmap for implementing an LMS, starting from selection to evaluation., Then, Section 0 introduce our proposed framework to audit the LMS. Then, In Section 0 and Section 0 evaluation for our proposed framework. Finally, we conclude our study in the section 0 with an overlook of future work.

2. Background and Literature Review

2.1. Types of LMSs and E-learning Challenges

Many e-learning challenges face e-learning institutions, authors in [6] developed a comprehensive conceptual framework on challenges for e-learning in developing countries, which covered course, individual characteristics, technological, and contextual categories, see Figure 1.

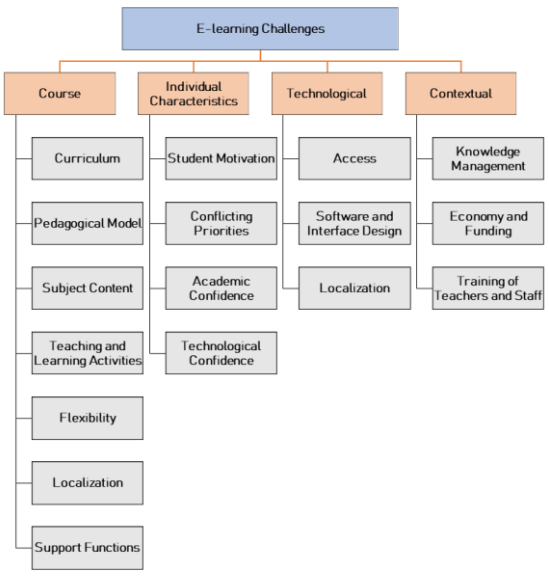

Figure 1. E-learning Challenges framework (reproduced from [6]).

The course category contains a pedagogical model, subject content, curriculum, teaching and learning activities, flexibility, localization, and support functions. The individual characteristics category contains student motivation, conflicting priorities, student economy, academic confidence, and technological confidence. The technological category contains access, cost, software and interface design, and localization. The contextual category contains knowledge management, economy and funding, and training of teachers and staff.

The main disadvantages of this framework are: (1) Educational quality assurance requirements are not well covered in that framework, like ILOs (intended learning outcomes), and course specifications, (2) Lack of learning styles and cultural challenges elements, and (3) Lack of time management element.

2.2. Types of LMS Risks

Although E-learning systems are changing the process of learning, especially concerning the quality of e-education services and support processes, hackers can change or modify the authenticated documents, like course materials, certifications, question banks, lecture materials, and course grades. We can define risk as the probability of a particular threat occurring and the expected loss. In the following part, we will focus on e-risks, how to avoid risks, and how to deal with them.

Authors in [7] identified a list of available risks in e-learning systems. The processes in the implementation phase comprise delivery, support, and feedback. They presented twenty-four risks of e-learning implementation. These risks need inspection for avoidable failure(s). User support is the most critical process when they encounter problems while using e-learning. The help system is highly expected. Support can be translated into documentation and guidance.

Authors in [4] categorized the risks into five main categories which are: (a) Author's risks where the author's lecture notes, home assignments, and class test papers should be hard to modify by hackers or attackers, (b) Teacher's risks where teacher's exams should be protected from cheating, (c) manager's risks where managers should maintain LMS servers and routers passwords, also there are responsible for authorization where the access strategy set (read, write, and execute) privileges are set, (d) system Administrator's risks where the system administrator must be aware of any type of attacks like SQL injections, and cross-site scripting attacks to save the multimedia database and users' passwords and files, and (e) Student's risks; example storing usernames and passwords for users so all students should be aware of misuse of login information to prevent attackers from using their accounts.

2.3. Types of LMS Threats

Several threats can cause denial-of-service for LMS, such as natural disasters: like fire, volcanic eruptions, earthquakes, and floods. Authors in [8] Introduced other types of threats and risks that may affect the learning management systems like (a) disruption of information security which can appear in various forms, such as viruses, spyware, (b) Denial of Service, (c) Illegitimate use, (d) Malicious program, (e) Repudiation, (f) Masquerade, (g) Traffic analysis, and (h) Brute-force attack.

2.4. Standards and Specifications

Although LMS solved the issue of delivering multiple content types, it needs to standardize the requirements for online learning content. Two standards were developed: (1) SCORM, which stands for Sharable Content Object Reference Model, is a set of technical standards for eLearning software products. It tells programmers how to write their code so that it can "play well" with other e-learning software, and (2) xAPI, which is an e-learning specification that allows one to collect data about the wide range of experiences a person has, whether via online or offline training.

2.5. Critical Success Factors for LMS Adoption

Authors in [9] grouped the critical success factors (CSFs) of any LMS implementation into three main categories:

- **Technology Factors**: Foundational drivers like LMS policy clarity, IT infrastructure, equipment availability, system integration, and reliable information flow.
- **Human Factors**: Professional development, IT literacy, training for staff and students, and overall competence in using LMS tools.
- **Organizational Factors**: Leadership support, strategic alignment, resource allocation, and institutional encouragement of LMS usage.

They emphasize that successful LMS adoption requires more than technology—it demands strategic investment and institutional commitment. Clear, well-defined policies are essential to guide LMS use, security, and pedagogy. Equally important is investing in robust infrastructure and ensuring continuous staff training. Most critically, strong leadership engagement is the cornerstone of driving adoption, aligning goals, and fostering a culture of excellence in digital learning.

2.6. Bridging CSFs with LMS Challenges, Risks, and Auditing

By aligning critical success factors (CSFs) with LMS risks and challenges, institutions can create more effective and strategic auditing frameworks. These audits go beyond technical performance—they ensure alignment with key success areas like training, leadership support, infrastructure, and security. Embedding risk management and threat mitigation into LMS policies strengthens compliance, boosts quality assurance, and drives sustainable e-learning success.

3. Information Systems Auditing

Information Systems (IS) auditing is a set of procedures that evaluate management controls within an organization's IT infrastructure and business applications. Its main goals are to protect assets, ensure data integrity, support organizational objectives, and enhance operational efficiency. Conducted by individuals outside of daily operations, IS auditing serves as both a preventive and detective measure against asset mishandling. IS audits assess information systems and provide recommendations for improvement, necessitating auditors to be knowledgeable in network security, operating systems, databases, and information security. Authors in [10] defined an IS audit as examining management controls within an information technology infrastructure.

An IS auditor assesses the information system and gives recommendations to measure and improve its value to the business, so IS auditors should be familiar with network security, learning management systems, operating systems, databases, web technologies, and information security. Auditors evaluate risks, gather and analyze data, audit business process efficiency, and ensure compliance with regulations. Tools such as Computer-Assisted Audit Techniques (CAAT) and Generalized Audit Software (GAS) can streamline the auditing process, enable the analysis of large data volumes, and automate tasks. CAAT can simplify or automate the data analysis and audit process, analyzing large volumes of electronic data records to achieve audit goals such as fraud detection, information retrieval and analysis, audit reporting, reviewing audit histories, computer-based training, online transactions, and data security [11]. GAS is used as a tool to extract and analyze data from multiple applications, helping auditors automate various audit tasks.

Although IS auditing provides comprehensive principles for ensuring integrity, availability, and security, its direct relevance to learning management systems (LMS) requires contextualization. Traditional IS auditing frameworks such as COBIT, ISO/IEC 27001, and NIST emphasize access control, risk management, compliance, and service continuity. In LMS environments, however, these principles translate into unique challenges: user role hierarchies (students, instructors, managers, and administrators), safeguarding assessment data and learning analytics, ensuring platform availability during peak academic periods, and aligning with institutional policies and educational regulations.

Beyond technical controls, the LMS context also demands attention to practical dimensions that determine institutional adoption and sustainability. From a *cost-effectiveness* perspective, systematic LMS auditing reduces overhead by minimizing downtime, preventing data breaches, and lowering manual monitoring costs. *Scalability* is another key consideration, as audits ensure that LMS platforms can expand to serve growing student populations and hybrid learning models without degrading performance or security. Finally, *policy-related constraints* reinforce the importance of LMS auditing, since institutions must comply with accreditation requirements, national education regulations, and data protection laws (e.g., GDPR, FERPA).

By explicitly mapping IS auditing concepts to LMS-specific risks and embedding cost, scalability, and policy considerations, this paper sharpens the focus of LMS auditing beyond general IT controls. In doing so, it highlights its distinctive role in safeguarding educational quality, institutional trust, and the long-term sustainability of hybrid and digital learning environments.

4. Existing Frameworks and Standards

This paper will discuss two key frameworks in IS/technology auditing: Control Objectives for Information and Related Technology (COBIT) and the ISO standards. Developed by ISACA, COBIT helps organizations ensure the quality and reliability of their information systems. Initially published in 1996 and updated in subsequent years, COBIT 2019 is the current version, designed to be comprehensive and flexible for all enterprises.

COBIT is based on five key governance principles, which are: 1. Meeting stakeholders' needs, 2. Covering the enterprise end-to-end, 3. Applying a single integrated framework, 4. Enabling a holistic approach, 5. Separating governance from management.

Additionally, it identifies seven governance aspects, including policies, processes, and information. The ISO standards address information security management systems (ISMS) and practices, encompassing fourteen domain controls relevant to information security. When auditing Learning Management Systems (LMS), the focus is on the LMS's performance, security, and compliance, to protect the institution's reputation while covering both commercial and open-source systems.

5. The Most Important Frameworks and Standards to Audit LMS

In this section, we illustrate the important frameworks and standards to audit LMS:

ISO 27001 / 27002 The International Organization for Standardization (ISO) produced the ISO 27000 series of standards. ISO 27001 is the specification for an organization's information security management system (ISMS) (I.S.O./I.E. C, 2013), and ISO 27002 is the code of practice for information security controls (ISO, 2013). ISO 27001/ 27002 has fourteen domain controls that cover the general concepts of information security, see Figure 2. ISO 270001 and ISO 270002 give guidelines about how the organization can apply information security standards and practices on how to select, implement, and manage controls side by side with information security risk management.

Figure 2. ISO 27001 / 27002 Framework (adopted from [12]).

ISO 9126: The model was developed by the International Organization for Standardization (ISO) to be used in measuring the quality of software. See Figure 3. This standard consists of six main characteristics that should be found in software:

1. Maintainability (how to modify the software easily?).
2. Efficiency (how efficient is the software?)
3. Portability (measures how to transfer the software to another environment?)
4. Reliability (how is the software dependable?)
5. Functionality (does the system do the required functions?)
6. Usability (Is the system easy to use?)

Figure 3. ISO 9126 Framework (adopted from ISO/IEC. (1999), ISO/IEC 9126 (1999- 2004) "Software Engineering - Product quality". Parts 1-4).

Authors in [13] applied the ISO 9126 model to evaluate an e-learning system, i.e. Blackboard LMS version 6.1. From the educator's point of view. They found that only three characteristics (functionality, reliability, and usability) were easily assessable, and the remaining (maintainability, efficiency, and portability) were difficult to measure except by trained IT professionals. The framework contains some strengths and weaknesses, one of the most important strengths is the ease of application in evaluating such software, especially e-learning systems, but one of the major weaknesses of the framework is the sub-characteristic covers too many different factors like usability, which usability can be classified to simplicity, legibility, use of color, and consistency, The other weakness of the framework is the lack to measuring performance and software controls.

6. Roadmap from Selection to Evaluation

After we introduced the types of LMS, standards and specifications, and the types of LMS stakeholders, we will introduce a roadmap for LMS Implementation from selection to evaluation. This roadmap is divided into three phases: selection, implementation, and evaluation. Table 1 shows the steps in each stage to mention the involved stakeholders and Table 2 shows the steps in each stage with risks and controls to be overcome or mitigated.

Table 1. Selection, Implementation, and Evaluation of Detailed Steps with Stakeholders.

Phases	**Key Elements**	**Involved Stakeholders**
Selection	Market research, stakeholder requirements, hosting and support options, integration and compatibility, reporting features, mobile access, cost–benefit analysis, LMS evaluation, and final selection.	• Organization Team • Management • Organization CIO • Faculty • Students • System Administrator
Implementation	Pilot testing, support and training, course development and migration, timeline and policies, system settings, authentication and integration, and final launch.	• Organization CIO • Faculty • System Administrator • Instructional Designer
Evaluation	Evaluation plan, data collection, and analysis.	• Organization CIO • Faculty • System Administrator • Learners

Phases	Key Elements	Involved Stakeholders
		• IT Support • Instructors • Instructional Designer

Table 2. Selection, Implementation, and Evaluation Steps, Risks, and Controls.

Phases	Key Elements	Risks	Controls
Selection	Market research, hosting & support, stakeholder requirements, integration, reporting, mobile compatibility, cost–benefit analysis, evaluation, final selection	Outdated or insufficient information; incomplete/conflicting requirements; overlooking critical features; poor usability or scalability	Use reputable sources; structured surveys /interviews; clear evaluation criteria; usability and scalability testing; alignment with goals
Implementation	Pilot testing, support & training, course development & migration, project timeline, policies & procedures, system configuration, authentication, final launch	Pilot not representative; tight timeline; configuration errors; data loss; inadequate support/training	Real-world simulation; detailed project planning; best practices in configuration; backups before migration; documentation, training, and awareness programs; compliance with standards and regulations
Evaluation	Evaluation plan, data analysis & monitoring	Lack of effective monitoring; poor alignment with institutional needs	Use performance metrics (usage, completion rates, feedback); apply monitoring tools; gather learner and instructor feedback

Selection phase:

The selection phase begins with market research to identify LMS options, features, and costs, ensuring comparison against organizational requirements. Risks at this stage include outdated or insufficient information, mitigated by relying on reputable sources and diverse options. Next, decisions about hosting, support, and updates must align with IT capacity and institutional goals; risks of overlooking features or misalignment can be reduced by consulting standards and involving stakeholders. Gathering stakeholder requirements (learners, instructors, IT, administrators) through surveys and meetings helps prevent incomplete or conflicting needs. Additional considerations include migration of existing content, integration of publisher materials, and adequacy of reporting and mobile compatibility. A cost–benefit analysis over a 3–5-year period ensures financial sustainability, while structured evaluation criteria help identify the best fit. Vendor selection concludes the process, with usability, support, and scalability testing serving as critical controls against poor adoption.

Implementation phase:

The implementation phase begins with a pilot test of the selected LMS, using a diverse user group to simulate real-world conditions and gather feedback. Training and support plans are essential to ensure adoption, while course creation or migration can proceed in parallel. A detailed project timeline, course migration plan, and updated institutional policies guide the process. System configuration, including backup and recovery settings, security, authentication, and communication tools, must follow best practices to avoid errors. Data migration should be carefully tested with backups in place, and final deployment requires integration with other institutional systems. Key risks—such as inadequate training, poor planning, configuration errors, or data loss—are mitigated through structured project management,

expert involvement, and comprehensive testing.

Evaluation stage:

After the LMS has been implemented and is running, the next framework will be used in the evaluation process.

7. Proposed Framework

Based on CBOIT5 and ISO 27001/27002, we can summarize that the process of LMS auditing must involve at least four steps, which are: 1. Measuring vulnerability of LMS by identifying the vulnerability of each aspect. 2. Identification of sources of threats where most of the threats and risks come from users, so LMS auditors should identify people and roles in the LMS, which may be students/learners, instructors, administrators, programmers, subject matter experts, and technical support users. 3. Identification of high-risk points by identifying the occasions. 4. Checking for LMS abuse.

The proposed framework aims to provide organizations with a comprehensive and systematic approach for auditing Learning Management Systems (LMS). While it emphasizes essential technical and administrative controls, it also integrates Educational Controls to capture the pedagogical dimension of LMS performance. This ensures that evaluation extends beyond system reliability, security, and data integrity to include the effectiveness of teaching, learning, and assessment practices. By linking technological soundness with educational effectiveness, the framework offers a holistic perspective that addresses both institutional requirements and learner-centered outcomes. Its main objective is to establish a robust method for measuring system performance and diagnosing issues that affect LMS security, quality, and usability. The framework is designed as a practical tool for IS auditing teams to guide the testing and examination of LMS operations, covering nine types of controls across six phases: (1) physical controls, (2) software controls, (3) administrative controls, (4) data controls, (5) performance controls, (6) risks and threats controls, (7) educational controls, (8) course controls, and (9) administration controls, see Figure 4.

Authors in [14] prioritized the controls to measure security issues. They started with physical controls, such as connectivity cables and security procedures. The second type of control is software controls, e.g., operating systems and database engine licenses. The third type is administrative controls, e.g., policies and procedures applied in the organization, such as backup policies, authentication, and training documentation. The fourth type is data controls, e.g., data loss prevention and information security policies. The fifth type is performance controls, e.g, the number of concurrent users and CPU, and memory usage. The sixth type is risk and threat controls, e.g., traffic analysis and security controls. The seventh type is educational controls, which are like learner tools and support tools. The eighth type is course controls, which are the features and tools that are used in introducing course content. The ninth type is administration controls, like reporting tools and integration with other systems.

The process of the proposed framework in Figure 4. It is divided into three steps. The first step begins with implementing physical, software, administrative, and data controls to find breaches and violations. These controls detect the breaks and violations to generate reports about the organization's status. The first report will be the input to the fifth phase, where deep testing and investigation will be done to detect the sources of hacks or violations. This phase will end with a more detailed report to be used in the sixth phase, which is related to educational controls. Then we get the final report, which describes the violations, breaks, and shortages in each point in the LMS. Now, we will describe each type of control and its elements:

1. **Physical controls:** safeguard critical assets like servers and network devices against unauthorized access. Risk analysis helps determine required resources, while IS auditors guide security teams in developing protocols, securing data centers, controlling access points, and enforcing environmental safeguards. The framework distinguishes mandatory from optional measures, with a final report documenting protected assets to strengthen organizational security.
2. **Software controls:** The second type of control which is essential for securing the LMS servers starting from using licensed operating systems, licensed database engines, licensed LMS products, update controls, backups for the databases or applications, software configuration, and load balancing, if possible, to directs traffic to the server with the fewest active connections and lowest average response time. Software reports will be generated to list and mention all software status in the organization.
3. **Administrative controls:** They are as follows: Policies, Standards, Procedures, Guides, Laws and Regulations, Instructions, Authorizations, Authentications, Training, Communication, Accountability, Documentation, Security awareness, Backups, Configuration management, and Change management. An administrative report will be drawn up to list and mention all administrative statuses in the organization.

4. **Data controls** are essential for safeguarding sensitive assets, usually classified as confidential, private, sensitive, or proprietary. In LMS environments, a key risk is unauthorized access to course content, which can be reduced through anti-spyware tools, USB and port restrictions, and monitoring data transfers. Preventive steps include managing removable devices, overseeing FTP and memory slots, and keeping security software current. At this stage, the consolidated reports support the next phase—technical controls—focused on detecting threat sources.
5. **Performance controls:** The first process in this step is gathering information about the LMS performance controls like CPU and memory usage, LMS debug messages which show if there are debugs in operations, the number of concurrent users, student satisfaction scores, instructor approval ratings, assessment results, enables statistics, student feedback, theme designer mode, java script caching, activity completion times, and course completion rates.
6. **Risk and threat controls:** The second part of this step is risk and threat controls, like traffic analysis, security controls, malicious programs, denial of service, confidentiality violations, and integrity violations. After this phase, the second report will be introduced to list performance and risk status in LMS. Now, the sixth phase will start, which is called educational controls, which concentrate on educational aspects that will affect LMS performance, and the quality of the services introduced.
7. **Educational Controls:** Like computer literacy, learner tools, Adjusting courses to students with special needs, support tools, Instructional design quality (e.g., alignment of content with learning outcomes, clarity of course structure), Learner engagement (e.g., active participation in forums, use of interactive activities, feedback cycles), Assessment quality (e.g., fairness, feedback timeliness, alignment with objectives), Teaching strategies (e.g., blended learning effectiveness, adaptation of pedagogy to the platform).
8. **Course Controls:** They are Course management features, grading features, career tracking features, student management, content types of support, customized electronic exams, class schedules, course registration, and interaction tools.
9. **Administration Controls:** System notifications, student orientation tutorials, record keeping, reporting tools, and integration with other systems.

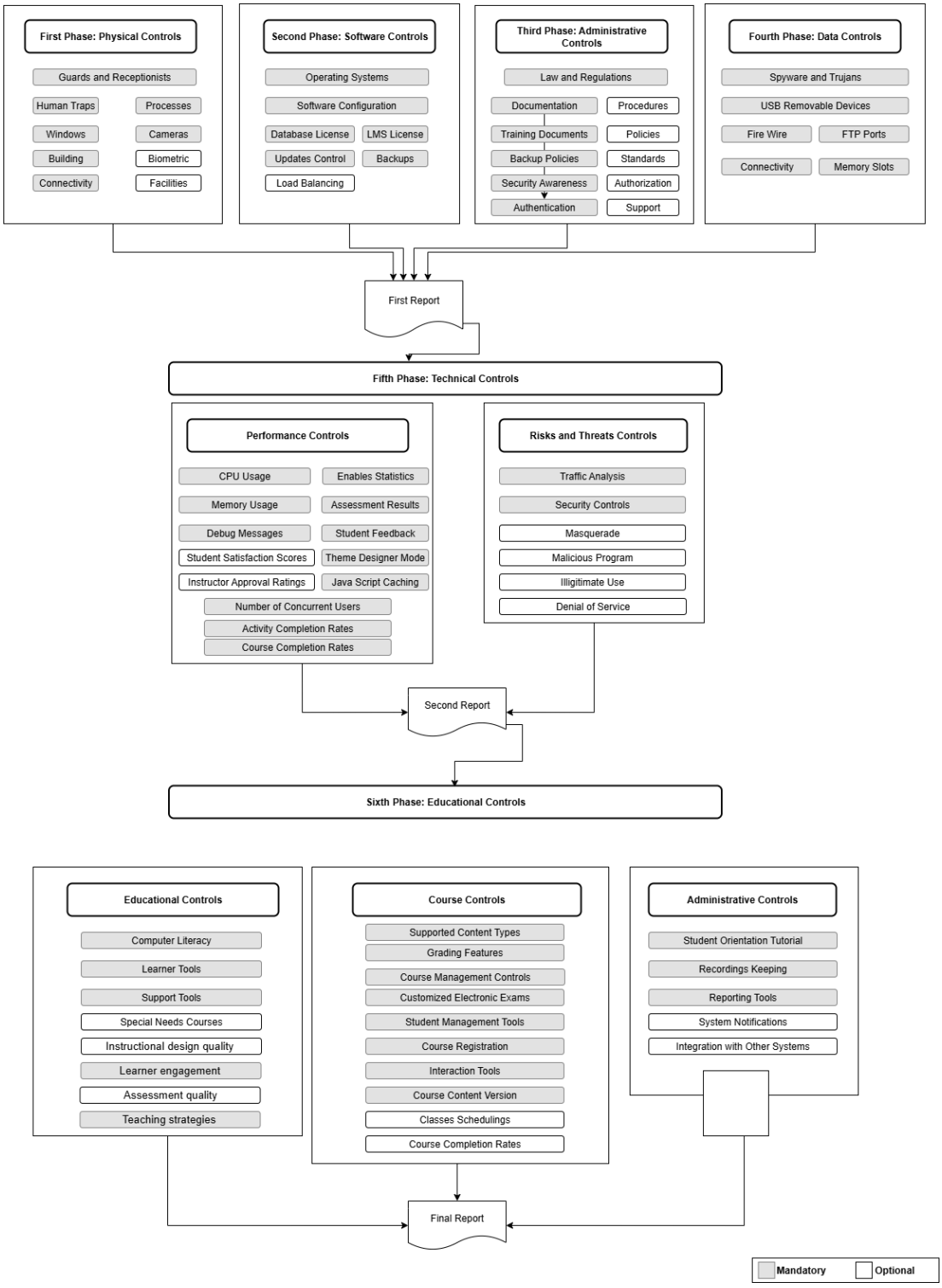

Figure 4. A proposed framework to audit LMS (reused parts from [14]).

8. Proposed Framework Evaluation

The proposed framework is applied to an Egyptian university using LMS in its educational system to evaluate its posture. This university has more than 150 teaching assistants and more than thirty instructors. There were fifty-three participants. 9.43% were systems administrators, 24.54% were instructors, and 66.03% were teaching assistants, see Table 3. All participants' employment types were full-time, Figure 5 shows the level of expertise for participants, where 13% were beginners, 51% had intermediate experience, and 36% were experts.

Table 3. Participants Distribution.

Participants Type	Percentage%
System Administrators	9.43%
Instructors	24.5%
Teaching Assistants	66.03%

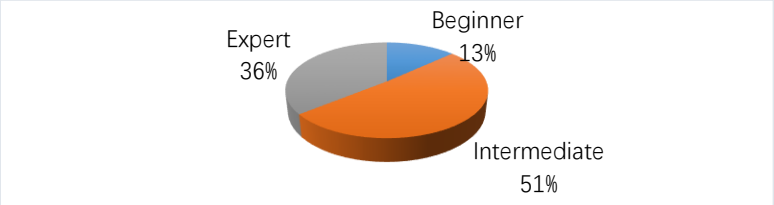

Figure 5. Participants' Level of Experience.

The questionnaire was separated into two questionnaires, the first for systems administrators (see Appendix A) and the second for instructors and teaching assistants (see Appendix B). The first questionnaire consisted of 7 sections of a total of 59 questions: identity questions (5 questions), Physical controls questions (7 questions), Software controls questions (7 questions), Administrative controls questions (12 questions), Data controls questions (6 questions), Performance controls questions (13 questions), Risk and threats control questions (9 questions). The second questionnaire consisted of three sections of a total of 22 questions: educational control questions (5 questions), course control questions (11 questions), and administration control questions (6 questions).

According to the first questionnaire, 80% of participants believe that the LMS server area is well-protected by guards, receptionists, and cameras, though 20% expressed uncertainty about its security. Additionally, 80% felt that the building housing the LMS servers is designed conveniently and securely, while 20% were unsure. Furthermore, 80% reported that all LMS processes are secured and tracked, and the same percentage confirmed secure connectivity in the LMS server area, with 20% uncertain in both cases. All participants acknowledged that the LMS operates on an open-source platform, featuring a Linux operating system, MySQL database engine, and Moodle application. Updates are performed manually, and all participants stated that backups are made daily, 60% per semester, and 20% weekly. Notably, 60% of participants do not use load balancing, while 40% do. Moreover, 80% indicated that a software configuration change policy exists, although 20% were unsure. All processes in the LMS are documented according to 80% of participants, while training on security risks is provided for users and students alike, with 20% disagreeing about student training. While all participants confirmed a backup policy is in place, 80% are aware that full backups are utilized. When asked about introductory security meetings, 60% answered affirmatively.

Regarding authentication methods, 60% use manual processes, and there were mixed responses concerning documentation, with 40% confirming its existence and 20% unsure. Despite this uncertainty, all participants agreed that the security procedures comply with Egyptian laws and regulations. All participants confirmed that the university employs tools to prevent and detect spyware and trojans. However, 60% indicated that USB removable devices are permitted on servers and users' PCs, while 40% disagreed. Regarding FTP port usage, 80% stated it is not allowed, with only 20% saying it is. For firewire usage, 60% reported it is not permitted, while 20% were unsure, and 20% believed it is.

In terms of memory slots, 60% confirmed they are closed, and 80% said there is a secure connectivity channel to LMS servers. All participants reported that the average CPU usage of the LMS server is between 50% and 75%. For memory usage, 25% said it ranges from 25% to 50%, 60% stated 50% to 75%, and 20% reported 75% to 90%. Debug messages are enabled for all participants' LMS, and the average number of concurrent users was reported as follows: 20% from 500-1000, 20% from 1000-1500, 20% from 1500-2000, and 40% over two thousand users.

Regarding theme designer mode, 20% believe it affects performance by 25% to 50%, another 20% said 50% to 75%, 20% claimed 75% to 90%, and 40% indicated an impact of over 90%. Additionally, 20% think JavaScript caching has a negative effect, with estimates varying from a 75% to over 90% decrease in performance. Regarding LMS performance, 20% believe LMS performance can impact course completion rates and student satisfaction scores by 50% to 75%, while 60% think the impact is over 90%. Likewise, 20% feel it may affect instructor approval by less than 25%, while 60% see a significant impact of over 90%. All participants confirmed that the university uses traffic analysis tools. Additionally, 80% reported utilizing security controls to detect threats, while the same percentage noted controls to prevent masquerading. Finally, all participants confirmed the use of security tools to counter various attacks and maintain data integrity.

According to the second questionnaire, c.f. Table 4, there are five conclusions derived. C1 shows that 91% of the participants reported that their university shares computer literacy between users and students, 7% were unsure, and 2% said no. On the other hand, C2 reveals that 34% of the participants agree that interaction between students and instructors can enhance the literacy level, 58% agree, while 8% do not agree. C3 reveals that 96% of participants stated that the learners' tools, like assessment, are used in their LMS, However, only 4% are not sure about it. C4 reveals that 79% of participants reported using support tools like chat in their LMS, while 13% said they did not. Only 8% were unsure. Finally, C5 indicates that 40% of respondents reported introducing special needs courses for students with determination in their LMS, while 17% did not, and 43% were unsure.

Table 4. Derived conclusions from Questionnaire No.2 and participants' results.

#	**Derived Conclusions**	**Yes**	**No**	**Other**
C1	Sharing computer literacy between users and students	91%	2%	7% (Not sure)
C2	Interaction between students and instructors and enhancing the literacy level	58% (Strongly agree) 34% (Agree)	N/A	8% (Neutral)
C3	Learner tools usage	96%	N/A	4% (Not sure)
C4	Support tools usage	79%	13%	8% (Not sure)
C5	LMS Special needs courses introduced	40%	17%	43% (Not sure)

According to Figure 6 quizzes are the most popular content type among 96% of participants who use LMS-supported content types, whereas gamification is the least used. According to Figure 7, 2% of participants believe that LMS only provides manual grading, while 15% use the automatic grading feature, and 83% use both manual and automatic grading features. Notably, 94% of the participants utilize course management controls in their LMS, which shows a strong engagement with the system. We understand that 6% believe the university does not use them, and we appreciate the feedback. Additionally, 98% of participants reported that LMS provides customized electronic exams, while 2% reported that LMS is not used. We need to address and understand these concerns. Furthermore, approximately 70% of participants reported that their LMS can be used for class scheduling, while 30% reported that it cannot. We recognize that these features are essential for efficient course management. On the other hand, we acknowledge that 79% of participants reported that their LMS can measure course completion rates, while 21% reported that it cannot. Finally, we are committed to addressing concerns, as 90% of the participants reported that their LMS had student management tools, while the remaining 10% reported that it did not.

In Figure 8, 54% of participants mentioned that they use the SIS system, which is integrated with the LMS, to enroll in courses or register for them. 16% of the participants reported that LMS allows self-enrollment on a course by end-users, while 24% mentioned that LMS allows staff enrollment into courses. Finally, 6% of participants use bulk enrollment by uploading CSV files. According to Figure 9 Most participants (94%) reported that they utilize e-mail as a social feature in the learning process. Meanwhile, 57% of participants stated that they use announcements, 30% utilize web conferences, 25% utilize instant messaging, 21% employ discussion forums, 8% use blogs, and 4% rely on journals. Finally, 9% of participants mentioned that they use other social learning features.

Based on the course content update, 89% of the participants reported that the university has a policy to check the course content version regularly to ensure it is up to date. Only 11% of the participants reported that there is no such policy. Among those who reported having a policy, 4% stated that the course content is updated every three years, whereas 4% stated that it is updated every five years. 32% of the participants stated that the course content is updated partially, whereas 55% of the participants reported that the update process takes place every year. Only 5% of the participants reported that no updates were made.

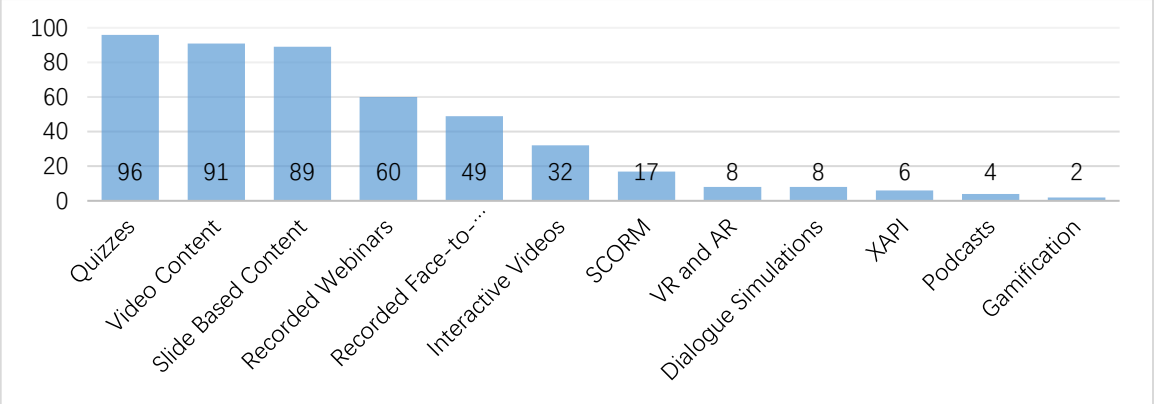

Figure 6. LMS Supported Content Types (%).

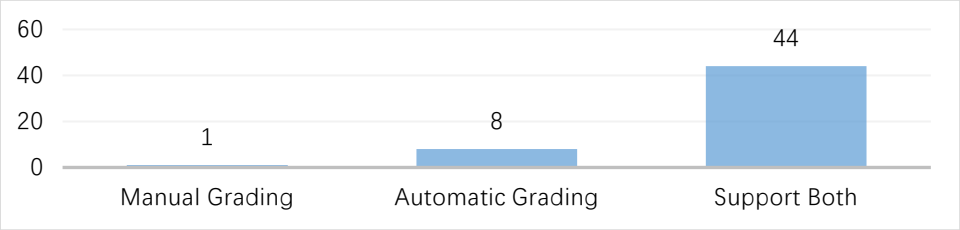

Figure 7. LMS Grading Feature.

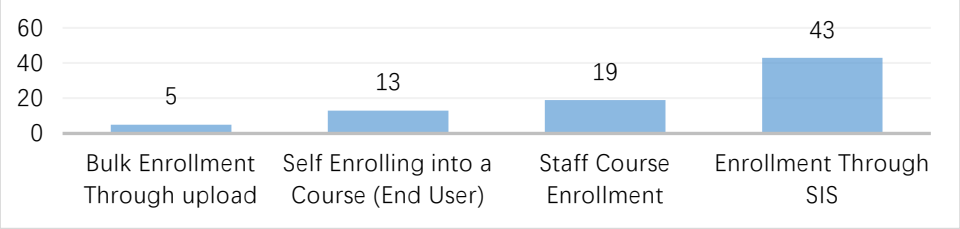

Figure 8. LMS Course Registration Types.

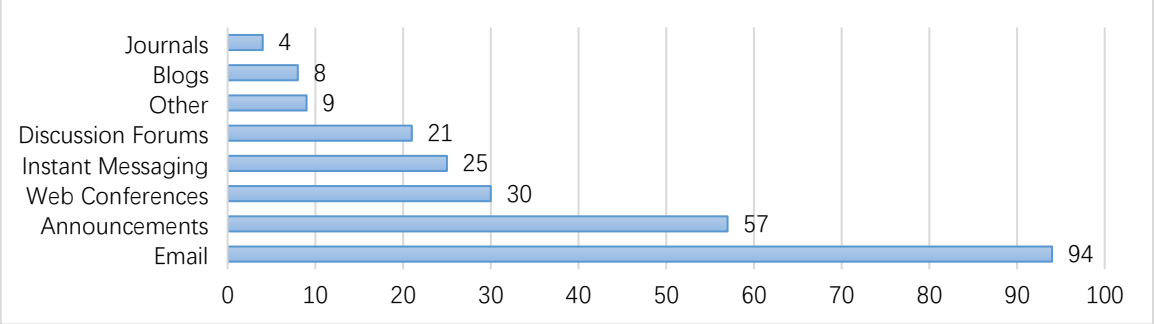

Figure 9. LMS Social Learning Features (%).

According to the questionnaire, 98% of participants confirmed that the university conducts student orientation every year to train them in using the Learning Management System (LMS), while only 2% disagreed. Similarly, 96% of the participants stated that the university keeps recordings, while 4% disagreed. Additionally, 85% of the participants reported that LMS provides reporting tools, while 15% disagreed. Finally, 79% of participants stated that LMS offers custom reporting tools and sends notifications to users when triggers occur, while 21% disagreed.

Based on Figure 10, the questionnaire shows that a large majority of participants (87%) reported that their Learning Management System (LMS) is integrated with the Student Information System (SIS). In addition, 68% of participants stated that their LMS is integrated with the Enterprise Resource Planning (ERP) system, while 43% of participants reported integration with Video Conferencing Tools. Only 13% of participants stated that their LMS is integrated with Customer Relationship Management (CRM) software such as Salesforce, while 8% of participants reported integration with Single Sign-On (SSO) -

Active Directory. Other integrations reported include LinkedIn (6%), Google Analytics (8%), Outlook Calendar (55%), E-payment tools (19%), Google Calendar (4%), Yahoo Calendar (2%), and Other Educational Platforms like McGraw-Hill and Pearson (21%).

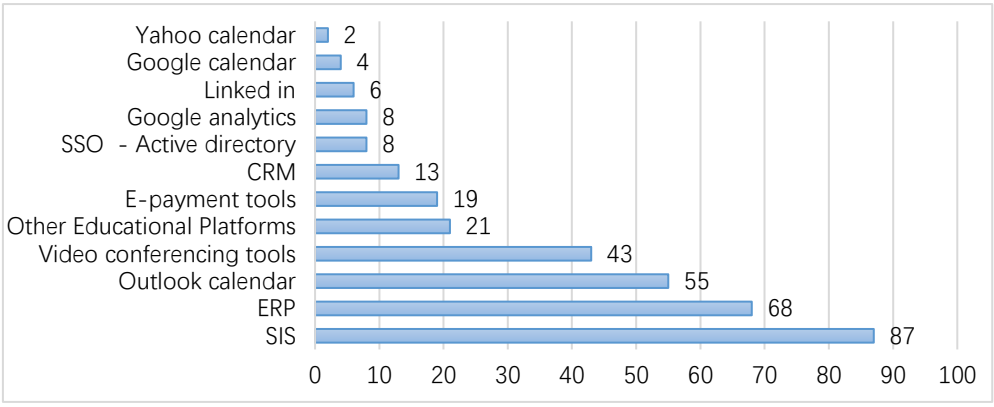

Figure 10. Systems that LMS can integrate with (%) Discussion.

The evaluation of the proposed LMS auditing framework at an Egyptian university provides several insights that both confirm and extend the findings reported in the literature. *First*, the results highlight that most participants perceived the physical and software controls of the LMS to be secure, with daily backups, secure connectivity, and policies in place for configuration changes. These findings align with the technological challenges identified by [6], particularly concerning infrastructure and access. However, our study extends their framework by incorporating explicit quality assurance measures, such as course version updates and orientation programs, which were not emphasized in their original model. By addressing educational quality and time management elements, the proposed framework responds to earlier gaps in the literature. *Second*, the evaluation exposed critical risks and vulnerabilities, such as reliance on manual authentication methods, lack of load balancing in 60% of cases, and the continued use of removable devices. These observations resonate with the risk categories identified by [7] and [4], who emphasized the importance of user support, system security, and protection against attacks such as SQL injection or unauthorized access. Our results not only validate these concerns but also highlight operational weaknesses—such as insufficient scalability and performance impact from theme customization—that extend the risk perspective to include usability and system optimization.

Third, the study confirmed the presence of multiple threats noted in the literature, including those outlined by [8], with institutions adopting tools for spyware prevention, traffic analysis, and masquerade detection. While the university demonstrated strong technical defenses, user practices (e.g., permitting USB devices) introduced vulnerabilities. This underscores the importance of balancing technological safeguards with human and organizational factors, reinforcing the CSFs emphasized by [9].

Fourth, the adoption of educational and course management controls was notably high: 96% reported the use of learner tools, 94% engaged with course management features, and 98% confirmed customized electronic exams. These results support the CSFs highlighted in [9], particularly the human factors of training, IT literacy, and professional development. At the same time, gaps remain in accessibility and inclusivity, as only 40% confirmed the introduction of special needs courses, revealing an area where institutional strategies must evolve.

Fifth, strong evidence of integration with other systems (SIS, ERP, and video conferencing) demonstrates alignment with the technological CSFs of system interoperability and reliable information flow. These integrations enhance institutional efficiency and decision-making, further validating the critical role of leadership and strategic alignment in LMS adoption, as stressed in previous studies.

Overall, the evaluation confirms that while the institution has addressed many of the technological and organizational challenges discussed in the literature, significant gaps persist in scalability, inclusivity, and risk mitigation practices. By bridging CSFs with risks and challenges, the proposed framework offers a more holistic approach than prior models. It not only ensures compliance with standards such as SCORM and xAPI but also embeds auditing as a continuous process that links quality assurance with institutional strategy.

In this way, the study extends existing literature by demonstrating how an auditing framework can operationalize risk management, strengthen institutional resilience, and provide decision-makers with evidence-based guidance for enhancing e-learning quality and sustainability.

9. Practical implications

The proposed LMS auditing framework offers clear practical implications for university decision-makers. By systematically assessing performance, security, user support, and integration, leaders can make informed choices when selecting or upgrading LMS platforms. The framework also highlights risks such as data loss, scalability issues, and inadequate support, enabling proactive measures that reduce operational and reputational threats. In addition, the auditing outcomes provide evidence for resource allocation, guiding investments in infrastructure, training, and technical support. Finally, by aligning LMS quality with institutional goals and accreditation standards, the framework assists decision-makers in enhancing teaching effectiveness, ensuring regulatory compliance, and improving overall student and faculty satisfaction.

10. Conclusion and Future Work

The success of any educational organization is closely tied to the effectiveness of its Learning Management System (LMS). Developing a successful LMS involves multiple stages, including selection, installation, evaluation, and auditing. It is crucial to foster a culture that ensures both learners and instructors are well-acquainted with the features and communication tools of the LMS. A study was conducted with 53 LMS users from various educational institutions in Egypt. The findings revealed that many stakeholders are unaware of the full capabilities of their selected LMS and the specific features most suitable for their organization's needs.

Looking forward, the evolution of auditing frameworks for LMS will focus on enhancing both compliance and effectiveness, ensuring that the learning experiences provided are not only meaningful but also impactful. This will be achieved through the integration of learning analytics, which will improve both compliance and the overall effectiveness of the LMS, better aligning it with user needs. Furthermore, these auditing frameworks will place a strong emphasis on user experience, tracking engagement and ease of use, and will adapt continuously based on user feedback. These advancements aim to create an LMS environment that is secure, efficient, and centered on the needs of its users.

Future developments in LMS auditing frameworks are set to focus on several key areas aimed at enhancing their effectiveness and adaptability. These include:

1. **Enhanced Data Privacy and Security:** In response to increasing concerns about data privacy, our frameworks will incorporate stricter guidelines for data handling, storage, and user consent to ensure compliance with evolving regulations.
2. **AI and Automation:** By harnessing the power of AI, we will automate auditing processes, significantly improving both efficiency and accuracy.
3. **Integration of Learning Analytics:** Learning analytics will be further integrated into the auditing process to enhance decision-making and improve the overall learning experience.
4. **User Experience Focus:** Our auditing frameworks will evolve to include metrics that evaluate user experience and engagement, ensuring that the LMS is not only compliant but also effective, intuitive, and user-friendly.
5. **Continuous Improvement and Feedback Loops:** Rather than being a one-time evaluation, future auditing will be a continuous process that incorporates ongoing user feedback, allowing for adaptive improvements based on this valuable input.
6. **Adaptability to Emerging Technologies:** As new technologies continue to emerge, our auditing frameworks will adapt to incorporate innovative learning modalities, such as VR/AR, and new pedagogical approaches.
7. **Sustainability Metrics:** Our future frameworks will include assessments of the environmental impact of LMS solutions, encouraging greener practices in line with the go-green initiative in Egypt.

These advancements will create a more secure, efficient, and user-centered LMS environment, aligning with the latest technological trends and sustainability initiatives.

Author Contributions

Conceptualization, Mohammed Alsaid Abdelkader, Sherif A. Mazen and Iman M. A. Helal; methodology, Mohammed Alsaid Abdelkader, Sherif A. Mazen and Iman M. A. Helal; software, Mohammed Alsaid Abdelkader; validation, Mohammed Alsaid Abdelkader, Sherif A. Mazen and Iman M. A. Helal; formal analysis, Mohammed Alsaid Abdelkader and Iman M. A. Helal; investigation, Mohammed Alsaid Abdelkader; resources, Mohammed Alsaid Abdelkader; data curation, Mohammed Alsaid Abdelkader; writing—original draft preparation, Mohammed Alsaid Abdelkader; writing—review and editing, Sherif A. Mazen and Iman M. A. Helal; visualization, Mohammed Alsaid Abdelkader and Iman M. A. Helal; supervision, Sherif A. Mazen and Iman M. A. Helal. All authors have read and agreed to the published version of the manuscript.

Funding
This research received no external funding.

Conflict of Interest Statement
The authors declare that they have no competing interests.

Data Availability Statement
The datasets used and/or analyzed are available from the corresponding author upon reasonable request.

Acknowledgments
The author would like to express deep appreciation to the Faculty of Computers and Artificial Intelligence, Cairo University, for their support and encouragement during the development of this research. Special thanks are extended to colleagues and academic supervisors for their constructive comments and valuable feedback that contributed to enhancing the quality of this paper.

List of Abbreviations

Abbreviation	Definition
API	Application Program Interface
COVID	Coronavirus disease of 2019
CPU	Central Processing Unit
FMEA	Failure Mode and Effects Analysis
FTP	File Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ILO	Intended Learning Outcomes
IS	Information Systems
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management Systems
SCORM	Shareable Content Object Reference Model
SSO	Single sign-on
VR	Virtual Reality
XAPI	Experience Application Programming Interface

Appendix A: LMS Administrators' Questionnaire

The following questionnaire was designed to collect information from LMS system administrators regarding security, performance, documentation, and organizational practices. The questions are grouped by category for clarity.

Section A: General Information
A1. Please fill in your name
A2. Job Title
A3. Job Type
A4. Employment Type
A5. Level of Experience

Section B: Physical Security of LMS Servers
B1. Is the LMS server's area protected by guards and receptionists?
B2. Is the LMS server's area protected by human traps to prevent unauthorized access?
B3. Is the LMS server's building convenient for safe and quick access/exit?
B4. Does the LMS server's building have well-designed and secure windows?
B5. Does the LMS server's area contain installed cameras for monitoring daily operations?
B6. Is the LMS server connectivity secured from tampering?
B7. Are LMS server processes (from login to implementation) secured and tracked?

Section C: LMS Software, Servers, and Policies
C1. LMS server operating system type (Please mention it).
C2. LMS server database system type (Please mention it).
C3. LMS application software type (Please mention it).
C4. LMS update policy type.
C5. LMS backup policy type.
C6. Does the LMS use load balancing for network/application traffic?
C7. Is there a policy for LMS software configuration changes?

Section D: Documentation, Training, and Security Policies
D1. Are processes and operations in your LMS documented?
D2. Are LMS users trained by special courses on risks and security measures?
D3. Are LMS learners trained by courses on risks and security measures?
D4. Does the organization have a backup policy?
D5. Which type of backup is used in your organization?
D6. Does the organization organize security awareness meetings?
D7. Which authentication method is used in your LMS?
D8. Is there any procedure documentation used in your LMS?
D9. Is there any policy documentation used in your LMS?
D10. Is there any standard documentation used in your LMS?
D11. Is there any authorization documentation used in your LMS?
D12. Are the security procedures aligned with Egyptian laws and regulations?

Section E: Organizational ICT Policies
E1. Does your organization use tools to prevent and detect spyware and trojans?
E2. Does your organization allow the use of USB removable devices in servers and users' PCs?
E3. Does your organization allow the use of FTP ports in servers and users' PCs?
E4. Does your organization allow the use of FireWire in servers and PCs?
E5. Does your organization open memory slots for server expansion?
E6. Does your organization secure connectivity channels to LMS servers?

Section F: LMS Performance and Usage
F1. Average CPU usage in LMS servers.
F2. Average memory usage in LMS servers.
F3. Are debug messages enabled in your LMS?
F4. Average number of concurrent users in LMS.
F5. Are statistics enabled in LMS?
F6. Assessment participation percentage in LMS.
F7. To what extent is student feedback impacted by LMS performance?
F8. To what extent does enabling theme designer mode affect LMS performance?
F9. To what extent does JavaScript caching affect LMS performance?
F10. To what extent are activity completion times affected by LMS performance?
F11. To what extent are course completion rates affected by LMS performance?
F12. To what extent are student satisfaction scores affected by LMS performance?
F13. To what extent are instructor approval ratings affected by LMS performance?

Section G: Security Tools and Threat Prevention
G1. Does your organization use traffic analysis tools?
G2. Does your organization use security controls to detect risks and threats?
G3. Does your organization use security tools to prevent masquerading?
G4. Does your organization use tools to prevent malicious programs?
G5. Does your organization use tools to prevent illegitimate use?
G6. Does your organization use tools to prevent denial-of-service attacks?
G7. Does your organization use tools to prevent confidentiality violations?
G8. Does your organization use tools to prevent brute force attacks?
G9. Does your organization use tools to prevent integrity violations?

Section H: Literacy, Accessibility, and Support Tools
H1. Does your organization promote computer literacy among users and students?

H2. To what extent does interaction between students and instructors enhance literacy?
H3. Does your organization use learner tools such as assessments?
H4. Does your organization use support tools such as chat?
H5. Does your organization introduce special needs courses for students with determination?

Section I: Content, Exams, and Course Management
I1. Supported content types in your LMS.
I2. Does your LMS provide manual and automatic grading features?
I3. Does your organization use course management controls?
I4. Does your LMS provide customized electronic exams?
I5. Can your LMS be used for class scheduling?
I6. Can your LMS measure course completion rates?
I7. Does your LMS have student management tools?
I8. Which type of course registration is used in your LMS?
I9. Which LMS communication/social learning features/modules are activated?
I10. Does your organization set a policy to check the course content version?
I11. Rate of updating your organization's electronic content (E-courses).

Section J: Orientation, Reporting, and Integration
J1. Does your organization prepare orientation tutorials for inexperienced users?
J2. Does your organization keep recordings?
J3. Does your LMS provide reporting tools?
J4. Does your LMS provide custom reporting tools?
J5. Does your LMS send notifications to users when triggers occur?
J6. Which systems are your LMS integrated with? (Please mention).
Other tools: Please mention whether there are additional tools used.

Appendix B—User Questionnaire

This appendix presents the questionnaire distributed to LMS users (instructors and teaching assistants) to collect research data.

Section A: General Information
A1. Please fill in your name
A2. Job Title
A3. Job Type
A4. Employment Type
A5. Level of Experience

Section B: Literacy and Learning Tools
B1. Does your organization share computer literacy between users and students?
B2. To what extent can the interaction between students and instructors help to enhance the literacy level?
B3. Does your organization use learner tools like assessments?
B4. Does your organization use support tools like chat?
B5. Does your organization introduce special needs courses for students with determination?

Section C: LMS Features
C1. What are the supported content types in your LMS?
C2. Does your LMS provide both manual and automatic grading features?
C3. Does your organization use course management controls?
C4. Does your organization's LMS provide customized electronic exams?
C5. Can your organization's LMS be used in class scheduling?
C6. Can your organization's LMS measure course completion rates?
C7. Does your organization's LMS have student management tools?
C8. Which type of course registration LMS use?
C9. Which LMS communication/social learning features/modules are activated in your organization?
C10. Does your organization set a policy to check the course content version?

C11. What is the rate of updating your organization's electronic content to keep pace with modern science?

_____

Section D: LMS Support and Reporting

D1. Does your organization prepare student orientation tutorials to be used by inexperienced users?

D2. Does your organization keep recordings?

D3. Does your LMS provide reporting tools?

D4. Does your LMS provide custom report tools?

D5. Does your LMS send notifications to users when triggers occur?

D6. What systems with which your LMS are integrated with?

In case of others, please mention it/them:

References

1. Ülker, D., & Yılmaz, Y. (2016). Learning Management Systems and Comparison of Open Source Learning Management Systems and Proprietary Learning Management Systems. *Journal of Systems Integration*, 18–24. https://doi.org/10.20470/jsi.v7i2.255
2. Rahrouh, M., Taleb, N., & Mohamed, E. A. (2018). Evaluating the usefulness of e-learning management system delivery in higher education. *International Journal of Economics and Business Research*, *16*(2), 162. https://doi.org/10.1504/ijebr.2018.10014170
3. Turnbull, D., Chugh, R., & Luck, J. (2019). *Learning Management Systems: An Overview*. *August*, 0–7. https://doi.org/10.1007/978-3-319-60013-0
4. Subramanian, P., Zainuddin, N., Alatawi, S., Javabdeh, T., & and Hussin, A. (2014). A study of Comparison between Moodle and Blackboard based on Case Studies for better LMS. *Journal of Information Systems Research and Innovation.*, *3–4*, 26–32. https://doi.org/10.1093/oxfordjournals.rpd.a032099
5. Turnbull, D., Chugh, R., & Luck, J. (2020). Encyclopedia of Education and Information Technologies. *Encyclopedia of Education and Information Technologies*, *August*, 0–7. https://doi.org/10.1007/978-3-319-60013-0
6. Andersson, A., & Grönlund, Å. (2009a). A Conceptual Framework for E-Learning in Developing Countries: A Critical Review of Research Challenges. *The Electronic Journal of Information Systems in Developing Countries*, *38*(1), 1–16. https://doi.org/10.1002/j.1681-4835.2009.tb00271.x
7. Muqtadiroh, F. A., Wahyu, E., Darmaningrat, T., & Savira, R. N. (2017). *Risk Assessment and Risk Mitigation of E-Learning Implementation in The Middle School using Failure Modes and Effects Analysis (FMEA)*. 18–19.
8. Sadikin, M., Purnomo, R., Sari, R., Ariswanto, D. A. N., Wijaya, J., & Vintari, L. (2023). Information Security on Learning Management System Platform from the Perspective of the User during the COVID-19 Pandemic. *Journal of Information and Communication Convergence Engineering*, *21*(1), 32–44. https://doi.org/10.56977/jicce.2023.21.1.32
9. Alduraywish, Y., Patsavellas, J., & Salonitis, K. (2022). Critical success factors for improving learning management systems diffusion in KSA HEIs: An ISM approach. *Education and Information Technologies*, *27*(1), 1105–1131. https://doi.org/10.1007/s10639-021-10621-0
10. Mustapha, M., & Jin Lai, S. (2017). Information Technology in Audit Processes: An Empirical Evidence from Malaysian Audit Firms. *International Review of Management and Marketing*, *7*(2), 53. http:www.econjournals.com
11. Nasrah, H., Muda, I., & Kesuma, S. A. (2023). Computer Assisted Audit Tools and Techniques Adoption: A Systematic Literature Review. *International Journal of Social Service and Research*, *3*(3), 630–638. https://doi.org/10.46799/ijssr.v3i3.301
12. Wilson, L., & Lemieux, R. (2016). A Controls Factory Approach Too Designing, Building and Managing a Cyber Security Program Based on the NIST Cybersecurity Framework (NCSF). October, 1–14.
13. Chua, B. B., & Dyson, L. E. (2004). *Applying the ISO 9126 model to the evaluation of an e- learning system*. 184–190.
14. Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. *Information Security Journal*, *30*(4), 189–204. https://doi.org/10.1080/19393555.2020.1834649