Security Risk Assessment in Conducting Online Exam

[1st] Danah AlDossary, [2nd] Danah AlQuaamiz, [3rd] Fai AlSadlan, [4th] Dana AlSharari,
[5th] Lujain AlOthman, [6th] Raghad AlThukair, [7th] Ezaz Aldahasi

[1,2,3,4,5,6.] Department of Computer Science, College of Computer Science and Information Technology,
Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[7] Computer Science Department, College of Science and Humanities,
Imam Abdulrahman Bin Faisal University, P.O. Box 31961, Jubail, Saudi Arabia

Abstract
This research is conducted to minimize the potential security risks of conducting online exams to an acceptable level as vulnerabilities and threats to this type of exam are presented. This paper provides a general structure for the risk management process and some recommendations for increasing the level of security.

Keywords:
Risk management; Risk identification; Risk; Security; Online exams.

1. Introduction

Electronic learning has become one of the requirements of the desired educational process, not only to keep pace with the current developments at a great speed in educational institutions all over the world, but also because of the real role of e-learning in improving education and its outputs. Electronic creativity is not a coincidence, but rather an inevitable result of scientific foundations and tracking rules, and among the most important of these rules is sharing thought and providing the opportunity to obtain information. The concept of education has changed in recent years, and reliance on information and communication technology has become one of the important pillars from which the concept of modern e-learning stems. The information and communication revolution in change management has become decisive, and it is now possible through the e-learning system to conduct the basic pillar in education (online exam). This process is automated [1].

Although online exam provides many advantages that make them always at the forefront, they face many challenges and risks, including the possibility of losing information due to system failure, electronic exam leakage, and others, which confirms the importance of a strong infrastructure that provides security for electronic exam systems. Computing and network applications are now a component of many institutions, including educational institutions. In fact hazard protection effectiveness is measured by risk management mechanisms [2]. To support an effective risk management process, the risk framework must incorporate management policies and guidelines for conveying new risks and the effectiveness of risk management at all company levels [3]. There are steps in risk assessment, as shown in Fig 1.

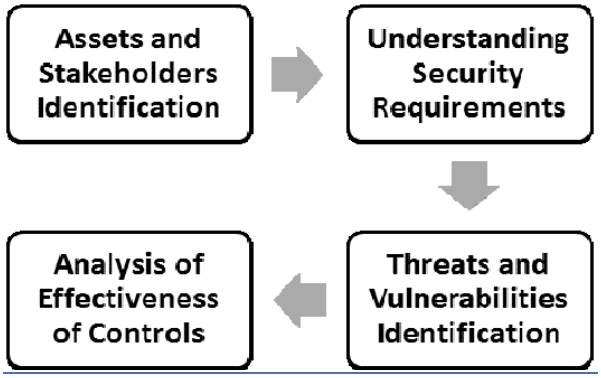

Fig.1 Steps in risk assessment [4]

As the risk management is a systematic approach to control that seeks to identify all organizational hazards before deciding what to do and how to address them.

Therefore, in this paper, we will study risk management in the case of conducting an online exam.

2. RELATED WORK

In [1], the authors presented a method to automatically indicate cheating in unprotected online exams, when someone other than the legitimate student takes the exam. This was during the period when the Covid-19 disease disrupted the fields of education as students' learning and examinations moved to the Internet. The method is based on the analysis of online student traces, which are recorded by distance education systems. The authors also worked with customized IP geolocation and other data to derive a student fraud risk score. Students' cheat risk scores were also compared across four academic semesters including

Manuscript received June 5, 2023
Manuscript revised June 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.6.9

two semesters of university closures due to COVID-19. What the researchers have done in this paper confirms that online exams are exposed to many risks that must be dealt with and prepared to face.

In [5], the techniques for quantitative information security risk evaluation and management in the university telecommunication networks have been taken into consideration by the writers. For the evaluation of risk factors, the authors used fuzzy logic, surveys, analytic hierarchy method, and fuzzy prediction rules. According to the findings, virus infection for hosts is the first significant risk in higher education, and phishing is the second. The writers then offered several remedies, such investing in a reliable antivirus program. The authors provided findings that can be applied to the control of information security risk in the telecommunication network. A study found that academic websites and activities carry complex dangers.

The authors in [6] presented an analysis of the security challenges in the electronic exam system and presented a proposal for a solution using attack and defense tree methods. The attack tree diagram was determined by risk assessment methods. The attack tree was evaluated through penetration exam experiments on a server running the cyber testing application. This contribution can be used as a guideline for planning similar electronic exam systems.

3. Electronic exam security

When conducting an online exam, preparation is essential to plan out the details of your exam, including the number and type of questions, how long it should take students to complete, etc. The organization or the company must implement security measures such as passwords and two-factor authentication to ensure that student data is protected, and that no unauthorized interference occurs during the exam. Additionally, a reliable technical infrastructure needs to be set up so that many users can access it simultaneously without crashing or slowing down significantly.

The results of conducting an online exam can vary depending on the type and purpose of the test, but generally, there are a few key benefits. One is that it allows quicker administration and grading processes since the system can store data electronically; this reduces human error or mistakes due to manual inputting/calculations. Additionally, online exams tend to have fewer distractions than in-person exams, as students can focus more quickly on their environment. Finally, many students prefer taking tests online as it provides them with more flexibility and autonomy when scheduling their examinations.

Conducting an online exam can come with a few potential risks. Some of these include:

1. Security risks - Inadequate security measures can lead to unauthorized access or cheating attempts during the test, which could invalidate results or jeopardize student data.
2. Technical failures - If your infrastructure is not set up correctly for large-scale usage, there may be difficulties with accessing the exam, crashing/slowing down of the system during peak times, etc., which could lead to delays in administering and receiving results from the test.
3. Unreliable responses - If students are unfamiliar with taking exams via computer or need an adequate understanding of how to interact with digital platforms, this could affect their answers to questions and overall satisfaction levels when taking the exam.

For management to successfully conduct an online exam, there are a few key actions that need to be taken:

1. Establish clear goals and objectives for the exam, so everyone is on the same page regarding expectations and desired outcomes.
2. Ensure security measures such as passwords and two-factor authentication have been implemented to prevent unauthorized access or cheating attempts during the test.
3. Develop a reliable technical infrastructure so many users can access it simultaneously without crashing or slowing down significantly.
4. Consider logistical preparation (e.g., printing out hard copies for those needing access) before administering the test, if necessary.
5. Monitor student responses during and after the administration of the test to evaluate any issues with accuracy or discrepancies arising from answers given by students on questions posed during the exam.

3.1 Identification Assets

In the assets identification step, every threat to the organization, regardless of the likelihood that it will materialize should be identified [7]. The owner must ensure that a thorough risk assessment is conducted, that it is identified early, and that enough measures are made to reduce the risk and effectively manage it. Risk identification must be a constant process. Identification assets includes elements such as people, procedures, data and information, hardware, software, and networking.

1- Software Assets

Software assets are an important component of conducting online exams as they provide the necessary tools and technology for the successful delivery and management of the exam.

Databases: database store essential information related to the exams, such as question banks and student answers.

They help ensure that each exam is administered correctly and securely while providing a convenient way of accessing data related to the exam.

Online examination platform is the software used to create and administer the exam, such as blackboard and other programs or applications needed to conduct the exam. An online examination platform can help streamline the process of administering exams while also providing additional security measures like authentication and access control.

Operating system (OS): The operating system controls many of the essential functions of a computer and provides an interface for users to interact with it. This helps protect against man-in-the-middle attacks and ensures that data is secure during exam administration.

Grade Books: These are tools used to keep track of exam scores and other information related to the exam. They should be easy to use and provide meaningful data analysis.

Analytics Tools: These are tools used to analyze the data collected from the exams, including student performance and exam results. They should provide meaningful and actionable insights.

2- Hardware Assets

Hardware assets when conducting online exams refer to the physical devices and equipment used to take the exam.

Computers or laptops: These are the primary devices used by the examinees to take the exam. They must have the necessary hardware specifications and software requirements to access the exam platform and run the required software.

Webcams: In some cases, webcams may be required to monitor the examinee during the exam to ensure integrity.

Microphones: Microphones may be required for voice-based exams or for audio recordings during the exam.

Backup devices: Backup devices, such as external hard drives or cloud storage, are important to ensure that the exam data is securely stored and can be retrieved in case of any technical issues.

3- Data Assets

Encryption: Secure Socket Layer/Transport Layer Security (SSL/TLS) protocol is employed to encrypt the data stream between the webserver and the browser.

Exam session logs: This data includes details about the date and time of the exam, the duration, and any other relevant information about the exam session.

Exam results: This data contains the scores and grades for each exam taker and is used to determine their performance and eligibility for certifications or qualifications.

Exam session logs: This data includes details about the date and time of the exam, the duration, and any other relevant information about the exam session.

Intrusion detection: intrusion detection is a data asset. It might be a system or process that monitors and detects malicious activities or unauthorized access to a network. It can identify suspicious behavior from user accounts, and alert administrators in the event of any potential security breaches.

Authentication methods: authentication methods to access this data should be evaluated for security measures (such as two-factor authentication).

4- Communication Lines and Networks

Communication lines and networks assets refer to the infrastructure and hardware required for the communication and delivery of online exams.

Internet Connectivity: A high-speed and reliable internet connection is critical to ensure that exams can be taken and submitted without interruption.

All network infrastructure: (such as server, routers, switches, and firewalls) to ensure that they are correctly configured and secured against unauthorized access.

Access control: aims to protect sensitive information from unauthorized users by limiting the types of activities they can perform and ensuring that only authorized users can gain access.

Communication Lines: Communication lines, such as Ethernet or Wi-Fi, are used to connect the different components of the network and allow data to flow between them.

3.2 Threat Statement

Malware: in the context of online exams, malware can be used to gain unauthorized access to exam systems and steal confidential information such as test questions or answers. Malware can also be used to disrupt tests by crashing servers or manipulating time limits, granting an unfair advantage to the perpetrators.

Social engineering: it can be used in various ways, such as stealing answers or manipulating results. Attackers may use phishing tactics to target unsuspecting victims; they might create fake accounts posing as legitimate students to obtain privileged access during the exam. Attackers may also use social engineering techniques such as phishing emails or SMS messages which contain malicious links that lead unsuspecting users into revealing sensitive information. They could impersonate exam proctors or other authority figures in order to gain control over the exam process, or they might threaten or blackmail individuals into taking specific actions during an online test.

Unencrypted data: it presents a significant security risk when conducting online exams. Malicious actors can access unencrypted data and manipulate it, exposing the exam takers to potential identity theft or other forms of fraud. Also, they may intercept the data and quickly gain access to sensitive information such as exam answers, grades, or other confidential information related to the exam.

Data leakage: it can occur when confidential exam materials are leaked to unauthorized individuals or groups, either accidentally or maliciously. Some common causes of data leakage include lax security protocols, system vulnerabilities, user error, and intentional attacks.

Third-party services: Those services provide a secure platform where tests and exams can be administered, monitored, and graded accurately and efficiently. They offer a range of features such as automated grading systems, real-time reporting tools, detailed analytics, and content management capabilities to quickly create assessments from existing materials or scratch questions/tests on the fly. With additional security measures such as automated proctoring solutions, third-party services make it easy to conduct safe and successful online exams with minimal effort.

3.3 Vulnerability Statement

Unsecured Network Communication

Unsecured communication channels can allow attackers to intercept sensitive information such as exam answers and personal details.

Technical Errors

Technical errors such as server crashes or connectivity issues can also pose a threat to online exams. If a student's exam is disrupted due to technical issues, it can result in a loss of data or a delay in the exam process.

Unsecured Devices

If students are using unsecured devices to take the online exam, it increases the risk of data theft or hacking. This is because these devices may not have up-to-date security software installed, leaving them vulnerable to cyber-attacks.

Insider threats

Employees or contractors with access to sensitive information can cause damage through carelessness, negligence, or malicious intent.

Sensitive data exposure

An online exam platform collects personal information from students such as their names, addresses, and Social Security numbers in order to identify them. However, the platform does not have proper security measures in place, such as encryption and secure servers. As a result, if the platform is hacked, the personal information of the students could be exposed and vulnerable to theft or misuse.

Vulnerabilities in the source code

Source code that doesn't properly validate user inputs can be vulnerable to injection attacks, where attackers can inject malicious code into the exam application.

Lack of strong encryption

Suppose an online exam platform is using weak encryption to protect sensitive data such as exam questions and answers. An attacker who gains access to the platform's database can easily decipher the encrypted data and obtain the exam content. This can lead to widespread cheating and compromise the validity of the exam results.

3.4 Risk Register

An instrument in risk management and project management is a risk registry. It is used to identify potential risks in a project or organization, occasionally to comply with regulatory requirements, but mostly to keep track of potential problems that could thwart intended goals. A risk register should be used to record the process. Often, the risks are arranged in ascending order of level. The specifics of how the various elements were decided upon, including the justification, justification, and supporting evidence employed, would support this. The purpose of this material is to give senior management the knowledge they need to decide how to handle the identified risks most effectively. It also offers proof that, if necessary, a formal risk assessment procedure was followed, and a record of decisions made together with justifications for those decisions [8]. TABLE I. describes the risk register for our state of conducting an online exam.

4. Discussion

Providing information security and data protection is a critical activity for the current telecommunications networks of different companies like Education. Our study of the educational institution found that the facility does not have anti-virus software on devices. Hence, the activity that needs to be done to increase the institution's security and risk management is to buy a good anti-virus product as it was used in study [5]. As it became clear to us in documentation study in the case of conducting an online exam. Where we highlighted the vulnerabilities and threats that we may face, and as shown in the TABLE I, there are some risks that are classified as high that must be addressed through the enactment of some new policies, conducting some exercises, applying some appropriate encryption algorithms, and using the latest security technologies. It became evident that the foundation needs an expert information technology (IT) team immediately to create backup plans for any emergency. As a detection tool for security violations, an intrusion detection system (IDS) can be used to improve security within the business.

As it became clear to us in calculating the risk of Wi-Fi penetration and unauthorized access to the network. Because the risk value is high, that means the need to increase the network protection by monitoring it. It became clear that the foundation is in urgent need of a specialized Information Technology (IT) team to develop alternative plans for any emergency. An Intrusion Detection System (IDS) can be used to increase security in the organization as a detection mechanism used to detect security violations.
The purpose of this documentation is to give senior management the knowledge they need to decide how to handle the identified risks most effectively. It also offers proof that, if necessary, a formal risk assessment procedure was followed, and a record of decisions made together with justifications for those decisions. After the specifics of any substantial risks are known, management must consider if it needs to take any action. This would consider the organization's risk profile and willingness to accept a particular level of risk, as determined in the process' initial creating the context step. Normally, products with risk ratings below the threshold would be accepted with no additional action necessary.
There are alternatives available to management for treating identified risks that can be used in our study [9].

• Risk transfer: Assigning a third-party responsibility for a risk. This is often accomplished by purchasing insurance to protect against the risk, signing a contract with another company, or employing joint venture or partnership structures to divide expenses and risks if the threat materializes.

• Reduce likelihood: By putting in place appropriate measures to lessen the risk that the vulnerability will be exploited. They could include of administrative or technological measures like implementing firewalls and access tokens, or rules like password complexity and change regulations. By lowering the asset's vulnerability, these measures seek to increase the asset's security by making it more difficult for an attack to be successful.

5. Conclusion and Future work

The purpose of this paper was to evaluate the security risks associated with conducting exams online. The results of the risk assessment indicate that conducting exams online has certain potential risk. Hence, it is necessary to choose potential treatment controls and assess their cost-effectiveness. A variety of management, operational, and technical controls are available and could be applied. Some of them have been listed in this paper for selecting of those that might address the identified threat most effect.

Finally, a recommendation for IT team applies practical tools by examining networks through programs to check networks, discover security vulnerabilities in them, and then match the empirical results with the theoretical results that we reached. Also, the educational institution should have an alternative plan is appropriate for any emergency in the organization, enabling it to control risks or mitigate risks.

TABLE I. Risk Register for the State of Conducting an Online Exam

Item No.	*Observation*	*Threat-Source/ Vulnerability*	*Existing controls*	*Likelihood*	*Impact*	*Risk Rating*	*Recommended controls*
1	Unauthorized access and disclosure of confidential information	Data leakage/Sensitive data exposure	- Restricting access to sensitive systems and data. - Regular security audits. - Encrypting sensitive data, both in storage and in transit.	Possible	Major	High	- Strong Authentication methods ex: Multi factor authentication. - Implementing firewalls.
2	Inability of system to perform primary functions such that system unavailable or slow.	Technical Errors Malware	- Monitoring the system performance and setting up alerts. - Regular Backups.	Almost Certain	Insignificant	Medium	- Disaster Recovery Plan. - Implementing traffic management techniques. - Implementing load balancing techniques can help distribute the load.
3	Malware attacks, which can compromise the privacy of the student's data and exam results.	Unsecured Network Communication/ Malware	- Access Control and Authentication. - Data Backup and Recovery.	Possible	Major	High	- Incident response plan - Antivirus and Anti-malware. - Firewalls.
4	Technical issues such as power outages, internet connectivity problems, and computer crashes can compromise the integrity of online exams.	Technical Errors/ Malware	- Regular Backups. - Regular maintenance and updates.	Likely	Insignificant	Low	- Disaster Recovery Plan. - Implementing traffic management techniques. - Implementing load balancing techniques can help distribute the load.
5	Files of data deleted denying access to users	Vulnerability in the source code/ Malware	- Access Control and Permission Management - Data Backup and Recovery - Encryption of data	Rare	Moderate	Medium	- Strong Authentication methods ex: Multi factor authentication. - Implementing firewalls.
6	Human error for accidently posting students sensitive data.	Insider threats/ Data leakage	- User Education and Awareness. - Implementing monitoring and alerting can help detect and respond to accidental data breaches quickly.	Unlikely	Minor	Low	- Providing privacy screens for users can help prevent sensitive data from being visible to others.
7	Altering or replacing of valid data or	Lack of strong encryption/ Malware	- Implementing version control software can help track changes to data and recover previous versions in case of alteration.	Possible	Moderate	Medium	- Implementing hash-based integrity checking can help detect unauthorized alterations by comparing the current data hash with the original hash.
8	Usage of easily guessed short passwords.	Lack of strong encryption/ Social engineering.	- Implementing a strong password policy. - Educating users about the importance of strong passwords and safe password practices. - Regular Password Changes	Almost Certain	Major	Low	- Two-Factor Authentication (2FA). - Use of Password Hash Functions.

6. References

[1] D. Komosny and S. U. Rehman, "A Method for Cheating Indication in Unproctored On-Line Exams," *Sensors*, vol. 22, no. 2, pp. 1–18, 2022, doi: 10.3390/s22020654.

[2] O. Salah, Ahmad; Moselhi, "Risk identification and assessment for engineering procurement construction management projects using fuzzy set theory," *Can. J. Civ. Eng.*, 2016.

[3] F. D. Culcleasure, "Risk management: A study of current practices at North Carolina's private colleges and universities," *Capella Univ.*, 2005.

[4] B. Almarri, F. Alraheb, S. Alramis, N. Almilad, E. Aldahasi, and A. Ali, "Security Risk Management of an Educational Institution: Case Study," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 3, pp. 172–176, 2021.

[5] I. V. Anikin, "Information security risks assessment in telecommunication network of the university," *IEEE*, pp. 1–4, 2016.

[6] A. Rosmansyah, Yusep and Ritonga, Mora and Hardi, "An Attack-Defense Tree on e-Exam System," *Int. J. Emerg. Technol. Learn.*, vol. 14, pp. 251--260, 2019.

[7] Y. Raanan, "Risk management in higher education: do we need it?," *Risk Manag. High. Educ.*, pp. 1000--1007, 2008.

[8] W. S. & L. Brown, *Computer Security, Principles and Practice*. 2017.

[9] J. Vacca, *Cyber Security and IT Infrastructure Protection*. 2013.