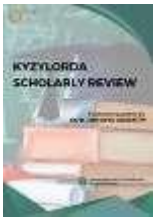
Journal of Kyzylorda Scholarly Review

P-ISSN:3006-0265 | E-ISSN:3007-4681. Published by the Open University of Kyzylorda
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC-BY).
https://bulletin.ouk.kz/index.php/bulletin/index



The Impact of Integration between Artificial Intelligence and Cybersecurity on Enhancing the Reliability of Accounting Information Systems: An Analytical Study of the Opinions of a Sample of Academics at the University of Tikrit

Ayad Dakheel Saleem [*1]
[1]College of Administration and Economics, University of Tikrit
Correspondance: aead54@tu.edu.iq

Article History:
Received: 10th Jan 2026; Revised: 20th Jan 2026; Accepted: 25th Jan 2026; Published: 31th Jan 2026

Abstract: This study aims to analyze and explain the impact of integrating artificial intelligence technologies and cybersecurity on enhancing the reliability of accounting information systems. It is an analytical study of the opinions of a sample of academics at the University of Tikrit. A questionnaire containing questions on the study variables was distributed to the target group, yielding 157 responses, which were statistically analyzed. The study found that integration alone explains 46.2% of the variance in reliability, a proportion higher than that explained by artificial intelligence (41.7%) or cybersecurity (39.1%) individually. The explanatory power increases to 58.4% when all three variables are included together. Academics also perceive the role of artificial intelligence technologies in accelerating accounting data processing and analyzing large volumes of data more strongly than their role in supporting decision-making and detecting financial risks. The study recommends establishing clear, written procedures for responding to cyber incidents and attacks that may affect accounting information systems, communicating these procedures to employees, periodically updating the security systems protecting accounting information systems, and strengthening preventive measures to protect accounting data.

Keywords: Artificial intelligence; cybersecurity; reliability of accounting information systems.

Introduction

In recent years, the world has witnessed rapid developments in information and communication technology, which have directly affected the business environment and accounting activities. Organizations have increasingly relied on electronic accounting information systems to collect, process, and store financial data and prepare the reports required to support administrative and financial decisions. This change has made it more urgent to develop these systems and improve their efficiency and reliability to provide accounting information that is accurate, objective, relevant and timely.

In particular, artificial intelligence technologies have proven themselves to be one of the most significant technologies of the modern era in accounting, as they provide opportunities for analyzing large volumes of information, automating accounting processes, identifying errors and deviations, forecasting financial risks, increasing information processing efficiency, and making decisions.

At the same time, the significance of cybersecurity has grown due to the increasing number of threats that information systems are facing, including electronic intrusion, data theft, manipulation of financial information and unauthorized use of accounting information. The need for appropriate protection of data and systems is a vital part of the business continuity process to ensure the integrity, confidentiality and availability of information.

This points towards the need for the convergence of artificial intelligence technologies and cybersecurity. AI technologies can improve organizations' digital threat detection capabilities, help identify abnormal behavior, and cybersecurity offers the frameworks, policies, and controls that can help organizations safeguard accounting data and maintain integrity. This integration can have a positive effect on the reliability of accounting information systems and their productiveness.

Accordingly, this study seeks to analyze the impact of integrating artificial intelligence technologies and cybersecurity on enhancing the reliability of accounting information systems through an analytical study of the opinions of academics at the University of Tikrit, with the aim of identifying their perceptions of the importance of these technologies and their role in developing the digital accounting environment.

Chapter One: Research Methodology

1. Research Problem

Developments in digital transformation within organizations have prompted the adoption of electronic accounting systems, which need to be more reliable and accurate in the accounting information they provide. The use of artificial intelligence technologies in accounting activities may, however, be accompanied by threats related to data privacy and security, as well as exposure to cyberattacks. This makes integration between the two technologies necessary to enhance the reliability of accounting information systems.

The research problem can be expressed through the following main question:

Does the integration of artificial intelligence technologies and cybersecurity affect the enhancement of the reliability of accounting information systems from the perspective of academics at the University of Tikrit?

A number of subsidiary questions arise from this main question:

1. Is there a statistically significant correlation between the integration of artificial intelligence technologies and cybersecurity and the reliability of accounting information systems?
2. Does the integration of artificial intelligence technologies and cybersecurity have a statistically significant effect on enhancing the reliability of accounting information systems?

2. Research Significance

The significance of this study stems from the importance of its subject, namely the integration of artificial intelligence technologies and cybersecurity and its implications for the reliability of accounting information systems. The significance of the study can be explained through the following two aspects:

First: Scientific Significance

1. Contributing to enriching the accounting literature on applications of artificial intelligence and cybersecurity.
2. Clarifying the theoretical dimensions of the complementary relationship between artificial intelligence and cybersecurity in the digital accounting environment.
3. Providing a scientific framework that clarifies the role of modern technologies in enhancing the reliability of accounting information systems.
4. Clarifying the importance of linking technological development with the requirements of accounting information security.
5. Providing a scientific foundation for future studies addressing digital transformation in accounting.

Second: Practical Significance

1. 1. Identifying the opinions of academics at the University of Tikrit regarding the importance of integrating artificial intelligence and cybersecurity.
2. 2. Providing scientific indicators that may be used to develop accounting information systems.
3. 3. Raising awareness of the importance of protecting financial and accounting data from cyber risks.

4. 4. Demonstrating the capabilities offered by artificial intelligence technologies in detecting accounting errors and risks.
5. 5. Providing recommendations that support academic institutions in adopting modern technologies and developing their digital environments.

1. Research Objectives

The main objective of this study is to analyze the impact of integrating artificial intelligence technologies and cybersecurity on enhancing the reliability of accounting information systems. This objective is pursued through the following sub-objectives:

1. 1. Explaining the concepts of artificial intelligence and cybersecurity and their importance.
2. 2. Analyzing the nature of the relationship between artificial intelligence, cybersecurity, and the reliability of accounting information systems.
3. 3. Measuring the impact of artificial intelligence technologies on enhancing the reliability of accounting information systems.
4. 4. Measuring the impact of cybersecurity on enhancing the reliability of accounting information systems.
5. 5. Measuring the interactive effect of integrating artificial intelligence and cybersecurity on the reliability of accounting information systems.

2. Research Hypotheses

Based on the research problem and objectives, the following hypotheses were formulated:

Main Hypothesis One (H1): There is a statistically significant correlation between the integration of artificial intelligence technologies and cybersecurity and the reliability of accounting information systems.

Main Hypothesis Two (H2): The integration of artificial intelligence technologies and cybersecurity has a statistically significant effect on enhancing the reliability of accounting information systems. The following sub-hypotheses arise from it:

• Sub-hypothesis One (H2a): Artificial intelligence technologies have a statistically significant effect on enhancing the reliability of accounting information systems.

• Sub-hypothesis Two (H2b): Cybersecurity has a statistically significant effect on enhancing the reliability of accounting information systems.

• Sub-hypothesis Three (H2c): Artificial intelligence technologies, cybersecurity, and the integration between them have a statistically significant joint effect on enhancing the reliability of accounting information systems.

3. Hypothesized Research Model

The study adopts a model illustrating the relationship between the independent variables and the dependent variable. The integration of artificial intelligence technologies and cybersecurity represents the main explanatory variable, while the reliability of accounting information systems represents the outcome variable.

4. Research Variables

The study includes four main variables, as follows:

First: First Independent Variable: Artificial Intelligence Technologies

These refer to a set of computer technologies and systems that simulate certain human capabilities in learning, analysis, inference, and decision-making. They contribute to improving the performance of accounting information systems through data processing, error detection, and the provision of decision-support information.

Second: Second Independent Variable: Cybersecurity

This refers to a set of technologies, policies, and procedures used to protect systems, networks, and data from electronic threats and attacks, thereby ensuring the confidentiality, integrity, and availability of information.

Third: Interactive Independent Variable: Integration of Artificial Intelligence and Cybersecurity

This variable is constituted by integrating artificial intelligence technologies and cybersecurity and examining the effect of this integration between these technologies on the dependent variable.

Fourth: Dependent Variable: Reliability of Accounting Information Systems

This refers to the ability of accounting information systems to provide accurate, complete, sound, secure, and timely financial and accounting information, thereby enhancing the possibility of relying on it in decision-making.

5. Research Method

The choice of the study method in the present study was descriptive-analytical method, which is suitable for the problem in this study and the objectives that will be achieved in this study. The descriptive aspect introduces theoretical concepts of artificial intelligence technologies, cyber security and reliability of accounting information systems besides reviewing the theoretical relationships among the variables.

The analytical dimension includes gathering primary data by a questionnaire to be distributed to academics of the University of Tikrit, and analysing the results of the questionnaire by statistical methods, then testing the hypotheses of the research and measuring the nature of the relationship and effects between the research variables.

6. Sources of Data Collection

Two major sources of data were used in the study:

The first: Primary Sources: These are the data that are collected by presenting the questionnaire to the research sample of academicians in the University of Tikrit in order to find their opinions about the study variables and dimensions.

Second: Secondary Sources: These are academic books, university theses and dissertations, research published in peer-reviewed scientific journals, and reports and special studies about the subject.

7. Research Population and Sample

First: Research Population: In the light of the importance of the subject of the research and considering the Colleges and scientific departments related to accounting and administrative and technical scientific disciplines in the University of Tikrit, the research population is composed of academic and teaching staff in these Colleges and scientific departments.

Second: Research Sample: The Research sample consisted of academics randomly selected from among the academics in the University of Tikrit using stratified random sampling to ensure that the sample represents the various disciplines of science existing in the Research population.

8. Research Limitations

The research limitations are as follows:

First: Geographical Limitation: The University of Tikrit.

Second: Human Limitation: Academics and teaching staff at the University of Tikrit.

Third: Time Limitation: The 2026–2027 academic year.

Chapter Two: Theoretical Framework of the Research

First: The Concept of Artificial Intelligence

Artificial intelligence is currently a controversial subject because researchers and specialists have differing views on establishing a precise and specific definition of it since its emergence. Initially, it was defined as a branch of computer science concerned with programming machines to perform tasks requiring a certain level of human intelligence. This field aims to

enable computers and intelligent systems to perform functions that were previously exclusive to humans, such as thinking, learning, and communication. Accordingly, artificial intelligence may be regarded as a virtual system capable of performing complex intellectual tasks that are difficult for humans to perform conventionally (Abuzabiba, et al., 2024: 56).

It has also been defined as the ability of a machine to perform cognitive functions associated with human minds, such as perception, reasoning, learning, interaction with the environment, and problem-solving (Gheetha, 2021: 110).

It has also been defined as a set of multiple technologies that work together to enable machines to sense, learn, understand, and act in ways that augment human capabilities. Artificial intelligence technology can handle enormous volumes of big data, anticipate needs, and make appropriate decisions (Abdel Fattah and Abu Al-Nasr, 2024: 425).

Second: The Importance of Artificial Intelligence

Artificial intelligence is important in many fields, as follows (Koutou, 2018: 26):

1. Improving productivity or efficiency: Artificial intelligence can often complete routine tasks faster, better, or more consistently than humans.
2. Understanding vast amounts of data: We live in a data-rich world, and human brains are not equipped to analyze enormous volumes of structured and unstructured data, make connections, and identify relationships and patterns across datasets.
3. Improving decision-making: Artificial intelligence can use data as inputs to make fact-based decisions that reduce bias and appropriately consider and weigh all the facts.
4. Improving customer experiences: AI-powered conversational interfaces can provide faster and more accurate customer service in multiple languages. Artificial intelligence can also personalize experiences and services and provide individualized services, such as personalized learning.
5. Enabling human-like vision: Artificial intelligence enables computer systems to see, process, and understand visual images, such as photographs and videos.
6. Augmenting human intelligence: Although the capabilities of the human brain are undeniable, there is only so much that can be accomplished within 24 hours.
7. Artificial intelligence can radically enhance people's intelligence.

Third: The Impact of Artificial Intelligence on Accounting Processes

Artificial intelligence, through its various applications and software, affects the accounting profession in the following ways (Zakaria, 2021: 346):

1. Automation of routine tasks: Automating routine accounting tasks through the use of technology improves efficiency and reduces errors, including purchasing, accounts payable, and organizing customers' digital invoices using scanning technology, among other tasks.
2. Data entry: The importance of artificial intelligence in data entry lies in replacing manual methods, with their associated possibility of error, with automated processes that increase the accuracy and efficiency of data entry.
3. Financial reporting: This is reflected in the ease and simplicity of presenting and disclosing financial reports published on the websites of accounting entities. This is attributable to automating report preparation and reducing human errors.
4. Data analysis: Artificial intelligence applications in accounting analyze data obtained from previous operations to identify strengths and weaknesses, evaluate performance, identify trends, and provide explanations for the results reached.
5. Predictive analytics: Artificial intelligence generates forecasts of future financial trends and performance using a combination of mathematical and statistical methods and advanced machine-learning techniques. It can also identify and extrapolate hidden trends.
6. Risk analysis: Artificial intelligence applications and software help detect abnormal patterns in a shorter time than manual processes and provide an assessment and analysis of financial risks.

Fourth: The Concept of Cybersecurity

Cybersecurity has been defined as information security for computer devices and networks,

and as the processes and mechanisms through which computer equipment, information, and services are protected from any unintended or unauthorized interference, alteration, or modification that may occur. A range of technical, organizational, and administrative means are used to prevent unauthorized use and misuse and to recover electronic information and the communications and information systems containing it (Al-Hiyari, 2022: 32).

It has also been defined as a set of technologies, processes, and practices aimed at preventing cyberattacks and unlawful access to the Internet, computers, software, and data (Abbas, 2026: 531).

The US Cybersecurity and Infrastructure Security Agency (CISA) defines it as the art of protecting networks, devices, and data from unauthorized access or criminal use, and as the practice of ensuring the confidentiality, integrity, and availability of information (Kazim, 2025: 2).

Fifth: The Importance of Applying Cybersecurity in Accounting

With the emergence of the digital era, the financial and accounting landscape has been exposed to cyber attacks, and the implementation of cybersecurity in accounting is necessary to safeguard institutions and companies against various risks and challenges. Cybersecurity in accounting is crucial for a number of reasons (Al-Taib and Al-Sayeh, 2025: 198):

1. Sensitive financial data - Accounting systems hold highly sensitive data, including an organization's financial data, customer records, account statements and financial reports. Unauthorized access to this information can result in its theft or alteration, resulting in significant financial damage, loss of a competitive advantage and loss of organizational reputation.
2. Compliance with laws and regulations: There are various international laws and regulations that place a high priority on financial and personal data protection, including the General Data Protection Regulation (GDPR) in the EU and the Sarbanes–Oxley Act (SOX) in the USA. Fines and penalties can be very high for non-compliance with these laws.
3. Fraud prevention: Cybersecurity technologies play a role in fraud detection and prevention, including the detection of fraudulent activities like financial manipulation or the misappropriation of funds.
4. Business continuity: Cyberattacks can cause work stoppage and/or business revenue loss. Cybersecurity plays a crucial role in safeguarding critical systems, thereby maintaining business continuity.
5. Safeguarding company reputation: A breach of security can have detrimental impact on a company's reputation, especially when it comes to leaking of any customer or supplier information. Cybersecurity helps to ensure that customers and investors trust the organization.
6. Risk management: Cybersecurity can help identify, assess, and manage risks related to financial data and accounting systems, which helps to minimize financial losses and reduce the risk of data corruption.

Sixth: The Concept of the Reliability of Accounting Information Systems

Reliability means that information is suitable as a basis on which a decision-maker can rely when making predictions. This characteristic also has three basic elements (Matar, 2012: 333):

1. 1. Verifiability: This means that the correctness of information can be verified. This element is closely related to the problem of accounting measurement and is also strongly associated with the principle of objectivity.
2. 2. Representational faithfulness and fairness: This element is also related to the theory of accounting measurement. It is extremely important as a fundamental criterion governing the preparation of published financial statements, which are of particular concern to auditors.
3. 3. Neutrality: This element is also closely related to the principle of objectivity. It is particularly important in preparing published financial statements, which should present the actual circumstances of the company issuing them rather than a representation designed to satisfy the wishes of a particular group, such as the company's management or shareholders.

Reliability has also been defined as the ability of a product or system to perform a specified function. It may refer to design reliability or operational reliability, which is the system's ability to remain operational, the possibility of determining maintenance requirements in advance, and the ease of repairing or maintaining the product or system (Al-Shami, 2018: 15).

Seventh: The Objective of Reliability in Accounting Information Systems
The aim of reliability is to safeguard the interests or benefits of information, information and communication systems used to provide information to the appropriate parties and information systems which enable the maintenance of the availability, integrity and confidentiality of information. The conditions in achieving the objective of reliability are that the system is configured and only used when necessary, and that data and information are distributed only to those authorized and entitled to access them, and it is protected against unauthorized modification (Al-Hasban 2009: 354).

Chapter Three: Applied Aspect

First: Analytical Methodology and Study Instrument
The data collection used in the study were questionnaires as the main instrument. It was sent electronically to a few academics at the University of Tikrit. A total of 157 questionnaires were returned and the data was free of missing values. The questionnaire had two sections; the first one contained the demographic data of the respondents (7 variables) and the second contained 44 items, which was divided into 4 dimensions with 11 items for each dimension, as presented in Table (1).

Table (1): Questionnaire Structure and Study Variables

Dimension	Variable Type	Items	Number of Items
Artificial Intelligence Technologies	Independent	1 – 11	11
Cybersecurity	Independent	12 – 22	11
Integration of Artificial Intelligence and Cybersecurity	Independent (Interactive)	23 – 33	11
Reliability of Accounting Information Systems	Dependent	34 – 44	11
Total			44

A five-point Likert scale was used, and responses were coded as follows: strongly agree (5), agree (4), neutral (3), disagree (2), and strongly disagree (1). To determine response levels, the class width was calculated as (5 – 1) ÷ 5 = 0.80; accordingly, the criteria for interpreting arithmetic means are presented in Table (2). The hypothetical mean (3) was also adopted as the criterion for testing the significance of the direction of responses.

Table (2): Criteria for Interpreting the Arithmetic Mean

Arithmetic Mean Range	1.00 – 1.80	1.81 – 2.60	2.61 – 3.40	3.41 – 4.20	4.21 – 5.00
Level	Very Low	Low	Moderate	High	Very High

The following statistical methods were used in the analysis: frequencies and percentages;

Cronbach's alpha and split-half reliability coefficients; Pearson's correlation coefficient for internal-consistency validity; skewness and kurtosis coefficients to test normality; the arithmetic mean, standard deviation, coefficient of variation, and relative importance; the one-sample t-test; Pearson's correlation matrix; simple and multiple linear regression; the independent-samples t-test; and one-way analysis of variance (One-Way ANOVA), at a significance level of 0.05.

Second: Description of the Study Sample Characteristics

Table (3) presents the distribution of sample members according to their personal and occupational characteristics.

Table (3): Distribution of Sample Members by Demographic Characteristics

Characteristics	Category	Frequency	Percentage
Gender	Male	137	87.3%
	Female	20	12.7%
Age	Under 30 years	3	1.9%
	30–less than 40 years	51	32.5%
	40–less than 50 years	80	51.0%
	50 years and above	23	14.6%
Educational Qualification	Bachelor's degree (Master's student)	17	10.8%
	Higher diploma	1	0.6%
	Master's degree	71	45.2%
	Doctorate	68	43.3%
Years of Experience	Less than 5 years	15	9.6%
	5–less than 10 years	27	17.2%
	10–less than 15 years	21	13.4%
	15–less than 20 years	53	33.8%
	20 years and above	41	26.1%
Academic Title	None (Master's student)	19	12.1%
	Assistant Lecturer	42	26.8%
	Lecturer	43	27.4%
	Assistant Professor	43	27.4%
	Professor	10	6.4%
Specialization	Business Administration	51	32.5%
	Accounting	42	26.8%
	Economics	29	18.5%
	Banking and Financial Sciences	11	7.0%
	Computer Science	7	4.5%
	Public Administration	4	2.5%
	Marketing	3	1.9%
	Cybersecurity	3	1.9%
	Information Systems	1	0.6%
	Other	6	3.8%
Assigned Duties	Teaching Staff	52	33.1%
	Section Head	41	26.1%
	Teaching and Administrative Staff	30	19.1%

Journal of Kyzylorda Scholarly Review
P-ISSN:3006-0265 | E-ISSN:3007-4681
https://bulletin.ouk.kz/index.php/bulletin/index

	Unit Head	21	13.4%
	Administrator	10	6.4%
	Department Head	3	1.9%
Total		157	100%

Third: Testing the Reliability and Validity of the Study Instrument

1. Reliability (Cronbach's Alpha and Split-Half Method)

Table (4): Reliability and Self-Validity Coefficients for the Questionnaire Dimensions

Dimension	Number of Items	Cronbach's Alpha	Self-Validity (√α)	Assessment
Artificial Intelligence Technologies	11	0.853	0.923	Very Good
Cybersecurity	11	0.920	0.959	Excellent
Integration of Artificial Intelligence and Cybersecurity	11	0.922	0.960	Excellent
Reliability of Accounting Information Systems	11	0.910	0.954	Excellent
Entire Questionnaire	44	0.959	0.979	Excellent

Table (4) reveals that Cronbach's alpha values were found to be between 0.853 and 0.922 for the dimensions and 0.959 for the questionnaire as a whole. The results showed that the values were above the minimum acceptable level (0.70), which means that they were reliable in terms of the instruments. The results showed that the instrument obtained a correlation coefficient of 0.958 between the odd and even items of the questionnaire, and a reliability coefficient of 0.979 after correction using the Spearman–Brown formula, which indicated the questionnaire, was reliable and suitable for use.

2. Internal-Consistency Validity

Pearson's correlation coefficient was calculated between the score of each item and the total score of the dimension to which it belongs, in addition to the corrected correlation (after excluding the item from the dimension total), as shown in Table (5).

Table (5): Correlation Coefficients between Items and the Total Scores of Their Dimensions

Item	r	Corrected r	Item	r	Corrected r	Item	r	Corrected r	Item	r	Corrected r
1	0.622	0.532	12	0.725	0.658	23	0.726	0.662	34	0.702	0.630
2	0.653	0.567	13	0.668	0.604	24	0.644	0.566	35	0.700	0.619
3	0.679	0.593	14	0.678	0.609	25	0.734	0.671	36	0.761	0.701
4	0.666	0.570	15	0.751	0.690	26	0.788	0.736	37	0.711	0.638
5	0.671	0.575	16	0.835	0.788	27	0.717	0.650	38	0.741	0.673
6	0.619	0.540	17	0.810	0.755	28	0.751	0.685	39	0.739	0.679
7	0.697	0.605	18	0.724	0.657	29	0.809	0.758	40	0.750	0.687
8	0.669	0.570	19	0.663	0.598	30	0.781	0.722	41	0.745	0.682
9	0.529	0.404	20	0.793	0.732	31	0.731	0.673	42	0.740	0.677
10	0.665	0.569	21	0.772	0.711	32	0.758	0.698	43	0.712	0.647
11	0.550	0.434	22	0.767	0.713	33	0.795	0.743	44	0.700	0.624

Journal of Kyzylorda Scholarly Review
P-ISSN:3006-0265 | E-ISSN:3007-4681
https://bulletin.ouk.kz/index.php/bulletin/index

Dimensions from right to left: artificial intelligence (1–11), cybersecurity (12–22), integration (23–33), and reliability (34–44). All correlation coefficients are significant at the 0.01 level.

As shown in Table (5), Item-to-Dimension correlation coefficients ranged from 0.529 to 0.835, with the positive values of all of them being statistically significant at 0.01. The corrected correlation coefficients also showed > 0.30 for all items, which revealed good internal consistency among the items and each of the dimensions.

Table (6): Correlations of the Dimensions with the Total Questionnaire Score (Construct Validity)

Dimension	Correlation Coefficient	Significance Level	Decision
Artificial Intelligence Technologies	0.790	0.000	Significant
Cybersecurity	0.848	0.000	Significant
Integration of Artificial Intelligence and Cybersecurity	0.881	0.000	Significant
Reliability of Accounting Information Systems	0.861	0.000	Significant

Table (6) shows that the correlation coefficients between the dimensions and the total score ranged from 0.790 to 0.881, and all were significant at the 0.01 level, confirming the construct validity of the questionnaire.

3. Normality Test

Table (7): Skewness and Kurtosis Coefficients for the Study Dimensions

Dimension	Skewness	Standard Error	Kurtosis	Standard Error	Decision
Artificial Intelligence Technologies	0.011	0.194	-0.050	0.385	Approximately Normal
Cybersecurity	-0.618	0.194	0.860	0.385	Approximately Normal
Integration of Artificial Intelligence and Cybersecurity	-0.590	0.194	1.220	0.385	Approximately Normal
Reliability of Accounting Information Systems	-0.188	0.194	0.204	0.385	Approximately Normal

Table (7) shows that skewness coefficients ranged from −0.618 to 0.011, within the range of ±1, while kurtosis coefficients ranged from −0.050 to 1.220, within the range of ±3. This indicates that the data for the dimensions approximate a normal distribution. Furthermore, the sample size (157) exceeds 30 observations, in accordance with the central limit theorem. Therefore, parametric tests (correlation and regression) can be used to test the hypotheses.

Fourth: Descriptive Analysis of the Study Variables

Journal of Kyzylorda Scholarly Review
P-ISSN:3006-0265 | E-ISSN:3007-4681
https://bulletin.ouk.kz/index.php/bulletin/index

1. Description and Diagnosis of the Artificial Intelligence Technologies Dimension

Table (8): Frequency Distributions, Arithmetic Means, and Standard Deviations of the Items in the Artificial Intelligence Technologies Dimension

NO.	Item	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)	Mean	Standard Deviation	Relative Importance	Level	Rank
1	The organization's use of artificial intelligence technologies helps perform accounting processing.	26.8	60.5	11.5	1.3	0.0	4.127	0.648	82.5%	High	5
2	Artificial intelligence technologies contribute to automating repetitive or routine accounting processing.	31.8	57.3	9.6	1.3	0.0	4.197	0.655	84.0%	High	3
3	Artificial intelligence technologies help detect and reduce accounting errors.	29.9	58.0	9.6	2.5	0.0	4.153	0.690	83.1%	High	4
4	Artificial intelligence technologies contribute to detecting atypical or unusual operations and activities.	26.1	58.0	11.5	4.5	0.0	4.057	0.745	81.2%	High	6
5	Artificial intelligence technologies are used to predict financial information and results.	26.1	56.1	14.0	3.8	0.0	4.045	0.745	80.9%	High	7
6	Artificial intelligence technologies help accelerate the processing of accounting data.	37.6	57.3	5.1	0.0	0.0	4.325	0.569	86.5%	Very High	1
7	Artificial intelligence technologies contribute to detecting financial risks to which the organization may be exposed.	24.2	52.2	20.4	3.2	0.0	3.975	0.759	79.5%	High	10

8	Artificial intelligence technologies help the organization's employees make appropriate accounting decisions.	22.9	54.8	19.1	2.5	0.6	3.968	0.763	79.4%	High	11
9	Applying artificial intelligence reduces human intervention in the organization's accounting data processing.	26.8	49.7	21.0	2.5	0.0	4.006	0.764	80.1%	High	9
10	Artificial intelligence contributes to analyzing large volumes of the organization's accounting data.	40.1	48.4	9.6	1.3	0.6	4.261	0.735	85.2%	Very High	2
11	Artificial intelligence technologies contribute to detecting cyberattacks and threats to accounting information systems.	25.5	55.4	15.9	3.2	0.0	4.032	0.737	80.6%	High	8
	Overall Dimension Indicator						4.104	0.453	82.1%	High	

Table (8) shows that the overall indicator for the artificial intelligence technologies dimension achieved an arithmetic mean of 4.104, higher than the hypothetical mean (3), with a standard deviation of 0.453, a coefficient of variation of 11.04%, and relative importance of 82.1%, representing a high level. The average agreement rate (strongly agree and agree) for the dimension's items was 84.1%. Item (6), stating that "Artificial intelligence technologies help accelerate the processing of accounting data," ranked first, with a mean of 4.325 and a standard deviation of 0.569. Item (8), stating that "Artificial intelligence technologies help employees in the organization make appropriate accounting decisions," ranked last, with a mean of 3.968 and a standard deviation of 0.763. The item means ranged from 3.968 to 4.325. The one-sample t-test confirms that the difference between the dimension's arithmetic mean and the hypothetical mean is statistically significant (t = 30.535, Sig. = 0.000). This indicates that respondents recognize the role of artificial intelligence technologies in accelerating accounting processing and analyzing big data, while their recognition of its role in supporting accounting decisions and detecting financial risks is relatively lower.

Journal of Kyzylorda Scholarly Review
P-ISSN:3006-0265 | E-ISSN:3007-4681
https://bulletin.ouk.kz/index.php/bulletin/index

2. Description and Diagnosis of the Cybersecurity Dimension

Table (9): Frequency Distributions, Arithmetic Means, and Standard Deviations of the Items in the Cybersecurity Dimension

NO.	Item	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)	Mean	Standard Deviation	Relative Importance	Level	Rank
12	The organization implements appropriate measures to protect accounting data from cyberattacks.	21.0	51.6	24.2	2.5	0.6	3.898	0.778	78.0%	High	9
13	The organization determines access permissions for accounting information systems in accordance with the permissions granted to each user.	22.3	61.1	15.3	1.3	0.0	4.045	0.654	80.9%	High	3
14	The organization uses methods to verify users' identities before they access the accounting information system.	24.2	59.9	12.1	3.8	0.0	4.045	0.719	80.9%	High	3
15	The organization uses encryption systems to protect sensitive accounting data from cyber threats.	25.5	58.0	12.7	2.5	1.3	4.038	0.775	80.8%	High	5
16	The organization continuously updates the security protection systems for accounting information systems.	21.7	52.9	20.4	3.8	1.3	3.898	0.826	78.0%	High	9
17	Clear and explicit procedures are available for dealing with cyberattacks and threats to which the accounting information system may be exposed.	17.2	50.3	26.1	4.5	1.9	3.764	0.856	75.3%	High	11
18	The organization protects accounting data from unauthorized access.	28.0	50.3	18.5	3.2	0.0	4.032	0.771	80.6%	High	6
19	The organization maintains backup copies of accounting data.	30.6	59.2	8.3	1.9	0.0	4.185	0.658	83.7%	High	1
20	The organization educates and trains employees on methods of dealing with cybersecurity risks.	24.8	52.2	16.6	4.5	1.9	3.936	0.875	78.7%	High	8

21	The organization strengthens cybersecurity procedures to maintain the confidentiality of accounting data.	28.0	52.9	14.6	3.2	1.3	4.032	0.820	80.6%	High	6
22	Through cybersecurity technologies, the organization maintains the accuracy and integrity of accounting data.	26.1	61.1	10.2	1.3	1.3	4.096	0.723	81.9%	High	2
	Overall Dimension Indicator						3.997	0.575	79.9%	High	

Table (9) indicates that the overall indicator for the cybersecurity dimension yielded an arithmetic mean of 3.997 rating which is higher than hypothetical mean (3) and a standard deviation of 0.575 rating, a coefficient of variance of 14.39%, and a relative importance of 79.9%, which is considered high. The average agreement rate (strongly agree and agree) for the dimension's items was 79.9%. The most popular response was to answer (19) "The organization maintains backup copies of accounting data," with a mean rating of 4.185 and a standard deviation of 0.658. The mean for the question in item (17) "Clear and explicit procedures are available for dealing with cyberattacks and threats to which the accounting information system may be exposed" was 3.764 with the standard deviation of 0.856 and ranked last. The item means ranged from 3.764 to 4.185. The results of the one-sample t-test show that the mean of the dimension differs significantly from the hypothesized mean (t = 21.714, Sig. = 0.000). This dimension had the lowest arithmetic mean value and the highest relative dispersion of all the study dimensions is mentioned. The point on procedures to address cyberattacks was the lowest, which highlighted the difference between cybersecurity and traditional security measures (such as backups and access rights) in terms of both procedures and training.

3. Description and Diagnosis of the Integration between Artificial Intelligence and Cybersecurity Dimension

Table (10): Frequency Distributions, Arithmetic Means, and Standard Deviations of the Items in the Integration between Artificial Intelligence and Cybersecurity Dimension

NO.	**Item**	**Strongly Agree (%)**	**Agree (%)**	**Neutral (%)**	**Disagree (%)**	**Strongly Disagree (%)**	**Mean**	**Standard Deviation**	**Relative Importance**	**Level**	**Rank**
23	Artificial intelligence technologies are integrated with cybersecurity tools and system procedures to protect	32.5	54.1	12.1	1.3	0.0	4.178	0.684	83.6%	High	1

	accounting information systems.										
24	Artificial intelligence technologies help in the early detection of atypical or unusual activities in accounting information systems.	26.8	57.3	14.0	1.9	0.0	4.089	0.692	81.8%	High	5
25	The integration of artificial intelligence technologies and cybersecurity helps reduce the risks of manipulating accounting data.	26.1	57.3	14.6	1.9	0.0	4.076	0.694	81.5%	High	8
26	The integration of artificial intelligence and cybersecurity helps reduce the risks of accounting data breaches.	28.7	55.4	14.6	1.3	0.0	4.115	0.688	82.3%	High	2
27	The integration of artificial intelligence technologies and cybersecurity enhances the system's ability to respond to cyber threats.	26.1	58.6	12.7	2.5	0.0	4.083	0.698	81.7%	High	6
28	The integration of artificial intelligence technologies and cybersecurity enhances oversight of the accounting system.	26.8	57.3	13.4	1.3	1.3	4.070	0.752	81.4%	High	9
29	The integration of artificial intelligence technologies and cybersecurity helps reduce the risk of loss or damage to accounting data.	27.4	58.6	10.8	2.5	0.6	4.096	0.732	81.9%	High	4
30	The integration of artificial intelligence technologies and cybersecurity contributes to enhancing trust in accounting information.	24.8	58.6	12.7	3.2	0.6	4.038	0.750	80.8%	High	11
31	The integration of artificial intelligence and cybersecurity contributes to improving the efficiency of the accounting information system.	21.7	65.6	10.8	1.9	0.0	4.070	0.632	81.4%	High	9
32	The integration of artificial intelligence and cybersecurity contributes to improving the quality of accounting information.	26.1	58.6	13.4	1.3	0.6	4.083	0.707	81.7%	High	6
33	The integration of artificial intelligence and cybersecurity contributes to increasing the	27.4	59.2	11.5	1.3	0.6	4.115	0.698	82.3%	High	2

accuracy of accounting information.				
Overall Dimension Indicator	4.092	0.526	81.8%	High

Table (10) shows that the overall indicator for the integration between artificial intelligence and cybersecurity dimension achieved an arithmetic mean of 4.092, higher than the hypothetical mean (3), with a standard deviation of 0.526, a coefficient of variation of 12.86%, and relative importance of 81.8%, representing a high level. The average agreement rate (strongly agree and agree) for the dimension's items was 85.0%. Item (23), stating that "Artificial intelligence technologies are integrated with cybersecurity tools and system procedures to protect accounting information systems," ranked first, with a mean of 4.178 and a standard deviation of 0.684. Item (30), stating that "The integration of artificial intelligence technologies and cybersecurity contributes to enhancing trust in accounting information," ranked last, with a mean of 4.038 and a standard deviation of 0.750. The item means ranged from 4.038 to 4.178. The one-sample t-test confirms that the difference between the dimension's arithmetic mean and the hypothetical mean is statistically significant (t = 26.001, Sig. = 0.000).

The arithmetic means of the items in this dimension are very close, reflecting broad agreement among respondents on the importance of integrating the two technologies to reduce the risks of intrusion and manipulation and enhance the accuracy of accounting information.

4. Description and Diagnosis of the Reliability of Accounting Information Systems Dimension

Table (11): Frequency Distributions, Arithmetic Means, and Standard Deviations of the Items in the Reliability of Accounting Information Systems Dimension

NO.	Item	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)	Mean	Standard Deviation	Relative Importance	Level	Rank
34	The system provides accounting information in a timely manner.	32.5	56.7	10.8	0.0	0.0	4.217	0.623	84.3%	Very High	1
35	The accounting information system provides accurate information.	30.6	57.3	9.6	2.5	0.0	4.159	0.693	83.2%	High	9
36	The accounting information system provides information that meets users' needs.	31.8	57.3	10.8	0.0	0.0	4.210	0.621	84.2%	Very High	2
37	The system enables access to accounting information whenever needed.	31.8	58.6	8.3	1.3	0.0	4.210	0.641	84.2%	Very High	2

38	The system helps reduce errors occurring during accounting data processing.	32.5	55.4	11.5	0.6	0.0	4.197	0.655	84.0%	High	7
39	The system helps accelerate the completion of operations and the processing of accounting data.	29.9	61.1	8.9	0.0	0.0	4.210	0.589	84.2%	Very High	2
40	The speed of accounting data processing in the system helps in making appropriate financial decisions.	30.6	60.5	7.6	1.3	0.0	4.204	0.628	84.1%	Very High	5
41	The accounting information system provides an appropriate level of protection for accounting information.	24.8	62.4	12.1	0.6	0.0	4.115	0.620	82.3%	High	11
42	The system enables verification of the accuracy of accounting information by referring to its supporting documents.	29.9	61.1	8.3	0.6	0.0	4.204	0.607	84.1%	Very High	5
43	The system enables financial transactions to be traced from their recording through to their presentation in accounting reports.	28.7	61.8	9.6	0.0	0.0	4.191	0.590	83.8%	High	8
44	The system enables accounting data to be updated regularly to reflect new financial transactions.	26.1	63.7	8.9	0.6	0.6	4.140	0.645	82.8%	High	10
	Overall Dimension Indicator						4.187	0.457	83.7%	High	

Table (11) shows that the overall indicator for the reliability of accounting information systems dimension achieved an arithmetic mean of 4.187, higher than the hypothetical mean (3), with a standard deviation of 0.457, a coefficient of variation of 10.91%, and relative importance of 83.7%, representing a high level. The average agreement rate (strongly agree and agree) for the dimension's items was 89.6%. Item (34), stating that "The system provides accounting information in a timely manner," ranked first, with a mean of 4.217 and a standard deviation of 0.623. Item (41), stating that "The accounting information system provides an appropriate level of protection for accounting information," ranked last, with a mean of 4.115 and a standard deviation of 0.620. The item means ranged from 4.115 to 4.217. The one-sample t-test confirms that the difference between the dimension's arithmetic mean and the hypothetical mean is statistically significant (t = 32.561, Sig. = 0.000).

This dimension recorded the highest arithmetic mean and the lowest dispersion among the

study dimensions, indicating respondents' conviction that reliability characteristics are available in accounting information systems, particularly timeliness and meeting users' needs, while the level of protection provided by the system ranked last.

Table (12): Ranking of the Study Dimensions According to Their Arithmetic Means

Dimension	Arithmetic Mean	Standard Deviation	Coefficient of Variation	Relative Importance	t-value	Sig.	Level	Rank
Artificial Intelligence Technologies	4.104	0.453	11.04 %	82.1%	30.535	0.000	High	2
Cybersecurity	3.997	0.575	14.39 %	79.9%	21.714	0.000	High	4
Integration of Artificial Intelligence and Cybersecurity	4.092	0.526	12.86 %	81.8%	26.001	0.000	High	3
Reliability of Accounting Information Systems	4.187	0.457	10.91 %	83.7%	32.561	0.000	High	1

Table (12) shows that all dimensions were at a high level. The reliability of accounting information systems dimension ranked first, with a mean of 4.187, followed by artificial intelligence technologies, with a mean of 4.104; integration between artificial intelligence and cybersecurity, with a mean of 4.092; and, finally, cybersecurity, with a mean of 3.997.

Fifth: Testing the Study Hypotheses

1. Test of the Correlation Hypothesis

Main Hypothesis One: There is a statistically significant correlation, at the 0.05 level, between the integration of artificial intelligence technologies and cybersecurity and the reliability of accounting information systems.

Table (13): Pearson Correlation Coefficient Matrix between the Study Variables (n = 157)

Variable	Artificial Intelligence	Cybersecurity	Integration	Reliability
Artificial Intelligence	1	0.492**	0.596**	0.646**
Cybersecurity	0.492**	1	0.684**	0.626**
Integration	0.596**	0.684**	1	0.680**
Reliability	0.646**	0.626**	0.680**	1

** Correlation is significant at the 0.01 level (two-tailed test). All Sig. values = 0.000.

Table (13) shows a strong, positive, and statistically significant correlation between the integration of artificial intelligence technologies and cybersecurity and the reliability of accounting information systems, with a correlation coefficient of r = 0.680 (Sig. = 0.000). Artificial intelligence technologies were also correlated with reliability at 0.646, while cybersecurity was correlated with reliability at 0.626. The correlation between integration and

reliability is the highest among the independent variables. Integration is also strongly correlated with both artificial intelligence (0.596) and cybersecurity (0.684), confirming that it represents the combination of the two technologies. Accordingly, the first main hypothesis is accepted.

2. Tests of the Effect Hypotheses

Main Hypothesis Two: The integration of artificial intelligence technologies and cybersecurity has a statistically significant effect, at the 0.05 level, on enhancing the reliability of accounting information systems. The following sub-hypotheses arise from it:

• Sub-hypothesis One: Artificial intelligence technologies have a statistically significant effect on enhancing the reliability of accounting information systems.

• Sub-hypothesis Two: Cybersecurity has a statistically significant effect on enhancing the reliability of accounting information systems.

• Sub-hypothesis Three: Artificial intelligence technologies, cybersecurity, and the integration between them have a statistically significant joint effect on enhancing the reliability of accounting information systems.

Table (14): Simple Linear Regression Results for the Effect of the Independent Variables on the Reliability of Accounting Information Systems

Independent Variable	Constant (α)	Slope (B)	Beta	t	Sig.	R	R^2	F	Sig. F	D–W
Integration of Artificial Intelligence and Cybersecurity	1.772	0.590	0.680	11.541	0.000	0.680	0.462	133.203	0.000	1.647
Artificial Intelligence Technologies	1.516	0.651	0.646	10.528	0.000	0.646	0.417	110.830	0.000	2.009
Cybersecurity	2.202	0.497	0.626	9.982	0.000	0.626	0.391	99.643	0.000	1.916

A. Effect of Integration (Main Hypothesis Two): The results show that the regression model is significant, with an F-value of 133.203 and a significance level of 0.000. The coefficient of determination (R^2) was 0.462, meaning that the integration of artificial intelligence technologies and cybersecurity explains 46.2% of the variance in the reliability of accounting information systems, while the remaining proportion is attributable to other factors not included in the model. The slope coefficient (B) was 0.590, meaning that a one-unit increase in the level of integration leads to a 0.590 increase in reliability. This effect is statistically significant (t = 11.541, Sig. = 0.000). The regression equation is: Reliability = 1.772 + 0.590 × Integration. Accordingly, the second main hypothesis is accepted.

B. Effect of Artificial Intelligence Technologies (Sub-hypothesis One): The model is significant

(F = 110.830, Sig. = 0.000), and artificial intelligence technologies explain 41.7% of the variance in reliability, with a slope coefficient (B) of 0.651 that is statistically significant (t = 10.528). Accordingly, the first sub-hypothesis is accepted.

C. Effect of Cybersecurity (Sub-hypothesis Two): The model is significant (F = 99.643, Sig. = 0.000), and cybersecurity explains 39.1% of the variance in reliability, with a slope coefficient (B) of 0.497 that is statistically significant (t = 9.982). Accordingly, the second sub-hypothesis is accepted.

The explanatory power of integration (46.2%) exceeds the explanatory power of artificial intelligence alone (41.7%) and cybersecurity alone (39.1%), supporting the study's central proposition that combining the two technologies has a greater effect on reliability than either technology separately. The D–W values ranged from 1.647 to 2.009, which are close to 2, indicating no autocorrelation problem among the residuals.

Table (15): Analysis of Variance (ANOVA) for the Multiple Regression Model

Source of Variation	Sum of Squares	Degrees of Freedom	Mean Square	F	Sig.
Regression	19.001	3	6.334	71.524	0.000
Residuals	13.549	153	0.0886		
Total	32.549	156			

Table 16): Coefficients of the Multiple Regression Model for the Effect of the Study's Independent Variables on Reliability

Variable	B	Standard Error	Beta	t	Sig.	VIF
Constant	0.901	0.231		3.901	0.000	
Artificial Intelligence Technologies	0.343	0.066	0.340	5.186	0.000	1.584
Cybersecurity	0.197	0.057	0.248	3.426	0.001	1.920
Integration	0.267	0.068	0.307	3.924	0.000	2.256

D. Joint Effect (Sub-hypothesis Three): The two preceding tables show that the multiple regression model is significant (F = 71.524, Sig. = 0.000) and that the three independent variables jointly explain 58.4% of the variance in the reliability of accounting information systems (adjusted R^2 = 0.576). All coefficients were statistically significant. Artificial intelligence technologies had the largest relative effect (Beta = 0.340), followed by integration (Beta = 0.307), and then cybersecurity (Beta = 0.248). The variance inflation factor (VIF) values ranged from 1.584 to 2.256, below 10, indicating no multicollinearity problem among the independent variables. Accordingly, the third sub-hypothesis is accepted.

Table (17): Summary of the Results of Hypothesis Testing

Hypothesis	Indicator	Value	Sig.	Decision
First Main Hypothesis (Correlation)	r	0.680	0.000	Accepted
Second Main Hypothesis (Effect of Integration)	R^2	0.462	0.000	Accepted
First Sub-Hypothesis (Effect of Artificial Intelligence)	R^2	0.417	0.000	Accepted
Second Sub-Hypothesis (Effect of Cybersecurity)	R^2	0.391	0.000	Accepted
Third Sub-Hypothesis (Joint Effect)	R^2	0.584	0.000	Accepted

Sixth: Differences in Responses According to Demographic Characteristics (Supplementary Analysis)

To determine whether respondents' opinions regarding integration and reliability differed according to their characteristics, the independent-samples t-test was used for gender, and one-way analysis of variance was used for the remaining variables. Categories with fewer than five members were excluded because they were statistically insufficient (the under-30 age group and the higher-diploma group).

Table (18): Results of Tests for Differences According to Demographic Characteristics

Demographic Variable	Dimension	Test	Value	Sig.	Decision
Gender	Integration	t	-0.319	0.750	No Differences
Gender	Reliability	t	0.673	0.502	No Differences
Age	Integration	F	2.124	0.123	No Differences
Age	Reliability	F	0.389	0.678	No Differences
Educational Qualification	Integration	F	0.095	0.909	No Differences
Educational Qualification	Reliability	F	0.081	0.922	No Differences
Years of Experience	Integration	F	3.962	0.004	Differences Exist
Years of Experience	Reliability	F	2.810	0.028	Differences Exist
Academic Title	Integration	F	0.189	0.944	No Differences
Academic Title	Reliability	F	0.363	0.835	No Differences
Assigned Duties	Integration	F	0.639	0.635	No Differences
Assigned Duties	Reliability	F	0.263	0.901	No Differences

The results show no statistically significant differences in respondents' opinions regarding integration and reliability attributable to gender, age, educational qualification, academic title, or assigned duties, indicating homogeneity in the sample's opinions. The only exception was years of experience, for which significant differences emerged in the integration dimension (F

= 3.962, Sig. = 0.004) and the reliability dimension (F = 2.810, Sig. = 0.028). The lowest mean was recorded for respondents with less than five years of experience, while the highest mean was recorded for the 5–less than 10 years group for integration and the 10–less than 15 years group for reliability.

Seventh: Conclusions

1. All study dimensions were at a high level. The reliability of accounting information systems dimension achieved the highest arithmetic mean (4.187), while cybersecurity recorded the lowest mean (3.997).
2. Academics recognize the role of artificial intelligence technologies in accelerating accounting data processing and analyzing large volumes of data more strongly than their role in supporting decision-making and detecting financial risks.
3. The weakest aspects of cybersecurity were the clarity of procedures for dealing with cyberattacks (mean = 3.764), updating security systems, and implementing protective measures, compared with the relative strength of maintaining backup copies.
4. There is a strong, positive, and significant correlation between the integration of the two technologies and the reliability of accounting information systems (r = 0.680).
5. Integration alone explains 46.2% of the variance in reliability, a proportion higher than that explained by artificial intelligence (41.7%) or cybersecurity (39.1%) individually. The explanatory power rises to 58.4% when the three variables are entered together, with a significant additional contribution from integration.
6. Respondents' opinions do not differ according to their demographic characteristics, with the exception of years of experience; those with less than five years of experience provided the lowest ratings.

Eighth: Recommendations

1. Establish clear, written procedures for responding to cyber incidents and attacks that accounting information systems may face, and communicate them to employees.
2. Periodically update the security systems protecting accounting information systems and strengthen preventive measures to protect accounting data.
3. Organize training programs for employees on cybersecurity risks and methods of dealing with them, particularly for those with limited experience.
4. Expand the use of artificial intelligence technologies to support accounting decisions and detect financial risks, rather than limiting their use to automating and accelerating processing.
5. Adopt an integrated approach that links artificial intelligence tools with cybersecurity systems (such as intelligent systems for detecting unusual activities), rather than implementing each separately, given the additional effect of integration on enhancing reliability demonstrated by the results.
6. Conduct future studies using samples of practicing accountants in economic entities and compare their results with the opinions of academics.

References

1. Abbas, S. K. (2026). Communication methods of digital public relations in the field of cybersecurity: An analytical study of the website of the Arab Regional Cybersecurity Center. *Lark Journal of Philosophy, Linguistics, and Social Sciences, 18*(1), 524–537.

2. Abdel Fattah, N. Y., & Abu Al-Nasr, S. A. M. (2024). The impact of using artificial intelligence in big data analytics on internal auditing. *Scientific Journal of Financial and Commercial Studies and Research, 5*(2), 413–449.
3. Abuzabiba, A. K., Al-Nasrawi, Z. Q. J., & Al-Nasrawi, K. Q. J. (2024). The role of artificial intelligence in improving the efficiency and quality of investment projects. *The American Journal of Management and Economics Innovations, 6*(1), 54–74.
4. Al-Hasban, A. A. (2009). The extent to which information technology systems auditors comply with international auditing standards relating to the information systems environment to maintain information security and confidentiality in Jordanian commercial banks. *Baghdad Journal of Economic Sciences*, (20).
5. Al-Hiyari, S. M. M. (2022). Jordan between digital services and cybersecurity. *Arab Journal of Human Sciences, 3*(2), 28–46.
6. Al-Shami, A. M. (2018). *The Arab encyclopedia of library, information, and computer science terminology*. Academic Library.
7. Al-Taib, A. M., & Al-Sayeh, J. O. (2025). The importance of applying accounting cybersecurity in Libyan commercial banks. *Journal of Economic Studies, Faculty of Economics, University of Sirte, 8*(1), 191–216.
8. Gheetha, A. (2021). Study on artificial intelligence in banking and financial services. *International Journal of Creative Research Thoughts (IJCRT), 9*(9).
9. Kazim, N. F. (2025). *Cybersecurity: Its concept and history*. ResearchGate. https://www.researchgate.net/publication/389361697_alamn_alsybrany
10. Koutou, K. O. (2018). *Artificial intelligence: Shaping a future New Zealand—An analysis of the potential impact and opportunity of artificial intelligence on New Zealand's society and economy*. New Zealand.
11. Matar, M. (2012). *The theoretical qualification of accounting professional practices* (3rd ed.). Dar Wael for Publishing.
12. Zakaria, H. (2021). *The use of artificial intelligence in e-accounting audit*. Helwan University.