The Republic of Yemen
Presidency of the Republic
Central Organization for
Control and Auditing (COCA)

The Role of the Central Organization for Control and Auditing in Detecting and Protecting Against Cybercrimes in Banks

Rsearch submitted for participation in the 14th Scientific Competition of the Arab Organization of Supreme Audit Institutions – ARABOSAI

Prepared by the researchers

Hanan Salem Saleh Baqtyan
Member of the Central Organization for Control and Auditing – Al Mukalla Branch

Ahmed Omer Ahmed Bakodah
Member of the Central Organization for Control and Auditing – Al Mukalla Branch

2024-1445

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

قَالَ تَعَالَى: ﴿ وَٱتَّقُواْ ٱللَّهَ ٱلَّذِى تَسَآءَلُونَ بِهِۦ وَٱلْأَرْحَامَ إِنَّ ٱللَّهَ كَانَ عَلَيْكُمْ رَقِيبًا ﴾ النساء [1]

قَالَ تَعَالَى: ﴿ وَكَانَ ٱللَّهُ عَلَىٰ كُلِّ شَىْءٍ رَّقِيبًا ﴾ الأحزاب [52]

قَالَ تَعَالَى: ﴿ وَكَذَٰلِكَ نُفَصِّلُ ٱلْأَيَٰتِ وَلِتَسْتَبِينَ سَبِيلُ ٱلْمُجْرِمِينَ ﴾ الأنعام [55]

Abstract

This study aims to highlight the role of the Central Authority for Control and Accountability (COCA) in the Republic of Yemen in the information systems for detecting cybercrime in banks under its oversight, such as the Central Bank of Yemen, the National Bank, and the Agricultural Credit Bank. With the rapid advancements in financial institutions, especially banks, cybercrimes have emerged as a new type of crime that transcends geographical borders and occurs in a short timeframe. Criminals possess the ability to conceal their identities, posing a significant threat to the state. In this context, the importance of regulatory bodies in protecting these institutions from cyberattacks and cybercrimes becomes evident.

A questionnaire was prepared and distributed to a sample of auditors at the presidency of the COCA, as well as its branches in Aden and Mukalla. The study employed a descriptive analytical approach and field study methodology, distributing 140 questionnaires that were analyzed using the SPSS statistical program.

The study concluded with several findings, including that control over information systems, represented by the Central Authority for Control and Accountability, plays a vital role in detecting cybercrimes and providing recommendations to enhance cybersecurity in banks. However, there is a need to strengthen the expertise and skills of these regulatory bodies in the field of cybersecurity through continuous training and development programs. Coordination and collaboration among oversight bodies and relevant entities are essential for effective protection against electronic threats. The findings can be summarized as follows:

1. The level of awareness of cybercrime in banks was high among COCA auditors.
2. The need for improved oversight and protection against cybercrime in banks was significant.

3. The likelihood of various types of cybercrime occurring in banks in the absence of oversight was high.
4. The challenges faced by the oversight body in implementing appropriate control mechanisms to protect against cybercrime were very high.

The study also reached several recommendations for COCA, including:

1. Giving more attention to control over information systems in banks by the government and COCA, and conducting regular audits and reviewing financial reports and banking operations.
2. Recognizing the strong positive correlation between the role of control over information systems and the detection and protection from cybercrimes in banks.
3. Training employees and auditors on the importance of control over information systems, as it plays a significant role in enhancing the detection and protection from cybercrimes in banks. Additionally, training them on assessing cyber risks faced by banks according to the latest threats and practices.
4. Paying more attention to the challenges faced in applying the role of control over information systems and developing solutions and strategies to address these challenges in light of the current technological revolution.
5. Granting COCA full authority to coordinate with security and intelligence agencies to exchange information regarding cyber threats facing banks.

Table of Contents

List of Tables

List of Figures

List of Appendices

Chapter one

The General Framework of the Study Problem and Review of Related Literature

1.1. First Section: The General Framework of the Study

1.1.1. Introduction

In light of the sweeping global developments, the presence of information systems has become a fundamental requirement in any government institution. This has compelled governments to establish control mechanisms for such systems. One of the primary objectives of control over information systems is to ensure the integrity and security of information and data within government entities and institutions. Accordingly, supreme audit bodies in the state are responsible for setting the necessary policies and procedures to safeguard electronic information from unauthorized access or tampering, ensure rapid detection in case of any breach, and verify that the audited entities comply with relevant laws and regulations.

The importance of control over information systems in the detection of cybercrimes continues to grow with the advancement of technology and the widespread use of the internet, as well as local and wide area networks. Cybercrimes pose a significant challenge to information security and privacy, necessitating the use of modern technologies to monitor and detect such crimes.

In this chapter, we will address the research problem, methodology, structure, and divisions of the study. Additionally, we will discuss the role and significance of information systems auditing, its impact on business sustainability and data integrity, and provide an overview of the study's objectives and the methods used to achieve them.

1.1.2. Research Problem and Questions

The features provided by information systems have made them a fundamental pillar in any organization. These features include reducing time and effort and producing better outcomes. For control bodies, this necessitates the implementation of controls over information systems. The situation significantly differs depending on whether or not such systems are subject to auditing procedures. This study focuses on identifying and clarifying the role of control over information systems, as represented by the Supreme Audit Institution (Central Organization for Control and Auditing), in government institutions, and examining its impact and benefits on those institutions.

Organizations and institutions today operate in a digital era characterized by rapid technological advancement and an increasing reliance on information systems. However, due to the rise in cybercrimes, these entities are facing growing security challenges. Cybercrimes can result in significant financial losses, disruption of business operations, and the leakage of sensitive information, making them a serious threat.

According to statistics, Saudi Arabia ranks third globally in terms of exposure to cyberattacks. The Kingdom experienced approximately 54,000 cyberattacks in one year—averaging around 150 attacks per day, or 6.25 attacks per hour. Saudi companies and institutions are frequent targets of hackers due to the strength of the country's economy, which is considered one of the most

powerful in the Middle East and among the top 20 economies worldwide. This was highlighted in a report issued by the Asharqia Chamber [1].

Research indicates that information systems auditing plays a critical role in detecting and preventing cybercrimes. However, institutions continue to face challenges in implementing effective control mechanisms that keep pace with modern technology.

Accordingly, the research problem lies in analyzing the role of information systems auditing—represented in this study by the Central Organization for Control and Auditing—in detecting and preventing cybercrimes, and in identifying the challenges faced by institutions, particularly the audited banks, in applying appropriate control mechanisms.

This study aims to provide effective recommendations and solutions to strengthen information systems auditing and enhance the cybersecurity of banks, specifically focusing on the Central Bank of Yemen and the National Bank.

Therefore, the research problem centers around answering the following questions:

1. What is the level of awareness of cybercrimes in banks from the perspective of the presidency of the Central Organization for Control and Auditing (COCA), including its Aden and Mukalla branches?
2. What is the role of control over information systems in detecting and preventing cybercrimes in banks, from the perspective of COCA presidency and its branches in Aden and Mukalla?

3. To what extent is there a need to improve control and protection against cybercrimes in banks, from the viewpoint of COCA presidency and its Aden and Mukalla branches?

4. What is the perceived likelihood of different types of cybercrimes occurring in the absence of control over information systems in banks, according to the COCA presidency and its branches in Aden and Mukalla?

5. Are the challenges faced by the auditing authority in implementing appropriate control mechanisms to prevent cybercrimes considered high in banks, from the perspective of COCA presidency and its Aden and Mukalla branches?

6. Is the impact of control over information systems perceived as very significant in banks, according to the presidency of COCA and its branches in Aden and Mukalla?

1.1.3. Study Hypotheses

In order to address the research problem and based on the study questions, the following hypotheses can be formulated:

- ✓ **Null Hypothesis (H_0):** There is no statistically significant role of the Central Organization for Control and Auditing (COCA) in control over information systems for detecting cybercrimes in banks, from the perspective of COCA presidency and its branches in Aden and Mukalla.
- ✓ **Alternative Hypothesis (H_1):** There is a statistically significant role of the Central Organization for Control and Auditing (COCA) in control over information systems for detecting and preventing cybercrimes in banks,

from the perspective of COCA presidency and its branches in Aden and Mukalla.

1.1.4. Research Methodology

This study adopts the descriptive approach for the theoretical framework, and the inductive approach for the practical and field aspects of the research. A structured questionnaire will be used to collect data from employees, department heads, sector managers, and bank auditors. This questionnaire is specifically designed to examine the role of the Central Organization for Control and Auditing (COCA) in control over information systems for the detection and prevention of cybercrimes.

1.1.5. Data Collection Sources

1. **Primary Sources**: Data collected through the questionnaire.
2. **Secondary Sources**: Scientific journals, previous studies including master's and doctoral theses, as well as academic research papers and articles.

1.1.6. Objectives of the Study

Main Objective: The main objective of this study is to identify the role of the Central Organization for Control and Auditing (COCA) in detecting and preventing cybercrimes in banks. Specifically, the study seeks to achieve the following:

Sub-objectives:

1. To identify the level of awareness of cybercrimes in banks from the perspective of the presidency of the Central Organization for Control and Auditing (COCA), including its branches in Aden and Mukalla.

2. To examine the role of control over information systems in banks from the viewpoint of COCA presidency and its branches in Aden and Mukalla.
3. To assess the extent of the need to improve auditing and protection against cybercrimes in banks, as perceived by COCA leadership and its Aden and Mukalla branches.
4. To determine the perceived likelihood of various types of cybercrimes occurring in the absence of control over information systems in banks, from the perspective of COCA presidency and its Aden and Mukalla branches.
5. To explore the role of control over information systems in detecting and preventing cybercrimes in banks, according to COCA presidency and its Aden and Mukalla branches.
6. To evaluate the perceived degree of impact of control over information systems auditing on banks, as viewed by the presidency of COCA and its branches in Aden and Mukalla.

1.1.7. Study Population and Sample

The study population consists of all auditors within the Central Organization for Control and Auditing (COCA), particularly those involved in auditing banks and individuals related to information systems. The study sample included 140 participants. To ensure accurate and representative results, various sampling techniques and surveys were applied across COCA presidency and its branches in Aden and Mukalla.

1.1.8. Limitations of the Study

The limitations of the study are divided into:

1. **Subject Matter Limitations**: The study is limited to examining the role of the Central Organization for Control and Auditing (COCA) in detecting and preventing cybercrimes in banks.
2. **Geographical Limitations**: The study covers the National Bank in Aden, the Central Organization for Control and Auditing in Mukalla, and the Central Bank in Mukalla.
3. **Human Limitations**: This study focuses on the auditors within COCA, specifically at COCA presidency and its branches in Aden and Mukalla, who are responsible for auditing banks under COCA's control such as the Central Bank of Yemen, the National Bank, and the Agricultural Credit Bank.
4. **Temporal Limitations**: The study period covers the year 1445 AH / 2024 AD.

1.1.9. Definition of Terms

1. Control

Control is defined as an administrative function carried out by a supervisory authority that has the power to verify the ongoing operations within the audited entity according to the established objectives, assessing its efficiency, adherence to deadlines, and compliance with applicable laws and regulations [2].

The researchers have operationally defined control as the process of monitoring, observing, and evaluating performance by a sovereign higher authority such as the Central Organization for Control and Auditing (COCA). This is carried out to ensure that the audited entity performs its duties in accordance with the state's rules, regulations, and laws, to identify any deviations or errors—whether intentional or unintentional—and to issue reports to decision-makers, thereby enabling timely corrective actions.

2. Cybercrimes

The Organization for Economic Co-operation and Development (OECD) defined computer crime at the Paris meeting as: "Any illegal, unethical, or unauthorized behavior related to the automated processing or transmission of data" [3]. The term **Cyber Crime** is not an Arabic word, but it is widely used in the modern era [4].

Researchers have operationally defined cybercrimes as any violation or infringement that occurs without physical violence or force, but rather through the use of computers and the internet. It is a form of crime that is complex and modern in nature. Cybercrimes are often elusive and difficult to detect, and frequently go unreported. These crimes can be used to gain financial profits while the perpetrator remains at a distance, without the need to be physically present at the crime scene. This characteristic has made banks, such as the Central Bank of Yemen and the National Bank, more vulnerable to such violations.

1.1.10. Structure of the Study

This study is divided as follows:

Chapter One contains the first section, which serves as the introduction to the study. It includes the research problem, methodology, data sources, study objectives, population and sample, limitations, hypotheses, and key terms. The second section of this chapter reviews the previous studies.

Chapter Two provides explanations of key concepts related to the study, such as the concept and types of control, data and information, auditing of information systems, and the concepts of crime and cybercrime.

Chapter Three presents a more detailed view of the methodological procedures followed in the study, alongside the presentation and explanation of the questionnaire analysis results in various tables and figures.

Finally, Chapter Four discusses the study's conclusions and presents the recommendations proposed by the researchers.

1.2. Second Section: Previous Studies

1.2.1. Introduction

Previous studies form a fundamental basis for any scientific research, as they represent a reference for understanding the available knowledge and guiding future research efforts. This section of the study aims to review and analyze prior research related to the topic of information systems auditing and its role in detecting cybercrimes. Given the advancement of knowledge in the field of information systems auditing and the increasing interest in it, understanding previous studies is a vital step toward defining the new research direction and identifying areas requiring further investigation and analysis.

This section will address prior studies, their limitations, and shortcomings. It is worth noting that the fields of auditing and information systems have attracted many researchers, resulting in numerous studies in these interconnected domains. Some studies have focused on the role of control over information systems, while others have examined the impact of

information systems on the control process. The following figure illustrates the relationship between these two distinct entities.

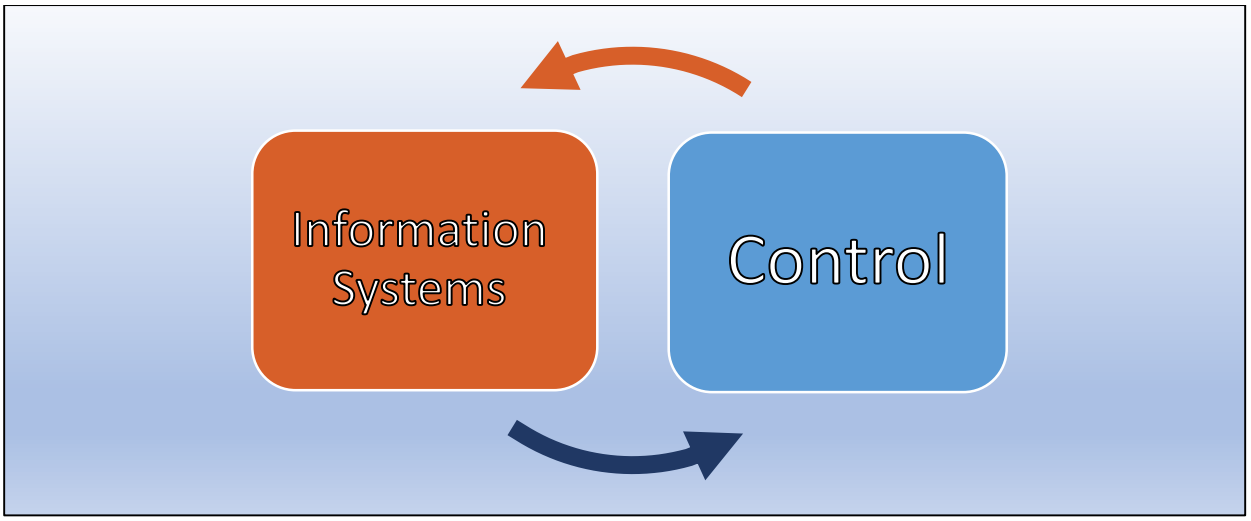

Figure 1-1: Control and Information Systems and Their Mutual Influence

The figure was designed by the Authers

Figure 1 above illustrates the mutual influence between control and information systems: on one hand, the impact and role of control over information systems, and on the other hand, the influence and role of information systems on control.

This research focuses primarily on the first aspect—the role of control over information systems. However, this section will review previous studies related to both aspects. Accordingly, the review will first present studies addressing the role of information systems in the control process, followed by studies focusing on the role of control over information systems.

1.2.2. Previous Studies on the Role of Information Systems in the control Process

1. Study (Warqali, 2023) titled "The Role of the Accounting Information System in Improving the Internal Control System: A Case

Study of the Electricity and Gas Distribution Company in Warqla": Researchers Warqali and Amzit conducted a study addressing the role of the accounting information system in enhancing the internal control system. The research included a case study of the Electricity and Gas Distribution Company. The study concluded that the accounting information system is a key tool in improving the company's financial performance by providing accounting and financial information. Moreover, the electronic accounting information system contributes to producing more reliable and comparable information for decision-makers [5].

2. **Study (Al-Sayyid, 2024) titled "The Role of Information Technology in Enhancing Control over the Resources of the National Postal Authority"**:

The study concluded that the SAP system—which stands for System, Applications, and Products—has a significant positive impact. The authority purchased this system to coordinate functions, store information, and support the internal control system in protecting the authority's resources from misuse and preserving its assets. Additionally, the system prevents unauthorized data extraction at any time without adhering to scheduled timings, thereby enabling quick correction of any deviations from the authority's plans and achieving internal control.

After implementing this system, it became impossible for the postal office agent to conceal any transaction, as each completed transaction is immediately reflected in the system accessible by the internal audit department. However, the system could not provide sufficient protection for depositors' accounts against embezzlement, due to the possibility of employees using the client's signature stamp instead of the client.

This system exemplifies the role of information technology. Thanks to it, the effectiveness and efficiency of the internal control system were enhanced, performance monitoring and evaluation improved, new electronic services were introduced, and regular activity revenues increased [6].

3. **Study (Sakah, 2020) titled "Management Information Systems and Their Role in Ensuring the Quality of Higher Education":** One of the roles provided by management information systems (MIS) is quality assurance, as explored in the study by researcher Wafaa Sakah. The study concluded that there is a statistically significant relationship between management information systems and the quality of education at the university. However, the study also found that the attention given to information systems at the university is low, which negatively affects the optimal utilization of these systems [7]. This highlights that information systems play a tangible role in improving quality across various aspects of life, not just in the field of auditing.

1.2.3. Previous Studies on the Role of control over in Information Systems

1. **Study (Hamada, 2010) titled "The Impact of General Control Measures for Electronic Accounting Information Systems on Increasing the Reliability of Accounting Information (A Field Study)":** Researcher Rasha Hamada conducted a study on the general control measures of electronic accounting information systems, including organizational controls, access controls, file security and protection controls, and system development and documentation controls, and their impact on enhancing the reliability of accounting information. The study

concluded that there is a significant impact of general control measures on increasing the reliability of accounting information in companies [8].

2. **Study (Al-Hakim, 2010) titled "The Feasibility of control Automated Accounting Information Systems in Public Economic Institutions by Inspectors of the Central Organization for Financial Control":** The researcher concluded that there are no significant differences indicating an increase in control effectiveness over information technology, despite the increased use of control measures in accordance with accepted auditing standards. Similarly, there are no differences reflecting improved control effectiveness with the increased use of control procedures by audit inspectors [9].
3. **Study (Muslim, 2024) titled "The Impact of Financial Control Procedures and Their Application Methods on the Quality of Accounting Information Systems in the Public Sector in Saudi Arabia":** The study concluded that there is a statistically significant positive effect of financial control procedures and their application methods on the quality of accounting information systems in the Saudi public sector. It also found an indirect relationship between financial control procedures and the quality of accounting information systems through the methods of applying financial control. The study recommended the continuous evaluation of financial control procedures to ensure that the objectives for which they were established are achieved [10].
4. **Study (Yamina, 2019) titled "Risks of Accounting Information Systems and the Role of Internal Control in Mitigating Them":** The study population consisted of employees of the Algerian External Bank. One of the key findings was that internal control plays a very important role in reducing these risks. Among the main recommendations

to maintain these results was the necessity of using proper documentation for data preservation and storage, as well as training employees to face these risks [11].

In commenting on these studies, the researchers' study agreed with study [7] in using the descriptive approach for the theoretical aspect and the inductive approach through questionnaires. However, it differed in focusing on the role of control over information systems rather than the role of information systems themselves.

The researchers' study also aligned with studies [8], [9], [10], and [11] in emphasizing the role of auditing in information systems. However, the focus here is specifically on the role of the Central Organization for Control and Auditing (COCA) in detecting cybercrimes, particularly within banks.

Chapter Two

Theoretical Framework of the Study

2.1. Section One: Control and Information Systems

2.1.1. Introduction

In this chapter, key concepts will be addressed in some detail, including the concept of control and its types, as well as the concept of crime from both the linguistic and technical perspectives, in addition to reviewing previous studies.

2.1.2. Definition of Control

This paragraph addresses the definition of control from both linguistic and terminological perspectives, highlighting various viewpoints.

Linguistically, **Definition of Control:**

The term *Control* (Arabic: **الرقابة**) is derived from the triliteral root **ر–ق–ب**, which carries meanings such as observation, inspection, examination, guarding, or monitoring. It can also imply *waiting*, especially when the letter **tā'** (ت) is added at the beginning to form the word "**taraggub**" (ترقّب). This root appears in several derivations throughout the Qur'an, including in one of the names of Allah — "**Ar-Raqīb**" (The Watchful) — as mentioned by Prophet Jesus (peace be upon him) in the verse:

قَالَ تَعَالَى: ﴿ إِنَّ ٱللَّهَ كَانَ عَلَيۡكُمۡ رَقِيبٗا ﴾ النساء [1]

قَالَ تَعَالَى: ﴿ فَلَمَّا تَوَفَّيۡتَنِي كُنتَ أَنتَ ٱلرَّقِيبَ ﴾ المائدة [117]

قَالَ تَعَالَى: ﴿ وَكَانَ ٱللَّهُ عَلَىٰ كُلِّ شَيۡءٖ رَّقِيبٗا ﴾ الأحزاب [52]

The verb '**al-irtiqāb**' (anticipation or watchfulness)- in arabic language (الارتقاب) , which is derived from the root '**raqaba**' in arabic language(رقب) , conveys the meaning of waiting, observing outcomes, and monitoring them. This verb appears in numerous contexts throughout the Holy Qur'an, including the following examples:

قَالَ تَعَالَى: ﴿ وَٱرۡتَقِبُوٓاْ إِنِّي مَعَكُمۡ رَقِيبٞ ﴾ هود [93]

قَالَ تَعَالَى: ﴿ فَأَصۡبَحَ فِي ٱلۡمَدِينَةِ خَآئِفٗا يَتَرَقَّبُ ﴾ القصص [18]

قَالَ تَعَالَى: ﴿ فَٱرۡتَقِبۡ إِنَّهُم مُّرۡتَقِبُونَ ﴾ الدخان [59]

Technical (Terminological) Definition of Control:

Control can be defined as the process of evaluating conformity with agreed-upon standards and expressing an opinion on the extent of that conformity. It may also be defined as a function carried out by a competent authority to verify that operations are proceeding according to predetermined objectives, to assess their efficiency, and to ensure that tasks are completed within the designated time frame. Therefore, control is considered an administrative function [2].

One of the key responsibilities of control is detecting any violations or deviations, and in some cases, it may involve correcting them or referring the matter to the appropriate authorities. As such, it provides the manager with reverse feedback that helps in setting future goals and establishing the necessary standards and benchmarks [12].

2.1.3. Types of Control

Control, in general, encompasses a variety of forms and types, each with its own characteristics and definitions. This section will address and explain these different types of control.

1. **Administrative Control (also referred to as Internal Control):** Administrative control is exercised within the administrative unit by superior authorities or the Ministry of Finance to detect financial violations and errors before they occur. It includes self-monitoring performed by the executive authority over its subordinates, as well as the oversight conducted by the Ministry of Finance over ministries and governmental agencies. This type of control involves financial and accounting procedures aimed at protecting assets, ensuring the accuracy of accounting data, enhancing operational efficiency, and ensuring compliance with management policies.

   Internal control encompasses the organizational plan and the financial and accounting procedures adopted by an entity to safeguard its assets, produce reliable and periodic reports for management, and ensure the accuracy of accounting records and both financial and managerial information [13].

2. **Financial Control:** This type of control is concerned with examining the final accounts of the entities under audit and issuing a professional opinion regarding the accuracy of the financial statements [14]. Financial control aims to determine whether the financial information of the audited entities has been presented in accordance with the applicable financial reporting and regulatory frameworks.

   This is achieved by obtaining sufficient and appropriate control evidence, enabling the auditor to express an opinion on whether the financial

information is free from material misstatements, whether due to fraud or error [15].

3. **Compliance Control:** This type of control involves examining the extent to which entities subject to audit by the oversight body comply with laws, regulations, and official decisions [14]. Compliance control assesses whether a specific subject adheres to reference points such as established rules, laws, and regulations that serve as benchmarks.

   It evaluates the compliance of financial activities, transactions, and information with all materially relevant reference points governing the audited entity. These references may include budgetary decisions, approved policies or procedures, agreed-upon terms, or general principles that ensure sound financial management in the public sector and ethical conduct of government employees [15].

4. **Performance Control:** Performance control focuses on effectiveness, efficiency, and economy, and evaluates the extent to which entities subject to audit comply with these principles [14]. This type of control applies appropriate criteria to examine whether interventions, programs, and institutions are operating in accordance with the principles of economy, efficiency, and effectiveness, and whether there is room for improvement to provide relevant recommendations.

   It also involves analyzing the causes of deviations from these standards in order to understand their root causes and propose corrective measures [15].

5. **Political Control:** Political control is exercised by a special political body established by the constitution to ensure that the actions of public authorities—particularly the legislative authority—comply with constitutional

provisions. It is considered a preventive form of control that precedes the enactment of laws.

This type of control is termed "political" because it involves reviewing the constitutionality of laws, a responsibility assigned to a specific political body designated by the constitution—not the parliament, government, or judiciary. It is referred to as "preventive" because it protects the state from passing unconstitutional laws or helps detect unconstitutionality before such laws are enacted. This type of control applies to laws approved by parliament but not yet issued by the head of state [16].

6. **Parliamentary Control:** Parliamentary control is exercised by a legally authorized body, with the aim of ensuring that all governmental actions are carried out in accordance with their planned objectives and within the designated timeframe. This authority is the parliament, which has been granted this power as a representative of the people, to oversee the activities of the executive branch.

   This form of control establishes a mutual influence between the parliament and the government, allowing the parliament to impact government actions through dialogue and the expression of opinions and recommendations. The main purpose of this control is to ensure that the executive branch fulfills its obligations. There are various mechanisms through which parliament can monitor the executive authority, such as questioning, interpellation, and parliamentary inquiries [17].

7. **Popular Control:** In ancient Greek cities, popular control was practiced directly by the citizens of the city. Unlike administrative control, which was later exercised by a designated committee, popular control involved the public overseeing the actions of officials. At the end of an official's term, a

special committee would review their records and accounts, and then present the findings to a people's court for judgment [18].

8. **Self-Control:** Self-control is a supervisory method whereby the governmental entity is responsible for monitoring its own operations in accordance with systems, regulations, and instructions [19].

It is also possible to classify types of control from different perspectives or according to various criteria. For example, if the criterion is the time dimension, control can be categorized into pre-control, concurrent control, or post-control. Pre-control consists of the procedures and arrangements set by the controlling authority prior to the activity or process to prevent the occurrence of any problems and to reduce their impact. Concurrent control, on the other hand, includes the procedures and standards applied by the controlling authority during the execution of activities to ensure that the process proceeds without deviations. Post-control refers to a set of procedures and methods applied to the outputs of the organizational activity after its completion and can be considered as an evaluation tool.

If the classification criterion is changed from the time dimension to the organizational method, control can be divided into surprise control, periodic control, and continuous control. Surprise control is conducted unexpectedly by the controlling authority without prior notice to the entity under supervision. Periodic control occurs at fixed intervals such as weekly, monthly, or annually. Continuous control involves ongoing monitoring and evaluation. Therefore, each criterion leads to different types of control depending on its nature [12].

2.1.4. Concept of Data, Information, and the Relationship Between Them

Data is defined as a collection of unorganized facts and measurements in the form of letters, numbers, words, or phrases that are unrelated to each other and do not influence consumer behavior. Data represents raw, primary material and facts that, in their original form, lack inherent value. After processing, information is extracted from data, and data alone is not useful.

Information, on the other hand, is organized data that has meaning and usefulness. Decision-makers use data by analyzing and interpreting it, thus information depends on data. By linking and processing data, information is generated. When information is gathered from various aspects and perspectives, it forms what is called "knowledge," which may be new and innovative—meaning it has not been discovered before—or it may be an addition to our existing information [7].

2.1.5. Concept of Information Systems

Information systems are generally defined as a set of interconnected and interacting components that collect, process, store data, and have the capability to query, retrieve, and distribute it. This is done to assist senior management in decision-making and problem analysis. Information systems can be manual or computerized.

Manual systems involve input, output, and data processing operations performed using traditional tools such as pen, paper, and calculators, without the use of computers or any advanced technology. On the other hand, computerized systems rely on computers to carry out their operations and data processing, characterized by high speed and accuracy [7].

2.1.6. Concept of Management Information Systems (MIS)

Management Information Systems (MIS) can be defined as a set of measures and organizational arrangements related to information, which involve collecting, retrieving, processing, and storing information to support decision-making, coordination, planning, and control within an organization. Thus, MIS assists in analyzing problems and finding solutions to aid managers and decision-makers. It is, therefore, a combination of a system consisting of people and computer equipment [7].

Information systems are composed of five essential elements [20]:

1. People (the workforce)
2. Hardware
3. Software
4. Data
5. Networks

2.1.7. Concept of Accounting Information Systems

Accounting Information Systems are information systems similar to those commonly known but specialized in financial and accounting operations. They assist decision-makers in analyzing financial issues and making appropriate decisions [7].

2.1.8. Concept of Control over Information Systems

When entities under supervision transition from using manual systems to automated systems, supervisory bodies impose control over the emerging information systems. Initially, these supervisory bodies conduct field surveys to collect data on the extent and usage of information technology within the supervised entities to determine how to control these systems. Administrative, accounting, and internal control systems related to the entities are studied and

examined to verify the efficiency and adequacy of these systems, ensure their protection against breaches, and identify areas for improvement.

The scope of control over information systems can be summarized into several areas: IT management, acquisition, development, implementation, and services of information systems, protection of information assets, as well as business continuity and disaster recovery [14].

2.1.9. Concept of Control over Accounting Information Systems

With the recent adoption of electronic accounting methods, there has been a critical need for controls that ensure the security of information systems through general and application controls.

General controls include computer-based programs such as control over the information system, control over the electronic accounting center, and controls related to the security and integrity of the system.

Application controls: involve protecting information systems at various levels, including the security and reliability of computers and their software, as well as safeguarding files, data, and information. These controls ensure the efficiency of computer operations by implementing controls on inputs, processing, software monitoring, and verifying that software is used for its intended purpose. Additionally, application controls oversee the accuracy, completeness, and proper distribution of outputs, error detection, and checking for any data loss during processing [11].

2.2. Section Two: Cybercrime

2.2.1. Concept of Crime

God created human beings with an innate disposition inclined toward peace and security—either in granting it to others or seeking it from their surrounding environment. This natural disposition does not tend to cause harm to others, whether materially or morally. However, humans have deviated from this sound nature, and in some cases, they dedicate their intellect and efforts to inflict harm in pursuit of personal material gain. From this deviation, the concept of crime emerged.

Before delving into the general definition of crime and the specific concept of cybercrime, it is important to reference the *Routine Activity Theory*, introduced by Lawrence Cohen and Marcus Felson in 1979. The theory posits that the likelihood of a crime occurring increases when three elements are present: a suitable target, the absence of effective guardianship, and a motivated offender. In other words, crime tends to occur when these three elements converge at the same time [21].

Based on this theory and focusing on these three elements, the "suitable target" in the context of this study is the bank—along with its assets, data, and information. The "motivated offender" could appear at any time and place. The most crucial element is the "absence of effective guardianship," where weak control over information systems in banks significantly increases the probability of cybercrime. This is where the role of the Central Organization for Control and Auditing, the focus of this research, becomes critical.

Turning now to the definition of crime both linguistically and legally:
Linguistically, (Arabic language) in *Mukhtar al-Sihah*, the term "crime" (جريمة) is derived from the root ج-ر-م (j-r-m), meaning “to commit a sin” or “to

perpetrate a wrongdoing." The Qur'an says:
" ولا يجرمنكم شنئان قوم على الا تعدلوا "—in which "yajrimannakum" (يَجْرِمَنَّكُمْ) connotes "to drive you into wrongdoing."
The root may also carry the meaning of "cutting off," as in the expressions *jarama al-thamar* or *jarama al-nakhl*, meaning to harvest or cut the fruit from a palm tree [22].

From a legal jurisprudence perspective, crime is generally defined as: "**An unlawful act committed with criminal intent, for which the law prescribes a penalty or preventive measure**" [23].

2.2.2. The Concept of Cybercrime

Cybercrime, also referred to as *information crime* or *electronic crime*, is a term surrounded by ambiguity and lacks a universally agreed-upon definition. It is often viewed as a traditional crime committed using electronic means [24].

Cybercrime can be defined as illegal and unlawful behaviors and actions involving the use of a computer or the internet—along with other technological tools—to cause harm to a victim, or to gain material or informational benefits by committing an unlawful act. This may include deliberately altering or destroying data, or merely accessing it for espionage purposes. Such crimes are usually committed by individuals with advanced knowledge, skills, and expertise in information systems and hacking techniques. Likewise, investigators and judges handling such cases must have sufficient knowledge of these technologies [3].

Although the terms *electronic crime* and *cybercrime* are often used interchangeably, some research highlights subtle differences between them:

- Electronic crimes can be committed in isolation and do not necessarily require a connection to the internet, making them more costly and

complex. In contrast, **cybercrimes** specifically require internet connectivity [25].

- Some scholars consider cybercrime to be broader in scope than electronic crime, as it encompasses all unlawful acts carried out via the internet [25].

The Organization for Economic Co-operation and Development (OECD) defined cybercrime during the Paris meeting in 1983 as: 'Any illegal, unethical, or unauthorized behavior related to the automatic processing or transmission of data.'" [3].

2.2.3. Types of Cybercrimes Likely to Occur in Banks

There are many types of cybercrimes that may occur in banks, including the following:

1. **Bank System Breaches:**
    - Exploiting security vulnerabilities in bank systems to access or steal confidential data, such as databases and servers, with the aim of seizing credentials or performing unauthorized actions.
    - Using malicious software (malware) such as viruses, spyware, and Trojans to infiltrate bank computers and leak information, steal data, or disrupt and take control of systems [1].
    - Carrying out Distributed Denial-of-Service (DDoS) attacks to disrupt bank operations.
2. **Banking Data Theft:**
    - Spying on customer transactions and accounts.
    - Using spyware and eavesdropping tools to steal credit card data and bank account information, often used to make unauthorized

purchases online or in stores—this is known as online financial fraud.

• Hacking into databases to obtain sensitive customer information.

3. **Personal Data Theft:**

The goal is to steal customer data such as names, birthdates, social security numbers, and ID numbers. These can be used to commit financial fraud or identity theft.

4. **Electronic Fraud and Forgery [26]:**

- Creating fake websites imitating banks or sending fake emails and messages claiming to be from the bank in order to trick customers into providing personal or financial information.
- Using phishing tools to steal login credentials.
- Forging financial transactions and making unauthorized money transfers.

5. **Cyber Extortion and Threats:**

- Using (ransomware) to encrypt bank data and demand ransom.
- Threatening to leak sensitive information or expose bank secrets unless a ransom is paid.
- Using phishing attacks to blackmail employees or customers.

6. **ATM Attacks:**

- Installing skimming and spying devices on ATMs to steal card data.
- Hacking ATM control systems and manipulating them.

- Using malware to clone credit cards and perform illegal withdrawals.

To counter these threats, banks must enhance their security infrastructure, implement best cybersecurity practices, provide continuous training to employees, and strengthen cooperation with relevant security agencies.

In addition to the aforementioned types, there are other cybercrimes that may affect banks:

7. **Financial Data Manipulation**:
    - Conducting fake money transfers or fraudulent financial transactions.
    - Altering financial data to conceal illegal activities.
8. **Insider Threats**:
    - Employees exploiting their privileges to gain unauthorized access to bank data and systems.
    - Leaking confidential information or misusing customer data for personal gain.
    - Collaborating with criminal groups to execute theft or embezzlement from within the bank.
9. **Supply Chain Attacks**:
    - Hacking bank vendors and manipulating shared data or software.
    - Conducting espionage attacks on partners and suppliers to access bank data.

10. Critical Infrastructure Targeting:

- Attacking critical infrastructure such as power and communication systems of the bank.
- Disrupting payment and financial settlement systems to cause service outages.
- Exploiting security vulnerabilities in cloud banking systems and Internet of Things (IoT) devices.

To address these threats, banks should implement multi-layered security measures, enhance staff awareness and training, adopt advanced cybersecurity solutions, and cooperate with relevant regulatory and security bodies.

11. Money Laundering:

Money laundering is defined as the process of concealing the true source of illicitly obtained funds (e.g., from drug trafficking or organized crime), disguising them within the formal financial system to give them legitimacy and avoid legal accountability. Banks, as providers of financial services, whether through traditional or digital means, are vulnerable to this crime. It is considered one of the most dangerous crimes and presents a major challenge to banks. It also serves as a measure of a country's legal and regulatory capacity, including its oversight systems represented by institutions such as the Central Organization for Control and Auditing (COCA).

Money laundering is carried out through financial transfers, deposits in banks and financial institutions, the use of electronic payment channels, and encrypted data to ensure confidentiality. Sometimes, it involves a series of complex, rapid, and successive financial operations, which can

destabilize international financial markets and devalue national currencies [27].

These examples represent some of the cybercrimes that may target banks, highlighting the importance of adopting strong security strategies to prevent such crimes and protect customer data and assets.

Chapter Three

Methodological Procedures of the Study

3.1 Introduction

In the previous chapters, the study's problem, objectives, relevant literature, and key concepts and terms related to the research were discussed. This chapter presents the methodological procedures adopted to examine the role of control over information systems in detecting and preventing cybercrime. It outlines the research methodology, the target population, and the selected sample.

3.2 First: Research Methodology

The descriptive-analytical method was adopted in this study as the most appropriate research approach for the subject, which focuses on identifying the role of control over information systems in detecting and preventing cybercrime. Given the nature of the field study, the research was conducted at the presidency of the Central Organization for Control and Auditing, as well as its branches in Aden and Mukalla. In this study, data and information related to the research topic were collected and described both qualitatively and quantitatively, then analyzed to derive findings and recommendations.

3.3 Second: Study Population

The population targeted in this study consists of all bank auditors operating under the supervision of the Central Organization for Control and Auditing,

specifically those based at the presidency, Aden branch, and Mukalla branch. The focus was particularly on information systems auditors within these banks. The total number of individuals in this population was 700 employees as of the year 2024.

3.4 Third: Study Sample

The study sample consisted of 20% of the original population of bank auditors and employees, selected through a random sampling method. Given that the total population was 700, the sample size was calculated using the following formula [7]:

$$\textbf{Sample Size} = (\textbf{Study Population} \times 20) / 100 = 140$$

Accordingly, 140 questionnaire forms were distributed to the primary sample group. A total of 75 questionnaires were returned, while 14 were excluded due to incomplete responses, rendering them invalid for statistical analysis.

Table 1: Study Population and Sample

	Study Sample	Study Population
Count	140	700

3.5 Fourth: Sample Characteristics

The selected sample in this study exhibits several characteristics in terms of gender, years of experience, academic qualifications, job type, and professional role. These attributes will be explored in detail as follows:

1. Gender Variable

The sample was divided into two categories: male and female. The table below presents the number and percentage of each gender group:

Table 2: Number and Percentage by Gender

Gender	Number	Percentage
Male	51	83.6%
Female	10	16.4%
Total	61	100.0%

As shown in the table above, the proportion of male participants was significantly higher than that of females, with 51 males accounting for 83.6% of the total sample. In contrast, the number of female participants was 10, representing only 16.4% of the sample. This distribution is also illustrated in Figure 1.

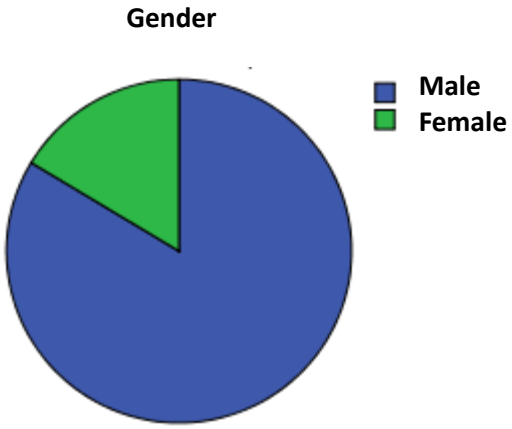

Figure 3-1: Distribution of Sample Members by Gender Variable

2. Years of Experience Variable:

Table 3: Distribution of Sample Members by Years of Experience

Years of Experience	Number	Percentage
15 years and above	19	31.1%
Less than 5 years	10	16.4%
10 years	22	36.1%
5 years	10	16.4%
Total	61	100.0%

The data presented in the table above indicate that the category of "10 years" represents the largest group within the research sample, comprising 22 individuals or 36.1% of the total sample. This is followed by the category "15 years and above", which includes 19 individuals, accounting for 31.1% of the sample. The categories "Less than 5 years" and "5 years" had the lowest representation, each with 10 individuals, making up 16.4% of the sample. Figure 2 illustrates this distribution.

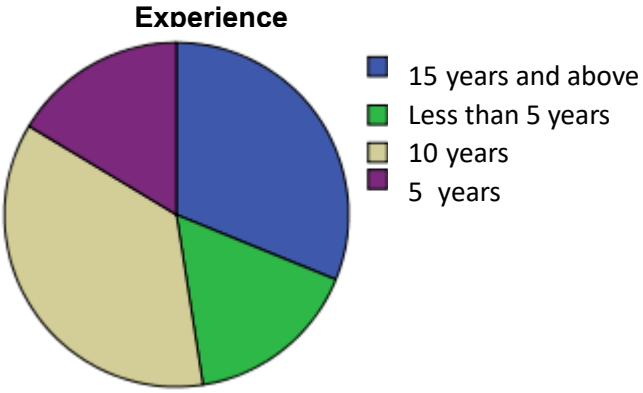

Figure 3-2: Distribution of Sample Members by Years of Experience Variable

3. Educational Qualification Variable

Table 4: Distribution of Sample Members by Educational Qualification

Educational Qualification	Number	Percentage
Bachelor's Degree	52	85.2%
Master's Degree	4	6.6%
Higher Diploma	3	4.9%
High School	1	1.6%
Doctorate	1	1.6%
Total	**61**	**100.0%**

The table above shows that the Bachelor's Degree category constitutes the largest portion of the sample, with 52 individuals, representing 85.2% of the total. In contrast, the High School and Doctorate categories had the lowest representation, with only 1 individual each, accounting for 1.6% of the sample. Figure 3 illustrates this distribution.

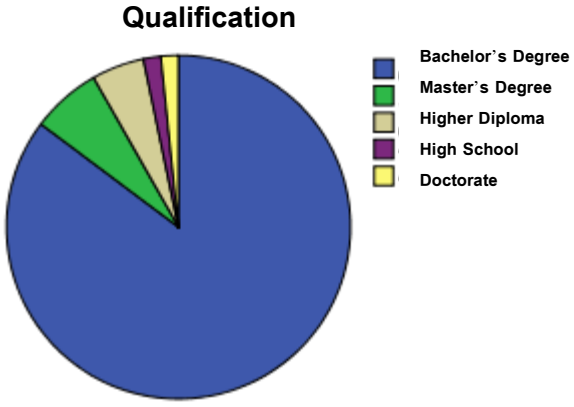

Figure 3-3: Distribution of Sample Members by Educational Qualification Variable

4. Specialization

Table 5: Distribution of Sample Members by Specialization

Specialization	Number	Percentage
English	14	23.0%
Accounting	30	49.2%
Business Administration	3	4.9%
Programming	1	1.6%
Information Technology	6	9.8%
Information Systems	1	1.6%
Banking Sciences	2	3.3%
Law	4	6.6%
Total	**61**	**100.0%**

The table above indicates that the Accounting specialization constitutes the largest segment of the sample, with 30 individuals, representing 49.2% of the total sample. Meanwhile, the Programming and Information Systems specializations have the lowest representation, with only 1 individual each, accounting for 1.6% of the sample. Figure 4 illustrates this distribution.

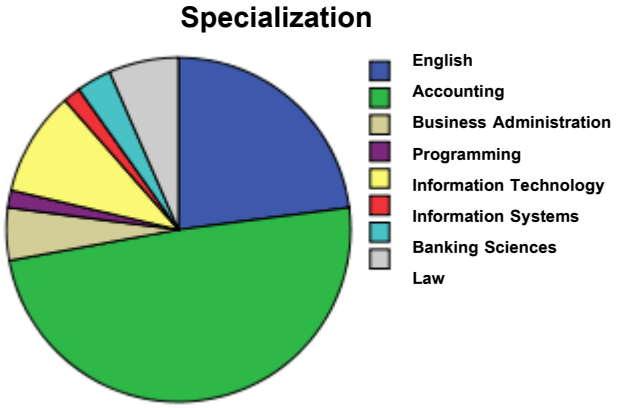

Figure 3-4: Distribution of Sample Members by Specialization Variable

5. Occupation Variable

Table 6: Distribution of Sample Members by Occupation

Occupation	Number	Percentage
Agent	2	3.3%
Auditor	25	41.0%
Information Technology Employee	16	26.2%
General Manager	1	1.6%
Legal Researcher	3	4.9%
Deputy Sector Manager	1	1.6%
Legal Specialist	1	1.6%
Compliance Unit	1	1.6%
Internal Auditor	1	1.6%
Department Head	3	4.9%
Accounts Supervisor	1	1.6%
Service Supervisor	1	1.6%
Accountant	2	3.3%
Employee	2	3.3%
Clearing Room	1	1.6%
Total	**61**	**100.0%**

The table above shows that the occupation of Auditor represents the largest proportion of the sample, with 25 individuals, accounting for 41.0% of the total. This is followed by the occupation of Information Technology Employee, which includes 16 individuals, representing 26.2% of the sample. Figure 5 illustrates this distribution.

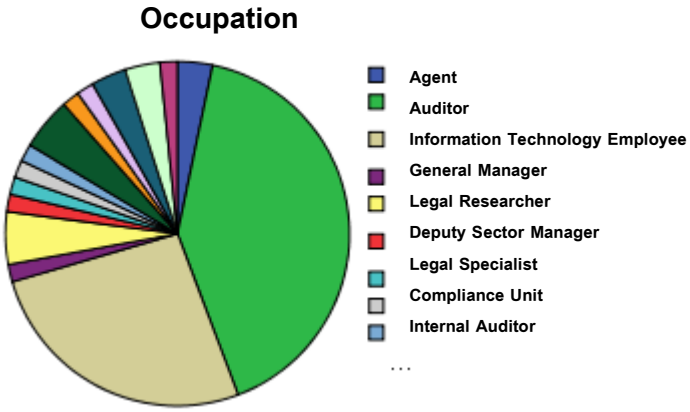

Figure 3-5: Distribution of Sample Members by Occupation Variable

3.6 Fifth: Study Instrument

Based on a review of relevant literature, studies, and research—especially in the fields of technical sciences and information systems—it was determined that the questionnaire is the most appropriate tool to achieve the objectives of the current study.

- **Description of the Study Instrument and Its Development Steps:**
  - Previous literature, including studies and research related to the study topic, was reviewed and utilized to construct the questionnaire and formulate its items.
  - The main domains of the questionnaire were identified.
  - The instrument's domains were defined as follows:
    1. **Domain 1:** Level of awareness regarding cybercrimes (consisting of 4 items).
    2. **Domain 2:** Role of control over information systems (consisting of 6 items).
    3. **Domain 3:** The need to improve control and protection (consisting of 3 items).
    4. **Domain 4:** Types of cybercrimes (consisting of 11 items).

5. **Domain 5**: Impact of challenges (consisting of 5 items).
6. **Domain 6**: Impact of control over information systems (consisting of 5 items).

- The questionnaire items were drafted for each domain. The following table shows the distribution of items according to each domain.
- The questionnaire was reviewed by three experts (**Appendix No. 3**).
- After receiving feedback from the experts, modifications, deletions, and additions were made accordingly, resulting in the finalized version of the questionnaire (see Appendix No. 2). The table below presents the final distribution of questionnaire items according to each study domain:

Table7: distribution of final Questionnaire items

Number of Items	Domain
4	Level of awareness of cybercrimes
6	Role of information systems auditing
3	Need for improving auditing and protection
11	Types of cybercrimes
5	Impact of challenges
5	Impact of information systems auditing
34	**Total**

3.7 Sixth: Statistical Treatment

The study employed the five-point Likert scale to assign relative weights to each statement in order to measure the degree of agreement:

- Likert Scale (Five-point) Specification:
  a. Range = Highest value – Lowest value = $5 - 1 = 4$
  b. Number of categories = 5
  c. Category length = $4 \div 5 = 0.8$

Accordingly, the mean scores for each item and for each domain were classified as follows:

Table 8: Likert Scale rang Interpretation

Rank	Mean Range	Level of Agreement	Verbal Description
1	4.21 – 5.00	Very High	Strongly Agree
2	3.70 – 4.20	High	Agree
3	2.61 – 3.40	Neutral	Moderate
4	1.81 – 2.60	Low	Disagree
5	1.00 – 1.80	Very Low	Strongly Disagree

This scale facilitated the interpretation of results based on calculated averages of responses.

3.8 Seventh: Validity and Reliability of the Instrument

1. Instrument Reliability:

To assess the reliability of the instrument, the researchers employed Cronbach's Alpha coefficient, as illustrated in the following table:

Table 9: Reliability Coefficient Values for the Instrument's Domains

Domain	Number of Items	Cronbach's Alpha
Level of awareness of cybercrimes	4	0.732
Role of information systems control	6	0.710
Need for improved control and protection	3	0.715
Types of cybercrimes	11	0.643
Impact rate of challenges	5	0.671
Impact rate of control over information systems	5	0.698
The instrument as a whole	**34**	**0.581**

It is evident from the table that the reliability coefficient (Cronbach's Alpha) for the items under the domain "Level of awareness of cybercrimes" is 0.732. Similarly, the domain "Role of information systems control" recorded a reliability coefficient of 0.710. The domain "Need for improved control and protection" yielded a coefficient of 0.715, while the domain "Types of cybercrimes" showed a coefficient of 0.643. The domain "Impact rate of challenges" had a reliability coefficient of 0.671, and the domain "Impact rate of control over information systems" recorded a coefficient of 0.698. Furthermore, the overall reliability coefficient of the instrument was 0.581, indicating that the instrument possesses a high degree of reliability and is suitable for application to a sample similar to the one used in this study.

2. Face Validity (Expert Judgment validity):

The questionnaire was presented to three expert judges specializing in the fields of management and auditing (Appendix 3), in order to evaluate the appropriateness, clarity, and relevance of each item to its corresponding domain, as well as the linguistic accuracy of the phrasing. The experts were also asked to provide their opinions regarding any deletions, modifications, or additions, with the aim of ensuring the instrument's alignment with the objectives of the study.

3. Construct Validity of the Instrument (Internal Consistency):

Pearson's correlation coefficient test was employed to determine the correlation between the score of each individual item and the total score of its respective domain.

Table 10: Pearson Correlation Coefficients Indicating the Construct Validity of the Instrument's Domain Items

Domain	Pearson Correlation Coefficient	Significance Level (Sig.)
Level of awareness of cybercrimes	0.224**	.000
Role of information systems control	0.395**	.000
Need for improved control and protection	0.522**	.000
Types of cybercrimes	0.610**	.000
Impact rate of challenges	0.691**	.000
Impact rate of control over information systems	0.570**	.000
The instrument as a whole	**1.000**	**.000**

** Correlation is significant at the 0.01 level (2-tailed).

It is evident from the table that there is a strong correlation between the score of each domain of the instrument and the total score of the instrument at a statistical significance level of less than 0.01. All correlation coefficients exceed 0.224, ranging from 0.224 to 0.691. This indicates that the instrument possesses a high level of validity. Accordingly, it can be concluded that the prepared instrument is reliable and effectively measures what it is intended to measure.

3.9 Eighth: Statistical Methods Used in the Study

Normality Distribution Test:

The Kolmogorov–Smirnov test was employed to assess whether the data follow a normal distribution or not. The following table presents the results of the normality distribution test.

Table 11: Results of the Normality Distribution Test

Main Variables	Statistical Significance (Sig.)
Level of awareness of cybercrimes	0.007
Role of control over information systems	0.000
Need for improved control and protection	0.001
Types of cybercrimes	0.006
Impact rate of challenges	0.001
Impact rate of control over information systems	0.000

It can be observed from the above table that the statistical significance for the domain "Level of awareness of cybercrimes" is 0.007, which is less than 0.05 for all study variables. The significance for the domain "Role of control over information systems " is 0.000, also less than 0.05. Similarly, the domain "Need for improved control and protection" has a significance level of 0.001, the domain "Types of cybercrimes" 0.006, the domain "Impact rate of challenges" 0.001, and the domain "Impact rate of control over information systems" 0.000—all of which are below the 0.05 threshold for all study variables. This indicates that the data are non-normally distributed and do not conform to a normal distribution. Consequently, non-parametric statistical tests are appropriate for analysis.

The following statistical measures and tests were used:

- Cronbach's Alpha test to measure the reliability of the study instrument.
- Pearson correlation coefficient to assess the construct validity of the instrument and the relationships among study variables.
- Arithmetic means, standard deviations, percentages, and relative weights to address the study questions.

Chapter 4

Results and Recommendations

4.1 Introduction

In this chapter, the research findings will be presented, interpreted, discussed, and followed by recommendations and suggestions as outlined below:

4.2 First: Results Related to the First Research Question:

The question states: "**What is the level of awareness of cybercrimes in banks from the perspective of the Central Organization for Control and Accounting, and its branches in Aden and Mukalla?**" To answer this question, arithmetic means, standard deviations, and relative weights were used to measure the level of awareness of cybercrimes in banks. Table 12 illustrates these results:

Table 12: Arithmetic Mean, Standard Deviation, and Relative Weight for Measuring the Level of Awareness of Cybercrimes in Banks

No.	Domain (Level of Awareness of Cybercrimes)	Mean	Standard Deviation	Relative Weight%	Rank	Response Degree	Awareness Level
F1	Familiarity with the concept of cybercrimes	4.09	1.578	81.8%	2	Agree	High
F2	Familiarity with common types of cybercrimes such as electronic fraud, espionage, and hacking	3.96	0.631	79.2%	2	Agree	High
F3	Understanding cyber protection methods used to prevent attacks and safeguard against cybercrimes	3.86	0.939	77.2%	2	Agree	High
F4	Understanding the necessity for employees to receive periodic training on information systems control, cybercrime protection, and cybersecurity	4.32	1.011	86.4%	1	Strongly Agree	Very High
	Overall Domain Score	**4.07**	**0.643**	**81.4%**		**Agree**	**High**

Result:

It is evident from the above table that the level of awareness of cybercrimes in banks, from the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla, was high. The overall mean score was 4.07 with a standard deviation of 0.643 and a relative weight of 81.4%. Items 1, 2, and 3 were rated at a high level, with mean scores ranging between 4.09, 3.96, and 3.86, respectively. Regarding the standard

deviations, they ranged between 1.578, 0.631, and 0.939, all of which are below 1. This indicates considerable homogeneity and agreement among the study sample members regarding their assessments of the level of awareness of cybercrimes in banks from the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla.

Conclusion:

The researchers conclude that the level of awareness of cybercrimes in banks, according to the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla, is high.

4.3 Second: Results Related to the Second Research Question:

The question states: "**What is the role of information systems control in detecting and protecting against cybercrimes in banks from the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla?**" To answer this question, the following main hypothesis was formulated:

- There is a statistically significant role at the 0.05 level for the Central Organization's control over information systems in detecting and protecting against cybercrimes in banks from the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla.

Results of the Main Hypothesis Analysis:

To test this hypothesis, correlation coefficients and simple linear regression analyses were employed to verify its validity.

Table 13: Correlation Coefficients and Multiple Regression Line

Independent Variable	Dependent Variable	Correlation Coefficient (R)	Coefficient of Determination (R^2)	F-Value	Significance Level (Sig)
Control over Information Systems	Cybercrimes	0.71	0.52	5.88	0.018

It is evident from the above table that:

1. **Correlation:** There is a positive correlation between information systems control and the detection of cybercrimes in banks, with a correlation coefficient (R) of 0.71. The F-value, which tests the relationship between information systems control and the detection of cybercrimes, is 5.88 and is statistically significant at the 0.05 significance level.
2. **Coefficient of Determination (R^2):** The R^2 value of 0.52 indicates that information systems control explains 52% of the variance in the detection of cybercrimes, with the remaining variance attributed to other factors.

Conclusion:

The researchers conclude that there is a statistically significant role at the 0.05 level for the Central Organization for Control and Accounting's supervision over information systems in detecting and protecting against cybercrimes in banks, from the perspective of the Central Organization and its branches in Aden and Mukalla.

4.4 Third: Results Related to the Third Question:

Which states: "What is the extent of the need to improve control and protection against cybercrimes in banks from the perspective of the Central

Organization for Control and Accounting, and its branches in Aden and Mukalla?"

To answer this question, arithmetic means, standard deviations, and relative weights were used to measure the extent of the need to improve control and protection against cybercrimes in banks. Table (14) illustrates these results:

Table 14: Level of Improvement in Control and Protection Against Cybercrimes in Banks

No.	Domain (Extent of Need to Improve Control and Protection Against Cybercrimes)	Mean	Standard Deviation	Relative Weight %	Rank	Response Level	Extent of Need for Improvement
F11	There is a need to improve control and protection	4.29	0.863	85.8%	1	Strongly Agree	Very High
F12	There is a need to strengthen laws and regulations related to control and protection	4.32	0.625	86.4%	2	Strongly Agree	Very High
F13	Relevant authorities perform their control and protection roles effectively	3.65	1.153	73.0%	3	Agree	High
	Overall Domain Score	**4.09**	**0.587**	**81.8%**	**Agree**		**High**

Result:

It is evident from the above table that the extent of the need to improve control and protection against cybercrimes, from the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla, was at a high level. The overall mean score reached (4.09) with a standard deviation of (0.587) and a relative weight of (81.8%). Items (11) and

(12), which state "There is a need to improve control and protection" and "There is a need to tighten laws and regulations related to control and protection," respectively, were rated very high, with mean scores ranging between (4.29 - 4.32). The standard deviations for these items ranged between (0.625 - 0.863), all below the value of (1), indicating a strong consensus and agreement among the study sample regarding their estimates **of the need to improve control and protection against cybercrimes**.

Item (13), which states "The relevant authorities perform their control and protection roles effectively," obtained a mean score of (3.65) and a standard deviation of (1.153), indicating a high level of agreement.

Conclusion:

The researchers conclude that the extent of the need to improve control and protection against cybercrimes in banks, from the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla, was high.

4.5 Fourth: Results Related to the Fourth Question:

This question states: "**What is the likelihood of occurrence of various types of cybercrimes in banks in the absence of control, from the perspective of the Central Organization for Control and Accounting and its branches in Aden and Mukalla?**"

To answer this question, arithmetic means, standard deviations, and relative weights were used to measure the likelihood of occurrence of different types of cybercrimes in banks under the absence of control. Table (15) illustrates these results.

Table 15: Illustrates the Probability Levels of Occurrence of Various Types of Cybercrimes in Banks

No.	Domain (Likelihood of Occurrence of Cybercrime Types in Banks)	Mean	Std. Deviation	Relative Weight %	Rank	Response Level	Likelihood Level
F14	Bank Systems Breach	4.09	1.028	81.8%	4	Agree	High
F15	Theft of Banking Data	4.19	0.653	83.8%	3	Agree	High
F16	Theft of Personal Data	4.21	0.709	84.2%	2	Strongly Agree	Very High
F17	Electronic Forgery and Fraud	4.19	0.770	83.8%	3	Agree	High
F18	Cyber Extortion and Threats	4.33	0.680	86.6%	1	Strongly Agree	Very High
F19	Attacks on Automated Teller Machines (ATMs)	4.19	0.678	83.8%	3	Agree	High
F20	Manipulation of Financial Data	4.10	0.796	82.0%	5	Agree	High
F21	Internal Attacks by Employees	3.91	0.936	78.2%	9	Agree	High
F22	Supply Chain Targeted Attacks	3.96	0.948	79.2%	7	Agree	High
F23	Targeting Bank's Critical Infrastructure	3.95	0.883	79.0%	8	Agree	High
F24	Malware (Malicious Software such as Viruses)	4.01	1.117	80.2%	6	Agree	High
	Overall Domain Score	**4.10**	**0.621**	**82.0 %**	**Agree**		**High**

Result:

It is evident from the above table that the perceived likelihood of occurrence of various types of cybercrimes in banks, from the perspective of the Presidency of the Central Organization for Control and Accounting and its branches in Aden and Al-Mukalla, was rated as high. The overall mean score

was (4.10) with a standard deviation of (0.621) and a relative weight of (82%). Item (1), which refers to "cyber extortion and threats," scored very high, with a mean of (4.33) and a standard deviation of (0.680). The remaining items also received high mean scores ranging from (3.91 to 4.19) with standard deviations between (0.770 and 0.936), all of which are less than (1). This indicates substantial consensus and agreement among the study sample regarding their assessments of the likelihood of occurrence of different types of cybercrimes in banks from the aforementioned perspectives.

Conclusion:

The researchers conclude that the perceived likelihood of occurrence of various types of cybercrimes in banks in the absence of effective control, as viewed by the Presidency of the Central Organization for Control and Accounting and its branches in Aden and Al-Mukalla, is high.

4.6 Fifth: Results Related to the Fifth Research Question:

This question investigates: "Are the challenges faced by the regulatory authority in implementing appropriate control mechanisms to protect against cybercrimes considered high in banks from the perspective of the Presidency of the Central Organization for Control and Accounting and its branches in Aden and Al-Mukalla?"

To answer this question, means, standard deviations, and relative weights were used to determine whether the challenges encountered by the regulatory authority in implementing effective control mechanisms for cybercrime protection are perceived to be high. Table (16) illustrates these findings.

Table 16: Illustrates the extent to which the challenges faced by the regulatory authority in implementing appropriate control mechanisms to protect against cybercrimes are perceived to be high.

No.	Domain (The proportion of challenges faced by the regulatory body in implementing appropriate mechanisms to protect against cybercrimes is considered high)	Mean	Std. Deviation	Relative Weight (%)	Rank	Level of Agreement	Degree of Challenge
F25	Rapid developments in information technology and cybercrimes	4.34	0.834	86.8%	2	Strongly Agree	Very High
F26	Lack of technical skills and training in the field of cybersecurity	4.34	0.772	86.8%	2	Strongly Agree	Very High
F27	Limited cooperation with other entities in exchanging information and expertise in combating cybercrimes	4.13	0.670	82.6%	3	Agree	High
F28	Weak technological infrastructure and electronic systems in the regulatory body, and the need for advanced tools and techniques	4.40	0.642	88.0%	1	Strongly Agree	Very High
F29	Presence of gaps and ambiguity in laws and legislation related to cybercrimes	4.40	0.715	88.0%	1	Strongly Agree	Very High
	Overall Domain Score	**4.32**	**0.512**	**86.4%**	**Strongly Agree**		**Very High**

Result:

It is evident from the above table that the level of challenges facing the regulatory body in implementing appropriate control mechanisms to protect against cybercrimes is very high, according to the perspectives of the Presidency of the Central Organization for Control and Auditing (COCA), and COCA branches in Aden and Mukalla. The overall mean score reached (4.32) with a standard deviation of (0.512) and a relative weight of (86.4%).

Item (28), which states: "Weak technological infrastructure and electronic systems within the regulatory body, and the need for advanced tools and techniques", received the highest score with a mean of (4.40) and a standard deviation of (0.642), indicating a very high degree of challenge. Similarly, items (29), (25), and (26) also received very high scores, while item (27), which states: "Limited cooperation with other entities in exchanging information and expertise in combating cybercrimes", obtained a slightly lower mean of (4.13) and a standard deviation of (0.670)—yet still indicates a high level of challenge.

Notably, all standard deviation values were less than 1, which reflects a high level of agreement and consistency among the study sample regarding their assessment of the challenges facing the regulatory body in implementing effective cybercrime control mechanisms, as perceived by the COCA presidency and its Aden and Mukalla branches.

Conclusion:

The researchers conclude that the challenges facing the regulatory body in implementing appropriate mechanisms to protect against cybercrimes were very high from the perspective of the Presidency of the Central Organization for Control and Auditing, as well as its branches in Aden and Mukalla.

4.7 Sixth: Findings Related to Research Question Six:

Which states:"Is **the impact of control over information systems in banks considered very high from the perspective of the Presidency of the Central Organization for Control and Auditing (COCA), and COCA branches in Aden and Mukalla?**"

To answer this question, means, standard deviations, and relative weights were used to determine whether the impact of control over information systems in banks is indeed considered very high. Table (17) presents the relevant results.

Table 17: Illustrates that the impact of control over information systems in banks is very high.

No.	Domain (The impact of control over information systems in banks is considered very high)	Mean	Std. Deviation	Relative Weight (%)	Rank	Level of Agreement	Degree of Impact
F30	Enhancing responsiveness to cyberattacks	4.26	0.834	85.2%	4	Strongly Agree	Very High
F31	Reducing the negative impacts of cyberattacks on the bank and its clients	4.32	0.772	86.4%	3	Strongly Agree	Very High
F32	Protecting account data and clients' financial information	4.22	0.670	84.4%	5	Strongly Agree	Very High
F33	Preserving the bank's reputation and trust among clients and partners	4.52	0.642	90.4%	1	Strongly Agree	Very High
F34	Compliance with cybersecurity-related laws and regulations	4.40	0.715	88.0%	2	Strongly Agree	Very High
	Overall Domain Score	**4.35**	**0.102**	**87.0%**	**Strongly Agree**		**Very High**

Result:

It is evident from the above table that the impact of control over information systems in banks is perceived as very high from the perspective of the Presidency of the Central Organization for Control and Auditing (COCA), and its branches in Aden and Mukalla. The overall mean score was (4.35) with a standard deviation of (0.102) and a relative weight of (87%). All item means within this domain were also very high, ranging between $(4.22 - 4.52)$, with standard deviations between $(0.670 - 0.715)$. These standard deviations are all less than 1, indicating a high level of consistency and agreement among the respondents regarding their assessment of the impact of control over information systems in banks as being very high, as viewed by COCA's headquarters and its Aden and Mukalla branches.

Conclusion:

The researchers conclude that the impact of control over information systems in banks was perceived as very high from the perspective of the Presidency of the Central Organization for Control and Auditing, as well as its branches in Aden and Mukalla.

4.8 Summary of Findings, Recommendations, and Suggestions

First: Summary of Findings

1. The level of awareness regarding cybercrimes in banks was found to be **high**, from the perspective of the Presidency of the Central Organization for Control and Auditing (COCA), and COCA branches in **Aden and Mukalla**.
2. There is a statistically significant role, at the **0.05 level**, for control over information systems in **detecting cybercrimes in banks**, as perceived by COCA and its branches in Aden and Mukalla.

3. The **need to enhance control and protection** against cybercrimes in banks was rated as **high**, according to the views of COCA and its regional branches.
4. The **likelihood of various types of cybercrimes occurring in banks** in the absence of proper control was perceived as **high**, based on the perspectives of COCA and its Aden and Mukalla branches.
5. The **impact of control over information systems on banks** was considered **very high** from the viewpoint of COCA and its regional branches.
6. The **level of challenges** faced by the regulatory authority in implementing appropriate control mechanisms to protect against cybercrimes was found to be **very high**, according to COCA and its branches in Aden and Mukalla.

Second: Recommendations

1. Greater attention should be given to control over information systems by both the **government and COCA**, through conducting regular audits and reviewing financial reports and banking operations.
2. It is crucial that COCA recognizes the **strong positive correlation** between its control role and the **detection and prevention of cybercrimes in banks**. Applying robust control over information systems practices enhances the organization's ability to uncover and mitigate cybercrimes.
3. COCA should assign **significant importance** to the control over information systems by **training staff**, as it plays a pivotal role in improving detection and protection capabilities against cybercrimes in banks.
4. COCA must pay **greater attention to the challenges** hindering the implementation of effective control over information systems, and should

develop solutions and strategies to address these challenges amidst the current technological revolution.

5. COCA should focus on **supporting and enhancing** all modern methods and proposals that facilitate the **implementation of control and auditing programs and cybercrime detection plans**, and work on activating, developing, and updating its information systems auditing processes.

Third: Suggestions

1. Conduct further **future studies** on the topic of control over information systems and cybercrimes in the banking sector.
2. Undertake additional research on **cybercrimes and their impact** on the effectiveness and performance of COCA.
3. Develop and study a **proposed model** for an information systems controlling and auditing framework within COCA aimed at addressing weaknesses and enhancing cybercrime detection and prevention in banks.
4. Conduct studies that assess the **current challenges and issues** facing the implementation of control over information systems in banks.

References

1. Z. A. Al-Otaibi, *"Cybercrimes Committed via Digital Media and the Concept Thereof: Forms, Characteristics, Elements, and Motives Behind Their Commission"*, The Global Academic Journal for Legal Studies, 2021.
2. M. Mohamed, M. A. Al-Noor, M. Khaled, and M. Khaldiya, *"Self-Censorship in Algerian Press Institutions: A Study on a Sample of Algerian Newspapers"*, Master's Thesis in Media and Communication Sciences, Specialization in Public Relations, Ibn Khaldoun University, Tiaret, 2022.
3. Sh. Qasmi and F. Belghith, *"International Strategies to Combat Cybercrime – A Case Study of Algeria"*, Master's Thesis, Department of Political Science, Larbi Tebessi University, Algeria, 2020.
4. S. Baytam, *"The Evolution of Cybercrime and the Legal Mechanisms to Combat It Amid Geopolitical Transformations"*, Journal of the College of Law and Political Science, Iraqi University, 2023.
5. M. Wergli and A. A. Amzit, *"The Role of the Accounting Information System in Improving the Internal Control System: A Case Study of the Electricity and Gas Distribution Company in Ouargla"*, Master's Thesis, Faculty of Economic Sciences, Commercial Sciences and Management Sciences, Kasdi Merbah University, Ouargla - Algeria, Journal of Kasdi Merbah University, Ouargla - Algeria, 2023.
6. S. M. El-Sayed, *"The Role of Information Technology in Enhancing Oversight of the Resources of the National Postal Authority"*, Journal of Commercial Research – Faculty of Commerce, Zagazig University, 2024.
7. W. S. Saqqah, *"Management Information Systems and Their Role in Ensuring the Quality of Higher Education"*, Master's Thesis, Faculty of Economics – Department of Management, Al-Zawiya University, Cairo, 2020.
8. R. Hamada, *"The Impact of General Control Measures for Electronic Accounting Information Systems on the Reliability of Accounting Information (Field Study)"*, Faculty of Economics, 2010.
9. S. M. Al-Hakim, *"The Possibility of Auditing Automated Accounting Information Systems in Public Economic Institutions by Inspectors of the Central Financial Control Authority"*, Doctoral Thesis, Faculty of Economics, Damascus University, Journal of Damascus University for Economic and Legal Sciences, 2010.
10. J. Al-Muslim, *"The Impact of Financial Oversight Procedures and Their Implementation Methods on the Quality of Accounting Information Systems in the Public Sector in Saudi Arabia"*, Arab Journal of Management, 2024.
11. M. Yamina, *"Risks of Accounting Information Systems and the Role of Internal Control in Reducing Them"*, Algerian Journal of Economic Performance, 2019.
12. M. Asia, H. Rania, and M. Salim, *"The Role of Digitization in Enhancing Control in the Institution: A Case Study of the Directorate of Algeria Post, Guelma Province"*, Master's Thesis, Financial and Accounting Sciences, 8 May 1945 University - Guelma -, 2023.
13. A. A. Jassim, *"Oversight of the Implementation of the General Budget of the State in Iraqi Legislation"*, Al-Rafidain Journal of Law, 2010.
14. Audit Bureau of the Kingdom of Bahrain. (2024, June 11). *Financial Oversight*.
15. General Directorate of Audit and Legal Affairs, *"General Guide for Oversight (Financial – Compliance – Performance) for Audit Bureaus in the Gulf Cooperation Council Countries"*, Gulf Cooperation Council Secretariat, 2022.

16. D. Z. Sharif, *"The Principle of Constitutional Supremacy"*, Master's Thesis, Faculty of Law, Al-Nahrain University, Journal of Al-Nahrain University, 2022.
17. Sh. Kh. A. Al-Dosari, *"Parliamentary Oversight"*, University Research and Studies Platform, 2020.
18. A. A. Jassim, *"Oversight of the Implementation of the General Budget of the State in Iraqi Legislation"*, Al-Rafidain Journal of Law, 2010.
19. Ministry of Finance of the Kingdom of Saudi Arabia, *Transformation of Financial Oversight*, 2023.
20. D. A. Mahmoud and M. Y. Hajem, *"Industrial Information Systems as a Tool for Marketing Industrial Products"*, Doctoral Thesis, Faculty of Education and Humanities, Diyala University, Diyala Journal, 2020.
21. M. S. Ali, *"The Contribution of Routine Activity Theory to Understanding Cybercrimes: An Exploratory Study"*, Egyptian Journal of Social and Behavioral Sciences, 2022.
22. D. F. Al-Muwaizri, *"Contemporary Jurisprudential Applications Related to Criminal Offenses in Islamic Jurisprudence and Kuwaiti Law"*, Journal of Arab Studies, 2022.
23. N. M. Al-Rubaie, *"Cybercrime and Mechanisms to Combat It – A Comparative Study"*, Al-Farabi Journal of Human Sciences, vol. 3, 2024.
24. S. Al-Mutairi, *"The Concept and Characteristics of Electronic Crimes"*, Legal Journal (A Specialized Journal in Legal Studies and Research), Peer-Reviewed Scientific Journal, 2023.
25. A. Bessafa, *"The Legal Frameworks for Cybercrime in Algerian Legislation Between Prevention and Combat"*, Annals of the University of Algiers, vol. 37, pp. 98–113, 2023.
26. S. S. Al-Jubouri, *"The Crime of Electronic Fraud – A Comparative Study"*, Master's in Public Law, Faculty of Law, Al-Nahrain University, Journal of Al-Nahrain University, 2014.
27. Middle East and North Africa Financial Action Task Force (MENAFATF), *"Typologies Report on Money Laundering Through Electronic Means"*, 2017.

Appendices

Appendix 1: The Initial Version of the Questionnaire (Before Expert Review)

Title of the Questionnaire:

The Role of the Central Organization for Control and Auditing in Detecting and Preventing Cybercrimes in Banks

Introduction:

Thank you for participating in this questionnaire. The purpose of this survey is to understand the role of control over information systems in detecting cybercrimes and protecting systems against them. Please answer the following questions honestly and select responses that best reflect your opinions and experiences. Completing the questionnaire will take approximately 10 minutes. We sincerely appreciate your time and cooperation in advance.

This questionnaire has been designed to provide a realistic picture of the role of information systems auditing in detecting cybercrimes, identifying weaknesses in information systems controls, and assessing their impact on the severity of cybercrimes.

Personal Information

1. **Gender:**
   - Male
   - Female
2. **Occupation:**
   - Auditor
   - IT Staff / Employee
   - Other (please specify):_____ ____
3. **Years of Experience in the Occupation Specified Above:**
   - ☐ Less than 5 years
   - ☐ 5 to less than 10 years
   - ☐ 10 to less than 15 years
   - ☐ 15 years and above
4. **Educational Qualification:**
   - General Secondary Education
   - Higher Diploma
   - Bachelor's Degree
   - Master's Degree
   - Doctorate (PhD)
5. **Field of Specialization:**
   - Information Systems
   - Accounting
   - Business Administration
   - Law
   - Information Technology
   - Other: _____

Section 1: Level of Awareness of Cyber Crimes

Please assess your level of awareness regarding cyber crimes and their various types by selecting the most appropriate response for each statement.

#	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	I am aware of the concept of cyber crimes.					
2	I know the common types of cyber crimes such as online fraud, espionage, and hacking.					
3	I am familiar with cybersecurity methods used to prevent attacks and protect against cyber crimes.					
4	I believe it is necessary for employees to receive regular training on information systems control and cybersecurity.					

Section 2: Role of Control over Information Systems

Please answer the following questions based on your personal perspective and experience regarding the role of information systems control in detecting and protecting against cyber crimes.

#	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Control over Information systems plays an important role in detecting cyber crimes.					
2	Control over Information systems can contribute to preventing cyber crimes.					
3	Training and awareness in cybersecurity matters play a crucial role in enhancing the effectiveness of Control over information systems.					
4	Cyber crimes pose a serious threat to bank security.					
5	There is a need to strengthen Control over information systems in banks to combat cyber crimes.					
6	Cooperation with external specialized entities in cybersecurity can help enhance control and protection within the bank.					

Section 3: Suggestions for Improving Control and Protection

Please share your ideas on enhancing control over information systems and protection from cyber crimes.

#	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	There is a need to improve control and protection.					

2	There is a need to tighten laws and regulations related to control and protection.					
3	The relevant entities responsible for control and protection are performing their roles effectively.					

Section 4: Types of Cyber Crimes

From your perspective, indicate the likelihood of occurrence of each type of crime in the absence of control over information systems in banks

#	Crime Type	Very High Probability	High Probability	Moderate Probability	Low Probability	Very Low Probability
1	Bank systems hacking					
2	Theft of banking data					
3	Theft of personal data					
4	Forgery and electronic fraud					
5	Cyber extortion and threats					
6	Attacks on ATM machines (ATM spying)					
7	Manipulation of financial data					
8	Internal attacks by employees					
9	Supply chain targeting attacks (hacking software and network providers)					
10	Targeting critical bank infrastructure (e.g., energy, communications, payment, and settlement systems)					
11	Malware (malicious software like viruses)					

Section 5: From your perspective, indicate the degree of impact of the challenges faced by the supervisory authority in implementing appropriate control mechanisms to detect and protect against cyber crimes?

#	Challenge	Very High Impact	High Impact	Moderate Impact	Low Impact	Very Low Impact
1	Rapid developments in information technology and cyber crimes require continuous updating of laws and policies, making it difficult for the					

	supervisory authority to keep pace with these developments.					
2	Lack of skills and technical training in cybersecurity and electronic investigations among human resources.					
3	Limited cooperation with other entities to exchange information and expertise in combating cyber crimes.					
4	Weak technological infrastructure and electronic systems at the supervisory authority and the need for advanced tools and techniques to detect and analyze cyber crimes.					
5	Presence of gaps and ambiguities in laws and legislation related to cyber crimes, thus increasing the need for comprehensive, detailed, and up-to-date legal frameworks to address these crimes.					

Section 6: From your perspective, indicate the degree of impact of control over information systems in the following points:

#	Item	Strongly High Impact	High Impact	Moderate Impact	Low Impact	Very Low Impact
1	Improving the response to cyber attacks					
2	Reducing the negative effects of cyber attacks on the bank and its customers					
3	Protecting sensitive data and financial information of customers					
4	Maintaining the bank's reputation and trust among customers and partners					
5	Compliance with cybersecurity laws and regulations					

----------The questionnaire has ended----------

Appendix 2: Final Version of the Questionnaire (Post-Validation)

Title of the Questionnaire:

The Role of the Central Organization for Control and Auditing in Detecting and Preventing Cyber Crimes in Banks

Introduction:

Thank you for participating in this questionnaire. The purpose of this survey is to understand the role of information systems auditing, as carried out by the Central Organization for Control and Auditing, in detecting cyber crimes and protecting systems from them. Kindly answer the following questions honestly and choose the responses that reflect your views and experiences. Completing the questionnaire will take approximately 10 minutes. Thank you in advance for your time and cooperation.

This questionnaire has been designed to reflect the reality on the ground in order to identify the role of information systems auditing in detecting cyber crimes, to pinpoint weaknesses in the oversight of information systems, and to assess how these weaknesses contribute to the intensity and occurrence of cyber crimes.

Personal Information

1. **Gender:**
   - ☐ Male
   - ☐ Female
2. **Occupation:**
   - ☐ Auditor
   - ☐ IT Staff / Employee
   - ☐ Other (please specify):--------
3. **Years of Experience in the Occupation Specified Above:**
   - ☐ Less than 5 years
   - ☐ 5 to less than 10 years
   - ☐ 10 to less than 15 years
   - ☐ 15 years and above
5. **Educational Qualification:**
   - ☐ General Secondary Education
   - ☐ Higher Diploma
   - ☐ Bachelor's Degree
   - ☐ Master's Degree
   - ☐ Doctorate (PhD)
6. **Field of Specialization:**
   - ☐ Information Systems
   - ☐ Accounting
   - ☐ Business Administration
   - ☐ Law
   - ☐ Information Technology
   - ☐ Other: _____

Section 1: Level of Awareness of Cybercrimes

Please rate your level of awareness regarding cybercrimes and their various types by selecting the most appropriate response to each statement.

No.	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Awareness of the concept of cybercrimes					
2	Awareness of common types of cybercrimes such as electronic fraud, espionage, and hacking					
3	Understanding of cybersecurity protection methods used to prevent and protect against cyberattacks					
4	Understanding the necessity for employees to receive periodic training on information systems auditing, cybercrime prevention, and cybersecurity					

Section 2: Role of Control over Information Systems

Please respond to the following statements based on your own views and experience regarding the role of control over information systems in detecting and preventing cybercrimes

No.	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Control over Information systems plays an important role in detecting cybercrimes					
2	Control over Information systems contributes to preventing cybercrimes					

Section 3: Need to Improve Control and Protection

Please indicate your agreement with the following statements regarding the need to enhance control and cybersecurity measures.

No.	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	There is a need to improve Control and protection measures					
2	There is a need to tighten laws and regulations related to control and protection					
3	The entities responsible for control and protection are					

	performing their roles effectively					

Section 4: Types of Cybercrimes

The likelihood of the following cybercrimes occurring is considered very high in the absence of effective information systems auditing in banks.

No.	Type of Crime	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Bank system hacking					
2	Theft of banking data					
3	Theft of personal data					
4	Electronic fraud and forgery					
5	Cyber blackmail and threats					
6	ATM attacks (e.g., skimming)					
7	Manipulation of financial data					
8	Insider attacks by employees					
9	Supply chain attacks (e.g., targeting network/software vendors)					
10	Targeting critical banking infrastructure (e.g., power, communication, settlement systems)					
11	Malware attacks (e.g., viruses, malicious software)					

Section 5: Challenges Facing Regulatory Entities

The impact of the following challenges on regulatory entities' ability to implement effective cybercrime detection mechanisms is considered very high.

No.	Challenge	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Rapid developments in IT and cybercrime requiring constantly updated laws and policies, making it difficult for regulatory entities to keep up					
2	Lack of technical skills and cybersecurity/investigation training for personnel					
3	Limited cooperation with other entities to exchange information and expertise in combating cybercrimes					

4	Weaknesses in technological infrastructure and the need for advanced tools to detect and analyze cybercrimes					
5	Gaps and ambiguities in laws and legislation related to cybercrime, requiring comprehensive and up-to-date legal frameworks					

Section 6: Impact of control over Information Systems

The impact of control information systems on the following areas is considered very high:

No.	Aspect	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Improving response to cyberattacks					
2	Reducing the negative effects of cyberattacks on the bank and its customers					
3	Protecting sensitive data and financial information of customers					
4	Preserving the bank's reputation and maintaining customer and partner trust					
5	Ensuring compliance with cybersecurity laws and regulations					

----------The questionnaire has ended----------

Appendix 3: Names of the Evaluators

No.	Name of Evaluator	Academic Degree	Specialization	Workplace
1	**Dr. Mohammed Ahmed Saeed Basanbal**	PhD	Accounting	Head of Auditing – Central Organization for Control and Auditing, Mukalla Branch
2	**Dr. Nawal Salem Saleh Baqatian**	Assistant Professor	Management and Planning	Office of Education
3	**Dr. Shatha Shafeeq Mohsen Ata'a**	PhD	Business Administration / Human Resources	Director General of Administrative Affairs and General Department of Secretariat and Documentation – Central Organization
4	**Prof. Abdulraqib Al-Samawi**	Professor	Educational Administration and Supervision	Member of the Academic Accreditation Council – Ministry of Higher Education, Yemen