DOI: 10.15849/IJASCA.241130.13

Int. J. Advance Soft Compu. Appl, Vol. 16, No. 3, November 2024
Print ISSN: 2710-1274, Online ISSN: 2074-8523

The Role of Governance Supported by Cybersecurity in Reducing Financial and Administrative Corruption in Public Institutions in Jordan

Mohmmad Husien Almajali[1], Ahmad Ghazi Alshanty[2], Osaid hasan althnaibat[3], Medyen Jamal ALmahasnah[4]

[1]Faculty of Law, Al-Zaytoonah University of Jordan, Jordan.
[2]Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan, Jordan.
[3]College of Law, Mutah University, Jordan
[4]Faculty of Law, Department of Law, Isra University, Amman 33, Jordan

Abstract

Administrative and financial corruption constitutes one of the most important challenges that face public institutions, especially in developing countries such as Jordan.It negatively affects their reputation towards people that they control over ways which may lead to erosion and cessation of legitimacy. Such issue has even been exacerbated with the propagation of e-government initiatives as well as ICT-based public services. In the fight against corruption, effective governance with a focus on transparency and accountability are critical in tandem with adherence to the rule of law. Jordan anti-corruption activities here range from institutional reform to capacity building and enforcement of anticorruption measures. This article takes a closer look at how governance, supported by cyber security mechanisms is able to reduce corruption within the public sector in Jordan. It checks if auditors are aware of contemporary control systems and evaluates the influence cybersecurity has on improving internal controls and audit activities. This reveals the endemic corruption in Jordan and identifies some of the root causes: weak internal controls, deficient accounting systems, inadequate penalties, low salaries and waste. These findings are valuable for academics, public sector managers and policy makers.

Keywords: ***Corruption, E-government, Cybersecurity, Governance, Law.***

Received 5 August 2024; Accepted 5 November 2024

1. Introduction

Corruption, at its core, denotes a deviation from righteousness and moderation, entailing deterioration, harm, disorder, imbalance, and disadvantage. Administrative and financial corruption, specifically, involves the misuse of institutional power to serve personal, self-interested objectives. Within institutional frameworks, the exercise of such power is typically sanctioned for specific purposes and within defined boundaries (Almahasnah et al., 2024). Administrative or financial corruption arises when individuals entrusted with authority overstep these boundaries for personal gain (Lagarde, 2017). The International Monetary Fund characterizes administrative corruption as the abuse of public authority for private benefit, typically involving the acceptance, solicitation, or extortion of bribes. Similarly, the International Bank for Reconstruction and Development defines corruption as the exploitation of public office for personal advantage. Transparency International expands this definition to include the distortion of political, legal, administrative, or economic authority. However, the most broadly accepted definition describes corruption as the abuse of public power for private or personal gain (Al-Faryan&Shil, 2023).

The vast majority of corruption perception indices, such as Transparency International's Corruption Perception Index (CPI), the World Economic Forum's Global Competitiveness Index featured in its Global Competitiveness Reports, the International Country Risk Group (ICRG) index by the Political Risk Services Group, and the World Governance Indicators compiled by the World Bank, adhere to the same definition: the misuse of public office for personal gain. These indices aim to assess the conduct of all public office holders, including government officials and politicians (Handoyo, 2023).

Corruption is a longstanding issue not confined to any particular era or location but has persisted throughout history. Corruption has a devastating impact across the world. It is estimated by the World Bank that every year, between US$20 to US$40 billion are lost from developing countries due to corruption and bribery (UNODC,2024). Jordan grapples with significant administrative and financial corruption, particularly exacerbated in the post-2003 period. In 2023, Jordan ranked fourth in the Arab world and 63rd globally out of 180 countries on the CPI, as reported by Transparency International (the Jordan times), as shown in Fig.1 (World Bank, 2023).

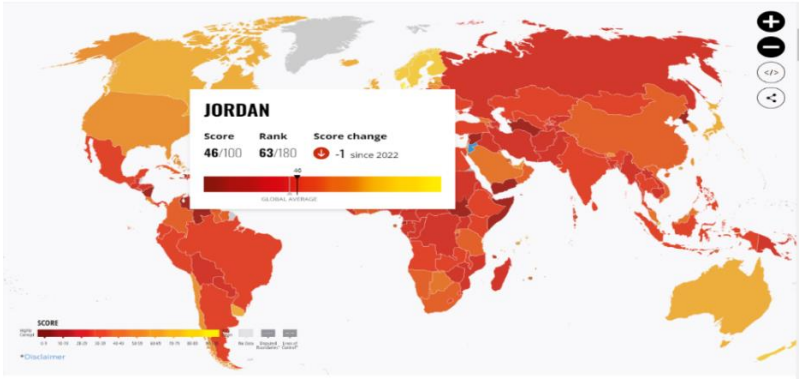

Fig.1: Transparency international

Based on the Transparency International, the CPI is the most widely used global corruption ranking in the world. It measures how corrupt each country's public sector is perceived to be, according to experts and businesspeople. The 2023 CPI shows that corruption is thriving across the world. The CPI ranks 180 countries and territories around the globe by their perceived levels of public sector corruption, scoring on a scale of 0 (highly corrupt) to 100 (very clean) as shown in Fig.2 (Koeswayo, et al., 2024).

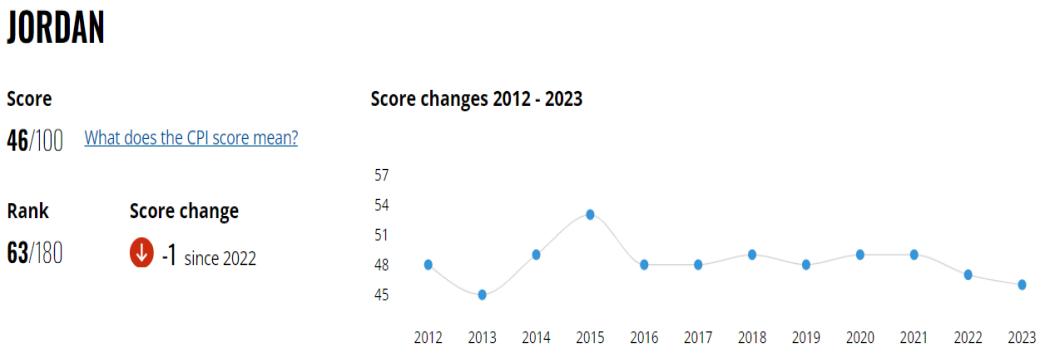

Fig2. Summary of the CPI for Jordan from 2012–2023 source: TI (https://www.transparency.org/en/cpi/2023/index/jor)

Figure 3 shows the level of public sector corruption based on a report released by Transparency international in 2023. As mentioned earlier, it measures how each country's public sector is corrupt (Makarenko, 2023).

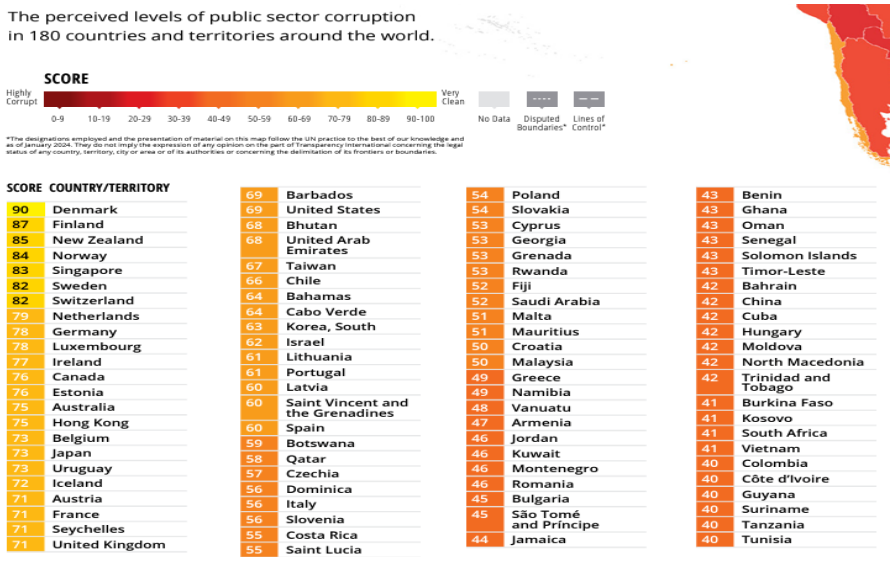

Fig3: The level of public sector corruption in many countries

However, there are many causes of corruption that vary among organizations, individuals, and countries. Three main groups of causes of corruption can be

identified as Firstly, personal factors: These factors stem from the inherent traits of an individual's character, shaped by their moral values. These values are typically instilled in individuals by their societal surroundings, influenced by customs and traditions (Yap et al, 2022). Greed and other psychological disorders represent inherent personal causes, often influenced by the individual's environment. Such traits may lead individuals to engage in unethical behavior. Several studies have established correlations between corruption offenses and certain personal attributes of the perpetrators. Secondly, organizational factors: An organization can significantly contribute to the prevalence of corruption. Senior management may act as a primary catalyst for corruption by:

A. Formulating strategies and policies that prioritize specific groups or personal interests, both within and outside the organization.
B. Making decisions that undermine the long-term sustainability and success of the organization.
C. Allowing loopholes in laws and regulations that facilitate corrupt practices.
D. Appointing leader who are ill suited for their roles.
E. Hiring employees based on factors other than merit, such as nepotism or shared interests, and placing them in positions without appropriate qualifications, fostering a culture of favoritism.

These factors collectively lead to poor decision-making and policy formulation that deviate from the organization's core objectives. Corruption becomes ingrained in the organizational culture, resulting in the emergence of informal communication networks and structures that undermine the formal organizational hierarchy. Consequently, this erodes the effectiveness of other essential organizational tools. Furthermore, environmental factors lie in the opportunities created for individuals to engage in administrative and financial corruption. Economic factors also stand out as significant contributors to the proliferation of administrative corruption. Inadequate individual incomes and low standards of living often result from government neglect in regulating wage structures. Additionally, disparities in the distribution of national resources may lead to injustice. The inability to balance between basic living needs and wage levels incentivizes certain individuals in order to seek supplementary income through illicit means (Campbell, 2015).

The concept in question may encompass ethical guidelines, legal statutes, or administrative protocols. Both the World Bank and Transparency International characterize corruption as "the misuse of entrusted authority for personal benefit." This definition enjoys widespread international consensus, assuming the existence of a regulatory framework delineating permissible administrative conduct. Any administrative action contravening these regulations for personal gain is classified as an instance of administrative corruption. Clarity and inclusivity are crucial for this definition to be comprehensive. The interpretation of corruption within a society is relative and contingent upon its prevailing value system (Pozsgai-Alvarez, 2020).

However, there is no interest in an effective and proper auditing process or in conducting training courses for internal audit management staff in public institutions by programmers or experienced personnel. One of the main reasons for the weakness of internal accounting and auditing systems in Jordanian public institutions is that the internal audit system does not have a high level of efficiency and effectiveness (Elmanaseer, 2023), and the internal audit management staff do not have sufficient qualifications and skills to do their job, and accounting information systems are not reliable (Abdulhussein et al., 2023). This is especially true with the absence of secure information systems, which can be offered by various cybersecurity techniques. Weak internal accounting and auditing systems lead to the inability of the internal audit department to protect public resources from corruption, fraud, and the illegal misuse of public property. There is a strong relationship between the internal audit function and corruption in the sense that whenever the audit function is exercised independently and without bias, the improved internal audit process makes it easier for auditors to uncover practices that have not yet been recognized, leading to reduced corruption (Kontogeorgis, 2018).

The fusion of various information and communications technologies (ICTs) has offered faster and more reliable communication, efficient and economical storage, retrieval, and processing of data, and the exchange and utilization of information to its users, be they individuals, groups, businesses, organizations, or governments. Most importantly, many governments, too, have realized the benefits of computerization, internet connectivity, and web enablement, and have ventured into process re-engineering, promising services to citizens and businesses anytime, anywhere. Furthermore, e-governance is a widely celebrated concept today, and its popularity is understandable. It can be applied in all government reforms and activities (Mountasser & Abdellatif, 2023).

The effectiveness of electronic government (e-government) depends on sound, reliable, and well-articulated electronic governance. E-governance is the tool for effective e-government. The delivery of public services in Jordan is underpinned by the principle of continuity and guaranteed data protection, which imposes greater responsibilities on the state as it moves toward becoming a digital country. This has created the necessity to gain a deeper understanding of cybersecurity challenges and to develop strategies for providing better e-governance and achieving digital sovereignty. Therefore, there is a demand to assess the level of public confidence and trust in the integrity of the systems and data exchanged on the e-governance platform, as well as the ability to use cybersecurity tools for mitigating risks and ensuring employee compliance by enhancing internal auditing within the institution itself (El Khatib & Al Harmoodi, 2024).

Weak oversight, lack of accountability, and low levels of transparency are some of the most important factors that create an environment conducive to the spread and growth of corruption. There is no doubt that the fight against corruption and efforts to curb its spread require the concerted efforts of many parties, especially regulatory bodies, with the most important being the higher oversight bodies, which are positioned to contribute significantly to anti-corruption efforts if their roles are

activated and they are equipped with the necessary resources and capabilities. Internal auditors perform important functions within public institutions, including enhancing the fight against fraud, improving credibility and reliability, treating government officials equally, taking care to guard against the risks of government corruption, and working to stop it. Corruption erodes respect for the law and deters honest people from entering public service. To counteract this, anti-corruption measures for compliance and good governance are essential (Erkkilä, 2020).

Under these circumstances, a new process of governing or a changed condition of ordered rule has emerged, known as good governance. Governance is a term that continues to expand and develop. In the past two decades, its current definition has evolved to signify cooperation among three active and participatory institutional stakeholders: the state, civil society, and the private sector, which jointly manage the country's affairs. It represents a system of control and guidance at the institutional level, defining the responsibilities, rights, and relationships of all involved groups and explaining the necessary rules and procedures for making rational decisions related to the organization's work. It is a system that supports justice, transparency, and accountability within institutions and enhances trust and credibility in the work environment. Governance also involves the traditions and institutions by which authority in a country is exercised. This includes (1) the process by which governments are selected, monitored, and replaced; (2) the government's capacity to effectively formulate and implement sound policies; and (3) the respect of citizens and the state for the institutions that govern economic and social interactions among them (Denters et al., 2023).

A compliance audit is considered an independent evaluation of adherence to applicable standards, including laws, regulations, and principles of financial and administrative management or discipline for the entity subject to audit. Administrative and financial corruption consists of dishonest acts carried out by people who occupy positions of authority, such as managers, government officials, and others, to achieve private gains. Examples of corruption phenomena include giving and accepting bribes, improper gifts, illegal political transactions, fraud or deception, tampering with election results, money transfer fraud, money laundering, and more. Target users may wish to have confidence in the credibility of the information available to them and its relevance to the decision-making process (Chari, 2023). Therefore, auditors should provide users with information based on sufficient and appropriate evidence by using cybersecurity tools, which play a significant role in activating governance in Jordanian public institutions.

This research aims to provide a conceptual framework for auditing compliance and a mechanism for combating administrative and financial corruption by enhancing governance with cybersecurity. It explains the most important observations and reservations contained in compliance audit reports that can be obtained through cybersecurity techniques and their role in combating administrative and financial corruption.

In an era marked by increasing digitalization, public institutions worldwide face escalating challenges in safeguarding sensitive information and ensuring transparent

governance. Jordan, like many nations, grapples with the imperative of bolstering cybersecurity measures to fortify governance structures and enhance internal auditing processes within its public sector (Almajali et al., 2023). This article explores the pivotal role of cybersecurity techniques in advancing governance and internal auditing practices in Jordanian public institutions.

The rest of this study is organized as follows: section 2 presents background, Section 3 describes the literature review. Section 4 shows the proposed model, Section 5 provides recommendations, and finally Sections 6 concludes the study.

2. Background

Governance and transparency seek to combat administrative corruption in various state institutions by presenting the government with challenges related to improving levels of development across multiple dimensions. According to Al-Shalfan (2021), corruption in some countries now exhibits a systematic nature, making it the rule rather than the exception; whereas the principle should be transparency and integrity, corruption has become the norm (Yaacoub et al., 2023). Therefore, the significance of governance lies in providing an organizational structure that enables public organizations and institutions to achieve their objectives efficiently. Furthermore, the importance of governance is also evident in the implementation of control mechanisms and self-supervision in enforcing regulations and instructions, which contributes to reducing corruption and highlighting deficiencies and weaknesses in institutional work (Al-Asmar, 2020).

To determine the role of governance in combating administrative corruption in its various forms and the extent to which cybersecurity impacts it, it is crucial to clarify the concept of governance, the concept of cybersecurity, and the concepts of administrative and financial corruption, as well as the legal framework for accountability associated with administrative and financial corruption, and the impact of cybersecurity on addressing these issues.

Governance is defined as "the exercise of economic, political, and administrative authority to manage state affairs at all levels, including the processes, mechanisms, and institutions used by citizens and groups to express their interests, exercise their legal rights, fulfill their obligations, and engage in mediation to resolve their disputes" (Basim, 2019). Conversely, Haddad (2008) defines it as achieving transparency, independence, justice, and integrity as guarantees against corruption and mismanagement. Similarly, as stated by Youssef (2007), governance is a system of control and direction at the institutional level that defines the responsibilities, rights, and relationships of all designated groups and clarifies the rules and procedures necessary for making rational decisions regarding the work of the organization. It is also a system that supports justice, transparency, and institutional accountability while enhancing trust and credibility in the work environment (Gharaibeh et al., 2023).

As derived from the previous definitions, these concepts align with an institutional and organizational framework that contributes to implementing the

provisions of the law and enforcing accountability for institutional and organizational actions, thus enhancing institutional activities to achieve their goals effectively and meet the needs and desires of the communities they serve. Applying these definitions creates what is known as "good governance" within a legal environment that upholds the provisions of the law and fosters transparency and integrity (Al-Wakeel, 2021). Consequently, a new term, "anti-corruption governance," has emerged, aimed at establishing "good governance" by verifying the implementation of legal provisions and combating corruption through specialized bodies.

Locally, within Jordanian legislation, it is evident that the Jordanian legislator has adopted this system through the Integrity and Anti-Corruption Law No. 13 of 2016 and its amendments in Article 4(c), which stipulates that "one of the most important obligations of the Integrity and Anti-Corruption Commission is to ensure that public administration adheres to the principles of good governance and standards of equality, merit, entitlement, and equal opportunities, along with the other functions held by that Commission in combating financial and administrative corruption and implementing oversight frameworks for institutions and individuals." Accordingly, the term governance is not limited to a specific domain; it is a system that subject's institutions and organizations to provisions aimed at ensuring the correct and sound application of the law and promotes systems of integrity, transparency, oversight, and accountability to support effective institutional work and hold accountable those who violate these standards (Nai et al., 2023).

Cybersecurity refers to protecting assets through information technology, such as hardware and software, by implementing various necessary measures to protect cyberspace from cyber attacks (Alzubi et al., 2024 and Ala'M et al., 2023). This is achieved through technical, organizational, and administrative means that prevent unauthorized access to electronic information and prevent its illegal exploitation. Such protection contributes to maintaining the continuity of systems and the security of the information they contain, as well as safeguarding their privacy through various methods, measures, and software (Al-Samhan, 2020). Cybersecurity encompasses cyberspace, regarded as a key element. Cyberspace is the communication space within the information environment (IE) formed through the global networking of automated digital data processing equipment, constituting a modern interactive environment that includes both tangible and intangible elements.

Cybersecurity also includes a combination of digital devices, network systems, software, and their users, whether operators or end-users. The primary security function focuses on achieving cyber-deterrence by preventing harmful actions against networks or systems, especially those undermining the capabilities and functions of a computer network for national or political purposes or exploiting weaknesses in digital systems (Al-Samhan, 2020). Accordingly, cybercrime encompasses acts arising from the use of modern digital and electronic means, such as computers and the Internet, in criminal activity to gain large financial returns via online transactions, stock trading, or commercial activities involving confidential information, and represents any illegal act related to the automated processing or transfer of information (Abdullah, 2007).

Given the development of the concept of civil and criminal protection for information security against infringement, violation, unauthorized access, or illegal use, the Jordanian legislator, in response to the evolving concept of crime on the one hand, and protection in both its civil and criminal aspects on the other, has moved to enact the necessary legislation to combat associated harms. The legislator has enacted the Cybercrime Law No. 17 of 2023 and the Personal Data Protection Law No. 24 of 2023, in addition to provisions in the Penal Code No. 16 of 1960 and its amendments. These laws and regulations govern the nature of actions considered criminal based on their legal description, the extent of legal protection for information against infringement, and the associated consequences (Graves &Acquisti, 2023).

Administrative corruption is defined as the abuse of public authority or public office for private gain at the expense of the public interest. This definition implies deviant and abnormal behavior where an individual or group exploits their position or authority to violate laws and regulations in order to obtain private benefits at the expense of the public interest (Joma, 2018; Sayed-Ali, 2020). Accordingly, the Jordanian legislator specifies in Article 16(a)(5) of the Integrity and Anti-Corruption Law that financial corruption is "every act that leads to the waste of public funds or the funds of public joint-stock companies, non-profit companies, or associations" (Integrity and Anti-Corruption Law, 2016).

In terms of economic impact, some scholars and researchers argue that governance contributes to evaluating the performance of senior management, enhancing accountability and responsibility, and combating administrative and financial corruption, which promotes justice and transparency (Alflaieh, 2022). Governance provides appropriate mechanisms for evaluating and correcting policies, addressing abuses of power and influence, preventing the waste of public funds, and holding negligent individuals accountable (Tashtoush, 2014).

Thus, implementing the rules of governance and subjecting administrative and institutional work to the provisions of the law on the one hand, and information systems and electronic archiving—that is, digital access to institutional work—could reduce illegal behaviors such as wasting public money and brokerage work in projects, whether through embezzlement, job trading, forgery, or fraud, i.e., reducing the phenomenon of "abuse of power for private purposes" (Tuiti&Khaira, 2019).

In the 2016 Integrity and Anti-Corruption Law, the Jordanian legislator stated that among the duties of the body formed according to its provisions are to ensure that public administration adheres to the principles of good governance and the standards of equality, merit, entitlement, and equal opportunities; to investigate financial and administrative corruption in all its forms; to detect violations and abuses; to collect evidence and information; to initiate investigations and carry out the necessary administrative and legal procedures; and to ensure that private sector oversight institutions and civil society organizations set standards for good governance and ensure their proper application.

As interpreted from Article 4, the explanatory decision issued by the Jordanian Constitutional Court No. 5/2018 on March 15, 2018, clarified the acts of corruption and the necessity for state agencies to take legislative and other measures

to criminalize the following acts, as they fall within crimes and acts of corruption, including the abuse of public positions, bribery, laundering of criminal proceeds, and embezzlement.

Accountability is achieved by ensuring the presence of a legal framework that regulates the accountability of officials and decision-makers in the public administration and their obligation to uphold the administration's commitment to applying the principles of transparency according to Article 15 of the Integrity and Anti-Corruption Law. Article 15 of this law stipulates that the public administration is committed to applying the principles of transparency and values of openness and disclosure in performing its organizational and procedural tasks and employing its personnel in its internal and external relations and contracts. The law also stipulates that the public administration must provide a special portal for public information that is available to citizens, in accordance with the provisions of relevant legislation.

Now that responsibility arises when the members of the Commission exercise the status of "judicial police" granted to them under Article 19 of the Integrity and Anti-Corruption Law, in the event of detecting any corruption crimes, they must refer the perpetrator of the act to the Public Prosecution, issue a decision regarding it in terms of accusation or suspicion, and refer the papers to the competent court to decide on the matter. They must also exercise their discretionary authority to monitor the work of the administration, assess its legitimacy and the presence of its elements, verify its controls, and study its implications (See Jordanian Administrative Court Decision 171/2020 on January 27, 2021, & the previous Jordanian Court of Justice ruling 362/1999 on January 24, 2000).

Cybersecurity enhances the confidence and resilience of the government, critical national infrastructure, business sectors, and the public to confront and respond to cyber threats by disseminating the necessary policies and procedures to establish a unified national methodology for cybersecurity and by establishing an appropriate governance model and institutions that ensure effective cybersecurity (Dotsenko et al., 2022). Other key methods for responding to cyber threats include building the institutional structure necessary to develop and operate national cybersecurity, providing a unified source of advice at the government level to address intelligence threats and verify information, and preparing specialized programs to spread awareness and build capabilities in the field of cybersecurity (Cybersecurity at the Media Authority, Department of Studies, Communication and Public Relations in the Hashemite Kingdom of Jordan, 2021).

Governance is one of the most significant and necessary mechanisms to reduce financial and administrative corruption by ensuring the proper functioning of bodies and companies and verifying the integrity of management, as well as the commitment to fulfill obligations and pledges in the public and private sectors in a legal and economically sound manner (Towaiti & Khaira, 2019). The quality of legislation and its application is verified by studying indicators of the government's ability to formulate and implement effective policies and regulations that support development in various sectors, assessing indicators of the government's desire to create an attractive investment environment for national and international investors,

and determining the impact of implementing technology in the aforementioned aspects and on data protection (Al-Bashir &Mitani, 2016).

On the other hand, governance contributes to using corruption perception indicators through data sources from independent institutions specialized in analyzing the government work environment, as the sources of information used in the corruption perception index are based on data collected over specific periods and a review of the extent of systematic transparency and the degree to which quality standards are met (Al-Shalfan, 2021). Given the previous analysis, it can be concluded that governance today is different from the past, especially in light of technical and technological development and the advancements in management information systems used in administrative agencies and institutions.

Entrusting these programs with specific legislative, technical, and technological controls makes them a weapon in the fight against administrative and financial corruption that many countries suffer from, especially since they are considered programmed systems that can only be manipulated by people with high skills in handling them and their software. Although these systems do not completely address administrative and financial corruption, they have—at least—limited its scope and severity. Furthermore, the legislative aspect of protecting data and information, along with tightening and increasing the penalties imposed for committing illegal acts, helps achieve general and specific deterrence in a manner that distances individuals, whether users or employees, from committing those illegal acts due to civil and criminal liability, as well as the disciplinary responsibility of public employees.

Notably, judicial oversight of administrative work becomes easier and more flexible in the case of digital oversight through the principles of transparency and integrity, in addition to oversight of the core of administrative work itself. In other words, it is the control of the legality of administrative work, which pertains to administrative decisions and physical activities related to public facilities.

Cybersecurity as a Foundation for Governance

Governance pertains to efficiency, transparency, and accountability. In fact, cybersecurity in Jordan constitutes a fundamental element in ensuring the implementation of these principles by protecting cyber assets from information infiltration, unauthorized access, and other types of cyber threats. Jordanian public institutions can secure sensitive data and uphold the integrity of governance processes by implementing robust cybersecurity measures such as encryption protocols, access controls, and intrusion detection systems (Al-Ma'aitah, 2022).

Enhancing Internal Auditing Through Cybersecurity

The role of internal auditing is closely related to the overall governance structures and public sector standards that apply across jurisdictions. Cybersecurity techniques have been shown to supplement internal auditing in Jordan by enabling real-time

monitoring, detection of anomalies, and prompting responses to potential risks to the integrity of the organization. Internal auditors can leverage advanced cybersecurity tools and technologies to perform comprehensive penetration testing of an entire digital infrastructure, identify weaknesses within the overall structure, and provide recommendations on mitigation to strengthen governance frameworks (Alqudah et al., 2023).

Mitigating Risks and Ensuring Compliance

Cybersecurity techniques are critical for mitigating the risk of fraud by protecting against data breaches and detecting unauthorized access to sensitive information. Jordanian public institutions should implement comprehensive cybersecurity processes that ensure regulatory compliance, secure financial transactions, and protect sensitive information from unauthorized access. In addition, cybersecurity measures enable public institutions to respond swiftly when new cyber risks emerge, minimizing their impact on governance processes and internal auditing activities (Salem & Al-Sayyed, 2022).

Building Trust and Resilience

A strong cybersecurity posture increases public trust between citizens and their government and strengthens societies against future cyber threats. Jordan embracing cybersecurity practices reflects transparency, accountability, and good governance. Investing in cybersecurity awareness and capacity-building programs can play a crucial role in raising the capacity of Jordanian public institutions by empowering personnel to identify and manage cyber risks, thus enhancing the overall resilience of governance structures and internal audit mechanisms (Almaiah & Nasereddin, 2020).

Cybersecurity technologies significantly enhance the effectiveness of governance and internal audit functions in public organizations in Jordan. Cybersecurity is the nexus of sound governance: by protecting digital assets, reducing cyber risks, and adhering to regulatory requirements, it ensures transparent, responsible, and durable governance. Amidst the evolving challenges of the digital era, equipping governance frameworks and internal auditing processes through robust cybersecurity is essential to safeguarding both institutional integrity and public confidence in government systems. By adopting proactive steps in the field of cybersecurity, Jordan can pave the way for a public sector that is more secure, resilient, and transparent — promoting sustainable development and fostering national prosperity.

An overview of the major functions of cybersecurity to improve governance and internal auditing in public institutions in Jordan is presented in Table 1. The following graphic provides a summary of its potential benefits, including the security of sensitive data, improved auditability, risk mitigation, and public trust. These findings underscore the necessity of strong cybersecurity in governance systems to safeguard transparency, accountability, and resilience.

Table 1: Overview of Cybersecurity's Role in Enhancing Governance and Internal Auditing Practices in Jordanian Public Institutions.

#	Cybersecurity Aspect	Key Features	Outcome
1	Foundation for Governance	Protects cyber assets from threats, ensures transparency, efficiency, and accountability with measures like encryption, access control, and intrusion detection.	Secures sensitive data and governance integrity.
2	Enhancing Internal Auditing	Enables real-time monitoring, anomaly detection, and mitigation strategies; supports comprehensive assessments of digital infrastructure for internal audits.	Improves auditing effectiveness and governance frameworks.
3	Mitigating Risks and Ensuring Compliance	Prevents data breaches and fraud; ensures regulatory compliance and protects sensitive data while facilitating swift responses to emerging cyber risks.	Minimizes fraud risks and maintains governance processes.
4	Building Trust and Resilience	Strengthens public trust, enhances resilience, and empowers personnel through awareness programs; promotes transparency and good governance.	Fosters a secure, transparent, and resilient public sector.

3. Literature review

As highlighted in the literature reviewed, the findings indicate that cybersecurity techniques play an important role in improving governance and internal auditing practices within Jordanian public institutions. Cybersecurity serves as an enabler of good governance by protecting digital assets, lowering cyber risk, and encouraging transparency and accountability. Amidst the challenges, there remain ample opportunities for innovative collaboration to position cybersecurity as a governance pillar in Jordan. Policies, practitioners, and researchers should continue their efforts to ensure that cybersecurity actions are a top priority for the sustainability of both Jordan's public institutions and institutional structures globally.

Cybersecurity initiatives in governance capability build the overarching structure of government as they address the integrity, confidentiality, and availability of digitally structured assets in public institutions. Cybersecurity is vital for safeguarding public confidence, providing transparency, and reducing fraud and data breaches (Alawneh& Al-Qirim, 2020). Secure governance structures in Jordanian

public institutions are bolstered when cybersecurity protects sensitive information and deters powerful hacking tools from obtaining unauthorized access.

Cybersecurity-related efforts are incorporated as a tool for internal audit processes to assess the effectiveness of governance frameworks and compliance with regulatory standards. According to Al-Momani et al. and Ezzat et al. (2019), with the help of cybersecurity, internal auditors can respond at a high level because they have the ability to monitor and detect any cyber threats in real time. This allows auditors to perform a comprehensive assessment of digital infrastructure, recognize exploitable weaknesses, and propose corrective measures that enhance governance controls.
Although all of these techniques have great advantages, there are numerous obstacles to implementing them in public institutions in Jordan. A recent paper by Alrawashdeh and Al-Azzam (2021) identifies financial issues, such as a lack of awareness and limited resources available for developing the necessary skill sets, as major obstacles to effective cybersecurity implementation. Additionally, the rapid changes in cyber threats mean that cybersecurity infrastructure and processes require continuous high levels of investment and effort.

However, there are also innovative and collaborative opportunities to strengthen cybersecurity governance. Al-Zoubi et al. and Piotrowski et al. (2020) highlight the need for informal and formal public-private partnerships as well as knowledge-sharing initiatives that are crucial in addressing cybersecurity challenges and building resilience in Jordanian public institutions. Finally, an overview of the related work section is included in Table 2.

Table 2: Summary of Related Work on Cybersecurity's Role in Governance and Internal Auditing within Jordanian Public Institutions

Authors	Focus	Key Points	Challenges/Opportunities
Alawneh& Al-Qirim (2020)	Role of cybersecurity in governance	Cybersecurity is foundational for ensuring integrity, confidentiality, and availability of digital assets; it helps in preserving public trust and transparency	N/A
Al-Momani et al. (2019)	Cybersecurity in internal auditing	Cybersecurity enhances internal auditing by real-time threat monitoring; supports assessment of vulnerabilities and compliance with regulatory standards	N/A
Alrawashdeh& Al-Azzam (2021)	Challenges in cybersecurity implementation	Highlights lack of awareness and resources as barriers to effective cybersecurity in Jordanian public institutions	Need for continuous adaptation and investment
Al-Zoubi et al. (2020)	Opportunities for strengthening cybersecurity through collaboration	Emphasizes public-private partnerships and knowledge-sharing initiatives to enhance resilience in public institutions	Innovation and collaboration opportunities

4. Proposed model

This model shows that cyber-secure-backed governance can be a holistic approach to combating financial and administrative corruption in Jordanian public institutions. As shown in Figure 4, safeguarding governance frameworks against cybersecurity corruption can only be addressed if public institutions mainstream such measures within their organization's processes and promote stakeholder engagement to enhance transparency, accountability, and integrity.

Description of the proposed Model:

Governance Framework:

At the core of the model is the governance framework, representing the principles, policies, and practices governing public institutions in Jordan.

Cybersecurity Integration:

Surrounding the governance framework is a layer representing cybersecurity integration, illustrating the incorporation of cybersecurity measures into governance structures.

Cybersecurity Techniques:

The cybersecurity integration layer includes multiple cybersecurity controls and approaches, such as access control and data encryption, as well as threat monitoring and incident response.

Reducing Corruption:

The overarching goal of the model is depicted at the top, illustrating the objective of reducing financial and administrative corruption in public institutions.

Feedback Loop:

Arrows indicate a feedback loop between governance and cybersecurity, highlighting the continuous interaction and reinforcement between the two domains. Governance practices inform cybersecurity measures, while cybersecurity measures enhance governance integrity.

Stakeholder Involvement:

Outside the model, in this silo example, stakeholders such as policymakers, government officials, cybersecurity professionals, and members of the public operate through any established international or national channels. The stakeholders listed all have an important role to play in the implementation and sustainability of the model.

Continuous Improvement:

This model emphasizes that organizations should constantly adapt and improve their strategies for addressing ever-changing cyber threats and corruption.

Fig.4. The proposed Model

5. Recommendations

Data Integrity and Transparency: Cybersecurity helps protect sensitive data in public institutions. It fosters accountability and transparency in governance processes by protecting financial and administrative records from unauthorized access, manipulation, or tampering. This safeguards against malpractices such as embezzlement, fraud, or bribery because tampering with records becomes difficult without detection.

Preserving Security for Cyber Transactions and Payments: Cybersecurity contributes to preserving financial transactions and payment systems against cyber threats such as hacking, phishing, or malware attacks. Governance supported by cybersecurity prevents the illegal siphoning of funds or their diversion to offshore accounts for corrupt practices by safeguarding online banking systems and other digital financial channels, such as e-procurement platforms.

Compliance and Regulation Enforcement: Cybersecurity governance includes regulatory frameworks and standards to ensure compliance with laws and regulations

pertaining to all financial and administrative practices. Cybersecurity supports the implementation of anti-corruption legislation and compliance requirements, thereby opposing corrupt behavior and sanctioning individuals or organizations for violations.

Risk Assessment and Management: Cybersecurity approaches include risk assessment and management best practices that identify weaknesses within financial and administrative systems, elements that represent potential threats. Governance supported by cybersecurity reduces the risk of fraudulent activities and corruption schemes in public institutions by proactively mitigating security risks and vulnerabilities.

Increased Accountability and Monitoring: Cybersecurity technologies, such as audit trails, access controls, and surveillance systems, assist in improved monitoring of financial and administrative activities within public institutions. Cybersecurity-supported governance offers real-time visibility into transactions and operations, allowing authorities to identify and respond rapidly to suspicious activity while deterring corrupt practices and enforcing accountability among employees and officials.

Capacity Building and Awareness: A cybersecurity governance approach should be comprehensive enough to build institutional capacity and awareness among stakeholders regarding cyber threats and best practices for risk mitigation. Governance initiatives can also create awareness among employees, officials, and the public about how cybersecurity combats corruption. This, in turn, contributes to an environment of alertness and accountability that hinders corrupt individuals from exploiting existing loopholes within public institutions.

Table 3 specifies the most important steps to take—protecting sensitive data, ensuring regulatory compliance, and improving monitoring. These steps help create a transparent ecosystem, reduce risks, and foster a proactive culture of accountability. This enables public institutions to combat fraud and corruption effectively while maintaining public trust over time by addressing these critical areas.

Table 3: Summarized Cybersecurity Recommendations for Improving Governance and Auditing in Jordanian Public Institutions

#	Recommendation	Key Actions	Expected Outcomes
1	Data Integrity and Transparency	Protect data and records from unauthorized access and tampering.	Prevent fraud and ensure transparency.
2	Secure Financial Transactions	Safeguard financial systems from cyber threats.	Protect funds from misuse.
3	Regulatory Compliance	Enforce compliance with regulations and anti-corruption laws.	Promote adherence to standards and reduce violations.
4	Risk Management	Identify and mitigate security vulnerabilities.	Minimize fraud and corruption risks.
5	Enhanced Monitoring	Enable real-time monitoring and rapid response.	Enhance accountability and deter corruption.
6	Capacity Building	Raise awareness and build institutional capacity.	Foster a proactive cybersecurity culture.

6. Conclusion

Ultimately, governance supported by cybersecurity is one of the key cornerstones in combating both financial and administrative corruption in the public sector of Jordan. Cybersecurity makes governance frameworks more effective by promoting transparency, accountability, compliance, risk management, and oversight. By incorporating stringent cybersecurity protocols into these strategic plans, institutional resilience to corruption can be strengthened, complemented by a culture of ethical behavior and legal compliance. Moreover, cybersecurity-supported, code-based governance discourages illegal behaviors and aligns with the rule of law by ensuring compliance with applicable laws and regulations, thereby reducing legal risks (e.g., lawsuits) for governments and increasing citizens' trust (Bastos, 2023a). These endeavors are vital for preserving the integrity and reputation of public institutions, ensuring they remain relevant in serving the common good.

References

[1] ALmahasnah, M. J., Almajali, M. H., Althunibat, A., Abuaisheh, B. N., Alqudah, F. T., & Ghazwi, M. F. (2024). The role of anti-corruption legislation in sustainable development. Journal of Infrastructure, Policy and Development, 8(10), 5611.

[2] Lagarde, C. (2017). Addressing corruption with clarity. Speech at the Brookings Institution.

[3] Al-Faryan, M. A. S., &Shil, N. C. (2023). Governance as an interplay between corruption and polity: Conceptualizing from a national perspective. Economies, 11(2), 65. Ala'M, A. Z., Mora, A. M., &Faris, H. (2023). A multilingual spam reviews detection based on pre-trained word embedding and weighted swarm support vector machines. IEEE Access.

[4] Alzubi, O. A., Alzubi, J. A., Qiqieh, I., & Al-Zoubi, A. M. (2024). An IoT Intrusion Detection Approach Based on Salp Swarm and Artificial Neural Network. International Journal of Network Management, e2296.

[5] Handoyo, S. (2023). Worldwide governance indicators: Cross country data set 2012–2022. Data in Brief, 51, 109814.

[6] World Bank. (2023). Enhancing government effectiveness and transparency: The fight against corruption.

[7] Koeswayo, P. S., Handoyo, S., & Abdul Hasyir, D. (2024). Investigating the Relationship between Public Governance and the Corruption Perception Index. Cogent Social Sciences, 10(1), 2342513.

[8] Makarenko, I., &Brin, P. (2023). Methodological principles for assessing the transparency of energy companies of Ukraine. The Journal of VN KarazinKharkiv National University. Series: International Relations. Economics. Country Studies. Tourism, (17), 87-93.

[9] Yap, J. B. H., Lee, K. Y., Rose, T., &Skitmore, M. (2022). Corruption in the Malaysian construction industry: investigating effects, causes, and preventive measures. International Journal of Construction Management, 22(8), 1525-1536.

[10] Campbell, M. J. L. (2015). Organizational cultures' impact on employees' corruption (Doctoral dissertation, UniversitätWürzburg).

[11] Pozsgai-Alvarez, J. (2020). The abuse of entrusted power for private gain: Meaning, nature and theoretical evolution. Crime, Law and Social Change, 74(4), 433-455.

[12] Elmanaseer, S. (2023). Responsibility of Public Administration in Managing its Electronic Facilities. Al-Zaytoonah University of Jordan Journal for Legal studies, Volume (4), Issue (1), 2023

[13] Abdulhussein, A. S., Al-Refiay, H. A. N., &Wahhab, A. M. A. (2023). The Impact of Internal Auditing on Corruption: Evidence from the Emerging Market. Journal of Governance and Regulation/Volume, 12(1), 367-375.

[14] Kontogeorgis, G. (2018). The role of internal audit function on corporate governance and management. International Journal of Accounting and Financial Reporting, 8(4), 100-114.

[15] Mountasser, T., &Abdullatif, M. (2023). Digital Transformation in Public Administration: A Systematic Literature Review. International Journal of Professional Business Review, 8(10), e02372-e02372.

[16] El Khatib, M., & Al Harmoodi, S. (2024). E-governance in projects management: Models and approaches and disruptive technologies. International Journal of Business Analytics and Security (IJBAS), 4(2), 210-236.

[17] Erkkilä, T. (2020). Global governance indices as policy instruments: Actionability, transparency and comparative policy analysis. In Institutions and Governance in Comparative Policy Analysis Studies (pp. 433-453). Routledge.

[18] Denters, E., Ginther, K., & de Waart, P. J. (Eds.). (2023). Sustainable development and good governance. MartinusNijhoff Publishers.

[19] Chari, D. (2023). Risk Management Practices And Service Delivery In Local Authorities. A Case OfZvimba Rural District Council (Doctoral dissertation, Great Zimbabwe University).

[20] Almajali, M., Ghazwi, M., Alqudah, F., Almahasnah, M., Alajarmeh, H. H., &Masarweh, A. (2023). The legal aspects and the enhanced role of cybersecurity in protecting the electronic voting process in the context of Jordan Parliament election law no.(4) of 2022. Information Sciences Letters, 12(8), 2839-2848.

[21] Al-Shalfan, A. (2021). The role of governance and transparency in reducing administrative corruption. Arab Journal of Management, 41(2), 16-32.

[22] Yaacoub, J., Noura, H., Salman, O., &Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions, and recommendations. Internet of Things and Cyber-Physical Systems, 3(1), 280-308. https://doi.org/10.1016/j.iotcps.2023.04.002

[23] Al-Asmar, M. (2020). Degree of administrative governance practice at Umm Al-Qura University: A field study. Educational Journal, 70(1), 33-50.

[24] Basim, M. (2019). The role of governance in promoting integrity and combating corruption: An analytical study of the transparency index and the accountability and accountability index in the Kingdom of Saudi Arabia. Umm Al-Qura University Journal of Sharia Sciences, Law and Islamic Studies, 77(2), 20-32.

[25] Haddad, M. (2008). The role of corporate governance in economic development, research presented at the scientific conference on Corporate governance and its role in reform. Damascus University, Syria.

[26] Youssef, M. (2007). Governance Determinants and Standards, Cairo: National Investment Bank.

[27] Gharaibeh, A., Abu Ghazaleh, S., Alabady, H., & Al-Senussi, M. (2023). Administrative obligations for diplomatic missions in the context of international and national law: implications and challenges for cybercrime. International Journal of Cyber Criminology, 17(2), 147-174.

[28] Al-Wakeel, M. (2021). The impact of governance principles on job performance: An applied study on the East Nasr City Neighborhood. Arab Journal of Management, 41(4), 16-30.

[29] Nai, R., Meo, R., Morina, G., &Pasteris, P. (2023). Public tenders, complaints, machine learning, and recommender systems: A case study in public administration. Computer Law & Security Review, 51(2), 2-22. https://doi.org/10.1016/j.clsr.2023.105887.

[30] Personal Data Protection Law No. (24) of 2023.

[31] Al-Samhan, M. (2020). Requirements for achieving cybersecurity for management information systems at King Saud University. Journal of the College of Education, 111(1), 20-32.

[32] Abdullah, A. (2007). Information and Internet Crimes: Electronic Crimes, Beirut: Al-Halabi Human Rights Publications.

[33] Graves, J &Acquisti, A. (2023). An empirical analysis of sentencing of "Access to Information" computer crimes. Journal of Empirical Legal Studies, 20(2), 434-471. https://doi.org/10.1111/jels.12349

[34] Joma, M. (2018). The role of civil service and penal systems in combating administrative corruption in the Kingdom of Saudi Arabia. Contemporary Egypt Journal, 109(530), 21-35.

[35] Sayed-Ali, S. (2020). The impact of corruption and governance indicators on economic growth in Arab countries between (1996) and (2017). Entrepreneurship Journal of Business Economics, 6(2), 31-46.

[36] Integrity and Anti-Corruption Law No. (13) of 2016 and its amendments.

[37] Cybercrime Law No. (17) of 2023.

[38] Alflaieh, M. (2022). Electronic Fraud in the Context of E-Commerce under Jordanian Legislation. Al-Zaytoonah University of Jordan Journal for Legal studies, Volume (3), Issue (3), 2022

[39] Tashtoush, H. (2016). The role of good governance in achieving sustainable development. Journal of Law and Human Sciences, 1(1), 15-32.

[40] Tuiti, M &Khaira, M. (2019). Governance mechanisms to combat financial and administrative corruption in light of the principle of disclosure and transparency.Al-Maqrizi Journal of Economic and Financial Studies, 3(1), 20-32.

[41] Dotsenko, S., Illiashenko, O., Kharchenko, V., &Morozova, O. (2022). Integrated Information Model of an Enterprise and Cybersecurity Management System: From Data to Activity. International Journal of Cyber Warfare and Terrorism (IJCWT), 12(2), 1-21. http://doi.org/10.4018/IJCWT.305860

[42] Al-Bashir, A &Mitani, B. (2016). Public Sector Governance: A Case Study of the Hashemite Kingdom of Jordan. Jerash University Journal, 17(2), 1-16.

[43] Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. The Electronic Journal of Information Systems in Developing Countries, 88(5), e12223.

[44] Alqudah, H., Amran, N. A., Hassan, H., Lutfi, A., Alessa, N., &Almaiah, M. A. (2023). Examining the critical factors of internal audit effectiveness from internal auditors' perspective: Moderating role of extrinsic rewards. Heliyon.

[45] Salem, A., & Al-Sayyed, R. (2022, November). Security Framework for Hosting Systems on the Cloud: Case Study of Jordan E-Government Websites. In 2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA) (pp. 1-6). IEEE.

[46] Almaiah, M. A., &Nasereddin, Y. (2020). Factors influencing the adoption of e-government services among Jordanian citizens. Electronic Government, an International Journal, 16(3), 236-259.

[47] Alawneh, A. and Al-Qirim, N. (2020). Cybersecurity Governance in Public Sector Organizations: A Conceptual Model. Journal of Enterprise Information Management, 33(5), 875-896.

[48] Al-Momani, A., Alomari, A., &Alomari, K. (2019). The Role of Cybersecurity in Enhancing Organizational Governance: An Analytical Study on Jordanian Banking Sector. Journal of Theoretical and Applied Information Technology, 97(2), 416-430.

[49] Alrawashdeh, M. and Al-Azzam, H. (2021). Cybersecurity Governance in Public Sector Organizations: A Case Study of Jordan. Journal of Cybersecurity, 6(3), 1-18.

[50] Al-Zoubi, M., Al-Qirim, N., & Qasaimeh, M. (2020). Strengthening Cybersecurity Governance in Jordan: Challenges and Opportunities. International Journal of Information Management, 52, 102041.