IJCEAS

*International Journal of Contemporary Economics and Administrative Sciences*
*ISSN: 1925 – 4423*
*Volume: XV, Issue: 2, Year: 2025, pp.548-570*

# The Impact of Internal Audit on Effectiveness in Cybersecurity: An Application of Internal Auditors' Perceptions

**Ebru Tüzemen**[1]
**Mihriban Coşkun Arslan**[2]

Received: 26.06.2025, Accepted: 10.12.2025
10.5281/zenodo.18141435

## Abstract

This study examines internal audit effectiveness in cybersecurity from the perspective of internal auditors at Turkish universities. Internal audit's role in cybersecurity governance within higher education represents an emerging research area, despite the rapid rise in cyber threats. Therefore, an online questionnaire was distributed to 168 internal auditors employed by state and foundation universities in Turkey, and 52 usable responses were received (30.9% response rate). The questionnaire contained demographic questions and 27 five-point Likert-scale items relating to internal audit effectiveness in cybersecurity. Exploratory factor analysis revealed five factors that summarized the 27 cybersecurity audit effectiveness items, accounting for 78.9% of the total variance. The study also discovered some significant demographics about internal audit in relation to cybersecurity. Over 51.9% of universities reported they outsourced cybersecurity services, 80.8% of internal audit units reported that they had never identified common cyber threats, while also 44.2% of the respondents reported that cybersecurity had never been discussed at the board level. An ANOVA test was also conducted, and the findings highlighted significant differences regarding cybersecurity perceptions based upon the educational background of auditors and knowledge level of the auditors (p<0.05). This study highlights important gaps in governance in relation to cybersecurity and provides evidence for promoting internal audit capabilities for dealing with digital risk management in Turkish universities.

**Key words:** Internal Audit, Cybersecurity, University Governance, Risk Management, Higher Education

**JEL Code:** M42, M41, O33

[1] MSc, Tokat Gaziosmanpasa University, Graduate School of Education, ORCID: 0009-0000-8843-7984 e-mail: eebrutuzemen@gmail.com.

[2] Prof. Dr., Tokat Gaziosmanpasa University, Faculty of Economics and Administrative Sciences, Department of Business Administration, ORCID: 0000-0002-6196-9304 e-mail: mihriban.arslan@gop.edu.tr.

# 1. Introduction

Digital transformation has fundamentally altered the cybersecurity landscape in higher education, making universities attractive targets for cybercriminals while simultaneously increasing their dependence on digital infrastructure to perform primary academic and administrative functions. Recent data indicate a 70% increase in education sector attacks during 2023, making it "the worst year for ransomware on record for education" (Malwarebytes, 2023). Notable incidents include the University of Michigan's inability to provide internet services to 230,000 students and the University of Minnesota's loss of thirty years of institutional data, demonstrating clear vulnerabilities facing higher education institutions (Inside Higher Ed, 2024).

Today's cybersecurity challenges require sophisticated internal audit responses. Currently, 59% of organizations test all controls rather than only critical ones, representing a 33% increase from the previous year (Hyperproof, 2024). The cybersecurity skills gap continues to widen, with 39% of organizations reporting skills gaps as a barrier to resilience; only 14% reported having the talent to achieve their cybersecurity goals (World Economic Forum, 2024). A significant skills gap exists in the public sector, with 49% of organizations lacking adequate cybersecurity workforce, a 33% increase from 2024 (World Economic Forum, 2024).

Universities face unique cybersecurity risks due to their complex organizational structures that serve multiple stakeholder communities, and the sensitive nature of the various data they hold, including student records, research data, and intellectual property. Universities handle vast amounts of extremely sensitive data, and now more than ever, cybersecurity audits are necessary to maintain their security posture (UpGuard, 2024). The complexity of a university's environment reveals an opportunity for internal audit functions to rethink traditional approaches to include how they will respond to new cyber risks emerging in institutions.

The evolving regulatory landscape highlights the need for adequate cybersecurity governance in higher education. The new Global Internal Audit Standards, effective 2025, require cybersecurity to be one of the first baselines in governance, risk management, and control processes (CrossCountry Consulting, 2024). Internal auditors are increasingly focusing on evaluating proactive incident management, compliance with industry standards, such as NIST and ISO 27001, and calculating essential metrics like mean time to detect and mean time to recover (CrossCountry Consulting, 2024).

Although cybersecurity is vital for higher education, there is little extensive research done on measuring cybersecurity audit effectiveness by internal auditors. Studies do show wide ranges of cybersecurity audit score effectiveness ratings, and there are significant differences in effectiveness (Slapničar et al., 2022). Higher education institutions have many risk areas, and reviews by internal audit can provide increased assurance regarding certain risk levels and actions to help mitigate some campus-based risks (Baker Tilly, 2024). The relationship between internal audit effectiveness and cybersecurity performance outcomes in university contexts remains unclear.

Through examining the effectiveness of internal audit in cybersecurity from the perspectives of internal auditors performing audits in Turkish state and foundation universities, this study aims to fill this gap in research. This research contributes to the increasing volume of literature on cybersecurity governance in higher education by presenting empirical evidence related to the factors of internal audit effectiveness in cyber risk management. Considering that university budgets for cybersecurity spending have increased over 70% in five years, yet attacks continue to increase (Moody's, 2024), especially in higher education settings, it is essential to understand the role of internal audit in facilitating cybersecurity governance.

The findings of this research will have implications for university administrators, internal audit practitioners, and policymakers of organizations hoping to improve their cybersecurity in institutional contexts based on changing governance and audit practices and processes. Through identifying the enablers of effective cybersecurity auditing in university environments, this study provides meaningful and actionable insights for improving the contributions of internal audit functions to help achieve organizational cybersecurity objectives.

The rest of the paper is structured as follows. Section 2 provides a full literature review on internal audit and cybersecurity research, a theoretical backdrop, and places research gaps. Section 3 identifies the research methodology, including the data collection approach, sample characteristics, and analysis procedures. Section 4 presents the analysis of the empirical findings, including descriptive statistics, factor analysis, and hypothesis testing. Section 5 discusses the implications of the findings, contributions to theory and practice, and limitations. Section 6 concludes with a summary of the findings, practical recommendations for the management of universities, and future research recommendations.

## 2. Literature Review

### 2.1. Internal Audit: Evolution and Contemporary Role

The literature documenting the transformation of internal audit from a traditional compliance-based function to one that is strategic and value-adding is substantial. The Institute of Internal Auditors specifically conceptualized internal audit as providing independent and objective consultancy and assurance services for the purposes of monitoring, developing, improving and adding value to both governance and all operational activities of the organization (Korkmaz, 2007). Arcagök and Erüz (2006) identified core characteristics of effective internal audit to include: functional independence; adding value to the organization; contributing to risk-based audit and governance processes; providing assurance and advisory services; and compliance with established standards.

Building on this understanding, Ceyhan (2010) argued that internal audit's principal role involves examining the efficiency and effectiveness of management-implemented controls to be consistent with aims and objectives of the organization. This clear evolution continues today, with Pickett (2010) stating that internal audit is a discipline that systematically seeks to help the organization to achieve its aims and objectives by assessing and improving the effectiveness of governance, control, and risk management processes.

More recent research by Hazaea et al. (2020) identified key factors impacting internal audit effectiveness, including internal audit function structure, audit planning, strategic communication, effective management, and professional qualifications of internal audit staff. This evolution culminated with the Institute of Internal Auditors releasing the January 2024 Global Internal Audit Standards, which will have an implementation date of 9 January 2025; the release of the 2024 standards represents one of the greatest improvements in internal audit practice standards (RSM, 2024; KPMG, 2024).

The 2024 standards outline 15 guiding principles across five domains: Purpose of Internal Auditing; Ethics and Professionalism; Governing the Internal Audit Function; Managing the Internal Audit Function; and Performing Internal Audit Services (Forvis Mazars, 2024). The effectiveness of internal audit today is assessed on its contribution to organizational resilience, with standards requesting internal audit to coordinate with both internal and external assurance providers as mandatory requirements (Forvis Mazars, 2024).

### 2.2. Cybersecurity Governance and Risk Management

Cybersecurity governance frameworks have changed considerably since the early 2000s and throughout the existence of this new sphere of work to contend with the increasingly sophisticated threat landscape. The work started with ISO/IEC 27001 and its systematic assessment of risk, selection of controls and implementation of Information Security Management Systems (ISMS). As of 2022, over 70,000 ISO 27001 certificates were reported across 150 countries, signifying that these practices have been adopted on a drastic scale (ISO, 2022).

Organizations assess their cybersecurity posture through cybersecurity maturity models. One such source is Güler and Arkın (2019) who put forth a detailed cybersecurity maturity model that presented five levels varying from "Not Available" to "Adaptable". Moreover, they indicated that organizations need to be at level 3 or higher to demonstrate effective cybersecurity governance. This body of work coincided with how auditing has moved as it relates to recognizing issues within each organizational body. Öztürk (2018) defined cybersecurity audits as key auditing practices in the detection and examination of issues related to organizational cybersecurity, which take place in the form of audits to achieve cyber controls for computer networks, servers, the software and other information systems.

The security field has made considerable advancements via the National Institute of Standards and Technology and its Cybersecurity Framework. In February 2024, NIST released updates for "CSF 2.0," its most significant update since 2018 (NIST, 2024; BitSight, 2024). A significant change was the expansion of the cybersecurity governance framework and its reach beyond critical infrastructure to apply to organizations of any size, and an introduction of six core functions: Govern, Identify, Protect, Detect, Respond and Recover. Notably, the Govern function presents a new emphasis on recognizing the importance cybersecurity governance plays in governance relative to enterprise risk management (Cybersecurity Tribe, 2024).

Contemporary organizations increasingly adopt hybrid approaches, integrating elements from multiple frameworks, including ISO 27001, COBIT and NIST 800-53 aimed at meeting organizational context relative to objectives and regulatory requirements. To provide an example, organizations that are ISO 27001 certified are expected to complete close to 83% of requirements for NIST CSF compliance. Organizations that are compliant with the NIST CSF would be 61% along the journey towards ISO 27001 compliance (OneTrust, 2024; ConnectWise, 2024).

### 2.3. Internal Audit in Cybersecurity Context

The combination of internal audit and cybersecurity was made possible when organizations began to understand that they needed more risk management avenues. Early research from Turkey by Selimoğlu and Saldı (2019) investigated cyber risk, its impact on organizations, and mechanisms for cyber risk analysis, mapping, and assessment from an internal audit perspective. In the study, the authors suggested that internal audit efforts in mitigating cyber risk were very similar to the focus on information technologies. The combined internal audit and cybersecurity efforts were expanded by Ocak (2021), who reviewed the relationships between cybersecurity and internal audit, including research on cybersecurity audit practices using actual cyber-attack scenarios and actions taken to respond to the attack.

In a first-of-its-kind initiative, Slapničar et al. (2022) developed a measure for measuring the effectiveness of cybersecurity audits called the Cybersecurity Audit Index, which broadly extended the domain into three dimensions: planning, performing, and reporting. The research reported significant differences in audit effectiveness scores, with a mean of 58 on a scale of 0-100. The researchers found a significant correlation between audit planning and performance. However, it is important to note that there was a weaker correlation between reporting on the effectiveness of cybersecurity risk management to the board. The researchers also suggested that the effectiveness of a cybersecurity audit was positively associated with maturity in cyber risk management but was unmapped to the actual reduction of the probability of a successful attack by a cyber threat actor.

The development of the internal audit profession was significant when the 2024 Global Internal Audit Standards established topical best practice requirements specifically for cybersecurity, approved for implementation in early 2025. The Global Internal Audit Standards establish baseline criteria for evaluating cybersecurity governance processes, risk management processes, and control processes (CrossCountry Consulting, 2024). Current conditions for organizations concurrently complicate their cybersecurity efforts due to the increased complexity of technology and the quickly evolving threat landscape. For instance, 59% of organizations are now testing all of their controls rather than just their critical controls. In the preceding year, 26% of organizations reported they would do so (Hyperproof, 2024). Unfortunately, a large majority of organizations found that they are losing accessibility to the talent they need for effective cybersecurity efforts, since 39% of participants identified skills gaps as a critical barrier to cybersecurity resilience (World Economic Forum, 2024).

### 2.4. Higher Education Cybersecurity Challenges

Cybersecurity threats to higher education have changed significantly in the past several years, especially in the wake of legislative and regulatory changes. The context of higher education in Turkey was influenced by the Constitution of Turkey 1982, which aimed to set up an institutional structure for creating universities as organizations to train qualified human resources, distribute knowledge, and deliver the benefits of knowledge to society. The Turkish universities were given scientific autonomy, a public legal personality, and made internal audit necessary as an entity in public law in Higher Education Law No. 2547 (Aydın, 2021).

The Public Financial Management and Control Law No. 5018 established in Turkish universities internally audit unit to help effectively organize public resources. Research on Turkish higher education institutions indicates that effective financial management and resource allocation remain critical challenges (Gürler & Demiroglari, 2020). Bayrakçı and Demirel (2017) discussed the structural and functional problems of internal audit in Turkish universities. They define internal audits within public administration as an activity to control, evaluate, and inspect organizational systems and processes to reduce wrongful and ineffective behaviors. Zorlu (2014) explained that without effective internal control and internal audit systems, the compliance and standards of universities are exposed to risk.

Uysal (2018) also states that when deciding how to develop risk-based internal audit activities, they are related to management awareness or perception of risk management. This was increasingly important, as threats to educational institutions increased; the threats being vastly superior to the cyber threat experienced by any other industry (with educational institutions being subjected to more than twice the monthly cyber-attacks than other industries) (Educause, 2023a).

More recently, another report, produced by Malwarebytes (2023), identified that universities were exposed to unprecedented challenges. Describing it as "the worst ransomware year on record for education," reporting a 70% increase in reported attacks (Inside Higher Ed, 2024). Universities are attractive targets due to the collaborative and open nature of their jobs, designed to accelerate knowledge development, which altogether puts a well-presented target upon themselves (BitLyft, 2023). Universities face multiple challenges including legacy systems, budget constraints, and regulatory complexity such as FERPA compliance and financial data protection requirements, which compound cybersecurity vulnerabilities.

Workforce issues do not help cybersecurity resilience in higher education. The Educause Cybersecurity and Privacy Workforce in Higher Education 2023 report found substantial gaps. Furthermore, while threats occurring across the educational organization did not diminish, only 46% of organizations reported increased cybersecurity budget allocations (Educause, 2023b). The challenges contribute to a worldwide cybersecurity labour gap of not much less than four million workers, creating competition between higher education institutions and organizations offering higher salaries (ISC2, 2023).

### 2.5. Research Gaps and Hypothesis Development

Although a diverse range of research has been conducted around both internal audit effectiveness and cybersecurity governance, significant gaps remain in our understanding of how the two intersect in alternative higher education settings. While the work of Slapničar et al (2022) provides a sound basis for cybersecurity audit measurement frameworks, the research did not focus specifically on higher education institutions, and instead was drawn from several industries, without any specific recognition of higher education institution characteristics.

In higher education, issues that exist include, but are not limited to, complex organizational governance structures, diverse stakeholder communities, open-access networks, and compliance requirements, all of which may affect traditional internal audit effectiveness, particularly in the context of the organization and its cybersecurity context (Baker Tilly, 2024). Due to the rapid advances in both the evolution of cybersecurity threats and the governance frameworks that have taken shape around them, there is a need for an empirical study into the factors that will help enable internal auditors to contribute to the overall cybersecurity resilience of universities.

Research gaps that remain regarding internal auditor effectiveness as it relates to university environments include, but are not limited to, an investigation of how internal auditor characteristics, such as education, professional experience, and level of knowledge, affect audit effectiveness. Academic institutions may simply be different, and because of their open nature, emphasis on collaboration, and influence of knowledge sharing, perhaps they require different processes and systems around cybersecurity auditing than institutions operating in the traditionally structured corporate environments.

This study will address the abovementioned research gaps by examining, as a case study, internal audit effectiveness in cybersecurity, from the perspective of internal auditors, within publicly funded university environments such as Turkish state and foundation universities. The study also adds to the literature in that it establishes associations between internal auditor characteristics and perceptions of cybersecurity audits; it allows for the development of hypotheses examining internal auditor characteristics such as education, professional experience, tenure, and level of cybersecurity knowledge as determinants of internal audit effectiveness in the context of higher education cybersecurity situations.

## 3. Implementation

The complementary relationship between internal auditing and cybersecurity provides organizations with a better opportunity to mitigate their cyber risk in a modern environment of cyber threats. The activities performed as part of internal audit processes provide one level of assurance by monitoring organizational cybersecurity implementation and measuring the effectiveness of security controls, as many organizations use a systems enterprise to measure and compare efforts against outcomes. Cybersecurity departments leverage risk assessments and the evidence provided by internal audit, so they can implement risk-based security strategies designed to increase organizational resilience. The complementary relationship of relying on internal audit and cybersecurity means organizations will develop a more resilient defense architecture against adaptive cyber threat attacks and simultaneously look to improve the processes related to the risk management of cybersecurity.

### 3.1. Research Purpose and Significance

This study's primary purpose is to investigate internal auditing processes at Turkish universities and how they relate to cybersecurity, through the lens of internal auditors' experiences. The secondary intent is to identify what the current internal auditing processes are, and how universities in Turkey are processing and implementing internal auditing to reduce emerging cyber risk.

This research denotes that there is an academic alliance internally within audit and cybersecurity functions that is critical for systematically exposing potential cyber vulnerabilities, exposing evidence-based security controls, and ensuring regulatory compliance is achieved in a complex landscape. Providing an integrated manner of delivering audit and cybersecurity functions allows for the university to create a stronger defense against emergent and more sophisticated cyber-attacks, while continuing to protect as much of the collaborative nature of the academic hyperspace to fulfill their mission-promoting inquiry.

This research study will explore the internal auditing processes of state universities and foundation universities under the regulation of Turkey, in examining their cybersecurity audit effectiveness related to their internal auditing mechanisms. This research contributes to internal auditing knowledge by examining relationships between auditor characteristics and their effectiveness perceptions in cybersecurity audit processes. As they were defined, the current articulation of internal audit practice within Turkish universities will develop an appreciation of two forms of phenomena that will aid the management of their organization's environment better - internal auditing processes and cyber vulnerabilities - that contribute to enhancing, to some degree, the security posture of the related entity.

### 3.2. Population and Sampling

For this research, the population is all internal auditors who operate under "Internal Audit" units with support to universities in Turkey (state and foundation). In formulating the population of research from universities' web pages, contact information was gathered for 168 internal auditors, which represents the total available population of this professional group of audit professionals in universities based in Turkey.

Data was collected using an online inventory instrument, and it was distributed electronically to all 168 identified internal auditors. Of the 168 emails sent, 60 were undeliverable due to various reasons: 12 non-existent addresses, 14 invalid contacts, and 34 changed addresses without notification. In the end, there were a total of 56 returned responses to participate in the results for operationalization of using the instrument. Therefore, 56 responses were received, yielding a response rate of 44.4%. When viewing the data, and removal of unusable responses, (52) dataset records of identified participants were achieved in this study. The sample size is reasonable based on similar research conducted in internal audits through organizational research, with many attempts to conduct enumerative population research, with response rates varying across studies (Saruhan and Özdemirci, 2018).

### 3.3. Research Methodology and Restrictions

This research employed survey methodology for systematic data collection guided by the study objectives. Development of the questionnaire began with the literature review, then formal semi-structured interviews were conducted with internal auditors at Tokat Gaziosmanpasa University and information technology department personnel for obtaining insights into internal processes and cross-department relationships, to inform the development of initial questions and to aid in maintaining functional relevance of survey items. Next, the questionnaire was reviewed with additional experts, and the survey was then pilot tested for content validity and reliability. Finally, after validating the instrument, ethical approval was received from the university's Institutional Review Board, and survey data collection began.

The final questionnaire included four sections; 1) current state of cybersecurity (10 closed-ended questions); 2) cybersecurity competency of the internal audit function as well as the university leadership (27 five-point Likert-scale items,); 3) demographic and professional characteristics of participants (16 mixed-format questions), and 4) seven-item exercise on the priority of importance of cyber risk management challenges. The data was statistically analyzed with SPSS software for in-depth analysis of the survey data for setting the cyberspace scene in Turkey.

The primary limitations of the research include a low response rate; while the response rate is statistically sufficient for research purposes, it nevertheless constricts the generalizability of the findings. Additionally, limitations include anticipated sampling bias due to incorrect email addresses on university websites and our approach to data collection as a cross-sectional study, limiting the research timeliness of evolving responses.

### 3.4. Results

The analysis was conducted in a series of steps; first, descriptive analysis of participants' demographic and situational data was undertaken, second, exploratory factor analysis was conducted to help identify construct validity, and third, formal hypothesis testing was undertaken. Participants' demographic characteristics are summarized in Table 1.

Table 1 reveals a predominantly male sample (84.6%) comprising experienced professionals. The age ranges of participants include 40.4% aged 46-55 years, 38.5% aged 36-45 years, and 21.2% over 56 years, which indicates the seniority of the internal auditor role. The education levels include 69.2% with bachelor's degrees, 23.1% with master's degrees, and 7.7% with doctoral degrees, which is important given the established professional qualifications.

The study demonstrated respondents' professional experience was generally high, as 48.1% had 6-10 years' university internal audit experience and 40.4% reported 11-15 years of experience. The university internal audit experience was supported by overall internal audit experience, showing 46.2% having 11-15 years, 30.8% with 6-10 years, and 21.2% with 16-20 years of internal audit experience, which indicates a professional group with high experience levels overall. Auditor characteristics are presented in Table 2.

**Table 1.** Frequency Table of Demographic Data

| Variable | Category | n | % |
|---|---|---|---|
| Gender | Woman | 8 | 15,4% |
| | Male | 44 | 84,6% |
| Age | Age 25 and under | 0 | 0,0% |
| | 26-35 years | 0 | 0,0% |
| | 36-45 years | 20 | 38,5% |
| | 46-55 years | 21 | 40,4% |
| | Age 56 and over | 11 | 21,2% |
| Education Status | Bachelor's degree | 36 | 69,2% |
| | Master's Degree | 12 | 23,1% |
| | PhD | 4 | 7,7% |
| Length of Service as Internal Auditor at the University | 1-5 years | 1 | 1,9% |
| | 6-10 years | 25 | 48,1% |
| | 11-15 years | 21 | 40,4% |
| | 16-20 years | 5 | 9,6% |
| | 21-25 years | 0 | 0,0% |
| | 25 years and above | 0 | 0,0% |
| Professional Experience as Internal Auditor | 1-5 years | 1 | 1,9% |
| | 6-10 years | 16 | 30,8% |
| | 11-15 years | 24 | 46,2% |
| | 16-20 years | 11 | 21,2% |
| | 21-25 years | 0 | 0,0% |
| | 25 years and above | 0 | 0,0% |

**Source:** Authors' calculations

**Table 2.** Frequency Table of Auditor Characteristics

| Variable | Category | n | % |
|---|---|---|---|
| **Cybersecurity and Information Technologies** | I have received training and have sufficient knowledge | 10 | 19,2% |
| | I have received training but I do not consider myself very competent | 22 | 42,3% |
| | I do not consider myself to have sufficient knowledge and experience | 20 | 38,5% |
| **Received Professional Certifications** | No | 9 | 17,3% |
| | Internal Auditor | 9 | 17,3% |
| | CGAP (Certified Government Audit Professional) | 14 | 26,9% |
| | Public Internal Auditor | 10 | 19,2% |
| | Accounting Officer | 3 | 5,8% |
| | Independent Auditor | 3 | 5,8% |
| | CPA | 4 | 7,7% |
| **Certificate Degree** | A1 | 7 | 16,3% |
| | A2 | 16 | 37,2% |
| | A3 | 7 | 16,3% |
| | A4 | 13 | 30,2% |

**Source:** Authors' calculations

Table 2 demonstrates significant cybersecurity competency gaps among participants. Nearly one-fifth of respondents (19.2%) report adequate cybersecurity training and knowledge, while 42.3% feel that they have been trained but have limited knowledge/competency, and 38.5% of respondents feel they just do not have enough knowledge. The breakdown of certifications by respondents reports that they specialized in operational audit and cybersecurity (26.9% CGAP), public internal audit (19.2%), internal audit (17.3%), and 17.3% of respondents did not have any credential or designation.

Table 3 presents university internal audit competencies. The main research findings indicate that 51.9% of university respondents outsource all of their cybersecurity services, and that 48.1% of universities have developed internal departments to oversee cybersecurity. Importantly, only 23.1% of the internal audit units now in place were deemed competent to assess cybersecurity risk, while 38.5% were considered incompetent and 38.5% were considered partially competent. Observable engagement at the board level about cybersecurity continues to be low; 44.2% of respondents reported that there have been no discussions on cybersecurity at the board level in the past year. Most critically, 80.8% of internal auditors have not identified common institutional cyber threats.

**Table 3.** Frequency Table of University Internal Audit Competency

| Variable | Category | n | % |
|---|---|---|---|
| Our university on cybersecurity issues | Purchases services | 27 | 51,9% |
| | Has its own department | 25 | 48,1% |
| Is the internal audit unit competent to assess cybersecurity processes and controls? | Yes | 12 | 23,1% |
| | No | 20 | 38,5% |
| | Partially | 20 | 38,5% |
| Have cybersecurity issues been on the agenda of the university board of directors in the last year? | It was discussed once as an agenda | 15 | 28,8% |
| | It was discussed as an agenda item in several meetings | 14 | 26,9% |
| | Frequently discussed as an agenda item in meetings | 0 | 0,0% |
| | Discussed as an agenda item in all meetings | 0 | 0,0% |
| | Never on the agenda | 23 | 44,2% |
| Has the internal audit unit identified common cyber threats that the university may face? | Yes | 10 | 19,2% |
| | No | 42 | 80,8% |
| | Partially | 0 | 0,0% |

**Source:** Authors’ calculations

Internal auditors' current cybersecurity status was assessed using 10 close-ended questions in the first part of the questionnaire form (Table 3). The results are shown in Table 4.

**Table 4.** Results of Internal Auditors' Assessment of the Current Situation Regarding Cybersecurity at the Universities Where They Work

| **Questions** | **Yes** | **No** | **Partly** | **No Opinion** |
|---|---|---|---|---|
| Important asset groups related to cybersecurity have been identified | 14 | 13 | 5 | **20** |
| | 26,90% | 25,00% | 9,60% | **38,50%** |
| Criticality of important asset groups related to cybersecurity has been determined | 14 | 12 | 5 | **21** |
| | 26,90% | 23,10% | 9,60% | **40,40%** |
| Current situation and gap analysis of important asset groups related to cybersecurity | 8 | 17 | 5 | **22** |
| | 15,40% | 32,70% | 9,60% | **42,30%** |
| Guidance on what to do with important asset groups related to cybersecurity has been determined. | 8 | 16 | 10 | **18** |
| | 15,40% | 30,80% | 19,20% | **34,60%** |
| When there is a change in important asset groups related to cybersecurity, the changes are managed in accordance with the guide. | 8 | 17 | 8 | **19** |
| | 15,40% | 32,70% | 15,40% | **36,50%** |
| Audits are conducted in accordance with the information and communication security guide published by the Presidential Digital Transformation Office. | 10 | **24** | 7 | 11 |
| | 19,20% | **46,20%** | 13,50% | 21,20% |
| The information and communication security guide published by the Presidential Digital Transformation Office is monitored and controlled. | 8 | **20** | 11 | 13 |
| | 15,40% | **38,50%** | 21,20% | 25,00% |
| Our university has a manual with rules and policies on cybersecurity | 6 | **25** | 9 | 12 |
| | 11,50% | **48,10%** | 17,30% | 23,10% |
| Internal audit units in universities should also employ personnel specialized in information technologies | **20** | 13 | 3 | 16 |
| | **38,50%** | 25,00% | 5,80% | 30,80% |
| In recent years, the role of internal audit in cybersecurity has increased. | **23** | 13 | 6 | 10 |
| | **44,20%** | 25,00% | 11,50% | 19,20% |

**Source:** Authors' calculations

The examination of status indicates that there are significant deficits in cybersecurity governance at Turkish universities. For instance, concerning the identification and management of critical types of cyber-related asset groups, 38.5% of survey participants examined the asset type groups and expressed having no opinion, while only 26.9% had identified the asset type. Similar responses were reported about determining the criticality of assets, with 40.4% of participants responding, "no opinion", and only 26.9% confirming criticality evaluations took place. Gap analysis results were even more concerning than status assessments, with 42.3% indicating no opinion and only 15.4% confirming status.

Regarding guidance development for cyber-related asset management, findings indicate limited progress for cyber-related asset guidance, with only 34.6% guidance considered produced, and only 15.4% confirming there were established processes for guidance. Like guidance, the cyber-related asset change management is similarly structured, with 36.5% of participants responding that they had no opinion, and 15.4% indicated proper cyber-related management.

Compliance with the Presidential Digital Transformation Office (PDTO) guidelines reveals significant gaps in terms of Turkish university status. Only 19.2% of participants indicated they audited processes relative to the published information and communication security guidelines, with 46.2% indicating they did not conduct audits relative to the information and communication security guidelines. Weaker compliance was reported with oversight and monitoring of the PDTO guidelines, as 38.5% of participants indicated they did not implement oversight of these processes, and only 15.4% indicated they performed the monitoring processes as intended.

Policy development with regards to cybersecurity at the university level revealed serious insufficiency as nearly half (48.1%) of participants indicated they did not have a cybersecurity manual with rules and policy guidance related to cybersecurity, while 11.5% participants indicated they had robust documentation of cybersecurity policy rules and policies. Notably, all participants acknowledged the need for staffing internally for IT specialists, and 38.5% indicated agreement with the internal audit unit employing IT specialists.

Most positively, 44.2% of participants acknowledge that the internal audit's role towards cybersecurity is increasing, which may suggest some consensus of recognition of this unit's importance relative to its intention in risk management.

Internal auditors were asked to consider the challenges universities face regarding cyber risk management by allowing internal auditors to rank the statements according to their importance. Seven statements were provided to participants, which were ranked according to their importance (Table 5).

The prioritization of cybersecurity challenges indicated systemic problems across all Turkish universities. The main concern was the difficulty in recruiting qualified cybersecurity experts, which was indicated as the first priority by the most participants (19.2%), with insufficient budget amounts as the second priority (32.7%). Relatedly, the top prioritized challenge was the lack of a standard cyber risk management methodology (21.2%), while the lack of a training program for employees in information security, privacy, and the fair use of information was indicated as the fourth priority by 19.2%.

Awareness and management follow-up of cyber threats at the sectoral and operational level was the fifth highest ranked priority (23.1%), which was indicative of a potential governance issue. The failures to understand new cyber threats ranked sixth (26.9%), while the lack of definition in who owns any cybersecurity issues was ranked the lowest (23.1%). Nonetheless, while not all challenges are considered a priority, they were all recognized as important challenges to consider.

**Table 5.** Importance of Difficulties Experienced by Universities in Terms of Cyber Risk Management

| Question | Importance | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| Recruitment of a qualified cybersecurity expert is difficult | Count | **10** | 6 | 7 | 10 | 5 | 5 | 9 |
| | Percentage | **19,2%** | 11,5% | 13,5% | 19,2% | 9,6% | 9,6% | 17,3% |
| Lack of a standard/common cyber risk management approach in the organization | Count | 11 | 3 | **12** | 5 | 10 | 8 | 3 |
| | Percentage | 21,2% | 5,8% | **23,1%** | 9,6% | 19,2% | 15,4% | 5,8% |
| Lack of follow-up and awareness at the management level on what cyber threats are sectoral and operational | Count | 1 | 7 | 7 | 10 | **12** | 9 | 6 |
| | Percentage | 1,9% | 13,5% | 13,5% | 19,2% | **23,1%** | 17,3% | 11,5% |
| Failure to train employees on information security | Count | 8 | 5 | 7 | **10** | 12 | 5 | 5 |
| | Percentage | 15,4% | 9,6% | 13,5% | **19,2%** | 23,1% | 9,6% | 9,6% |
| The institution does not allocate sufficient budget/investment for this issue | Count | 9 | **17** | 6 | 7 | 3 | 3 | 7 |
| | Percentage | 17,3% | **32,7%** | 11,5% | 13,5% | 5,8% | 5,8% | 13,5% |
| Failure to take measures against new cyber threats | Count | 6 | 8 | 8 | 2 | 4 | **14** | 10 |
| | Percentage | 11,5% | 15,4% | 15,4% | 3,8% | 7,7% | **26,9%** | 19,2% |
| Lack of a clear owner of cybersecurity in the organization | Count | 7 | 6 | 5 | 8 | 6 | 8 | **12** |
| | Percentage | 13,5% | 11,5% | 9,6% | 15,4% | 11,5% | 15,4% | **23,1%** |

**Source:** Authors' calculations

### 3.4.1. Explanatory Factor Analysis

The sectoral context questionnaire form measuring internal audit effectiveness, from a cybersecurity viewpoint, was subjected to exploration factor analysis testing and explicating the construct validity. The analysis resulted in the elimination of 2 statements from the scale due to shared factor loadings. The resulting analysis consists of 5 factors derived from factor analysis which explained a total variance of 78.9%. The KMO value was 0.823, greater than the minimum acceptable value, and the result of Bartlett's test was significant ($p<0.001$), suggesting that the sample size was sufficient and the data set was appropriate for factor analysis.

The factor structure identifies five conceptually distinct dimensions of cybersecurity audit effectiveness:

Factor 1 (information security audit perception) consists of eight statements that explained 20.112% of variance and have excellent reliability ($\alpha$=0.935). This factor reflects perceptions or the degree of satisfaction in what are perceived as the processes and methodology involved in achieving effective information security audit results within a university context.

**Table 6.** Results of Exploratory Factor Analysis

| Factors | Number of Statements in Factor | Explained Variance | Cronbach's Alpha |
|---|---|---|---|
| Factor 1: Perception of Information Security Audit | 8 | 20,112 | 0,935 |
| Factor 2: University Administration and Cybersecurity Perception | 6 | 17,932 | 0,905 |
| Factor 3: Perception of Internal Audit and Cybersecurity | 4 | 15,167 | 0,891 |
| Factor 4: Perception of Cybersecurity Knowledge Level | 4 | 13,190 | 0,837 |
| Factor 5: Cyber Risk Management and Perception of Cyber Threats | 3 | 12,499 | 0,890 |
| **Total Variance** | | **78,900** | |

**Source:** Authors' calculations

Factor 2 (university administration and cybersecurity perceptions) consists of six statements that explained 17.932% variance and have high reliability (α=0.905). This dimension reflects perceptions of engagement and support for cybersecurity-related matters from university leadership and administration.

Factor 3 (internal audit and cybersecurity perceptions) consists of four statements that explain 15.167% of variance and have strong reliability (α=0.891). This factor reflects perceived engagement and effectiveness of internal audit functions associated with cybersecurity and cyber risk.

Factor 4 (perceptions of knowledge level in cybersecurity) consists of four statements that explained 13.190% of variance and have good reliability (α=0.837). This dimension reflects self-ratings of competency levels in cybersecurity knowledge and skills.

Factor 5 (cyber risk management and perceptions of cyber threats) consists of three statements that explain 12.499% of variance and have high reliability (α=0.890). This factor reflects institutional approaches to cyber risk management and awareness of cyber threats.

### 3.4.2. Testing Hypotheses

Four research hypotheses were created to examine the influence of internal audit on cybersecurity from the viewpoint of internal auditors in universities. All hypotheses were analyzed using one-way analysis of variance (ANOVA) to examine relationships between auditors' characteristics, and perceptions of the effectiveness of an internal audit of cybersecurity.

**H1:** There is a significant difference between the perception of cybersecurity in internal audit based on the educational background of internal audit staff working in universities in Turkey.

**H2:** There is a significant difference between the perception of cybersecurity in internal audit based on the length of time that internal audit staff working in universities in Turkey worked as an internal auditor at the university.

**H3:** There is a significant difference between the perception of cybersecurity in internal audit based on the professional experience of internal auditors working in universities in Turkey.

**H4:** There is a significant difference between the perception of cybersecurity in internal audit based on the level of knowledge of internal auditors on cybersecurity and information technologies.

Table 7 shows the F and p values resulting from the hypothesis testing.

**Table 7.** Hypothesis Test Results

| **Hypotheses** | **$H_1$** | | **$H_2$** | | **$H_3$** | | **$H_4$** | |
|---|---|---|---|---|---|---|---|---|
| **Factors** | **F** | **p** | **F** | **p** | **F** | **p** | **F** | **p** |
| Factor 1: Perception of Information Security Audit | 4,524 | **,016** | ,262 | ,771 | ,256 | ,775 | ,280 | ,757 |
| Factor 2: University Administration and Cybersecurity Perception | 9,010 | **,000** | ,811 | ,450 | 2,430 | ,099 | ,624 | ,540 |
| Factor 3: Perception of Internal Audit and Cybersecurity | 3,368 | **,043** | ,003 | ,997 | 2,301 | ,111 | 5,463 | **,007** |
| Factor 4: Perception of Cybersecurity Knowledge Level | 4,670 | **,014** | ,915 | ,407 | 3,010 | ,058 | 2,896 | ,065 |
| Factor 5: Cyber Risk Management and Perception of Cyber Threats | 2,073 | ,137 | ,199 | ,820 | ,616 | ,544 | 3,551 | **,036** |

**Source:** Authors' calculations

### 3.4.3. Hypothesis Testing and Statistical Analysis

The study contained four main hypotheses, which were used to examine the relationships between the characteristics of internal auditors and their perceptions of the effectiveness of cybersecurity audits conducted in Turkish higher education settings. One-way ANOVA analysis was used to address each hypothesis. Post-hoc Scheffe tests were conducted when significant differences by factor or group were found after ANOVA. Hypothesis framework testing was used to determine how demographic factors, years of professional experience, and levels of cybersecurity knowledge (K) impact internal auditors' perceptions of effectiveness when working in cybersecurity audit-related contexts.

### ✓ *Evaluation of Hypothesis H1*

ANOVA results demonstrate significant differences between educational levels across four of five factors (p<0.05). Specifically, significant differences emerged for Information Security Audit Perception (F=4.524, p=0.016), University Administration and Cybersecurity Perception (F=9.010, p<0.001), Internal Audit and Cybersecurity Perception (F=3.368, p=0.043), and Cybersecurity Knowledge Level Perception (F=4.670, p=0.014). Only Cyber Risk Management and Perception of Cyber Threats showed no significant differences (p>0.05).

Post-hoc Scheffe tests revealed that master's degree holders consistently demonstrated higher perceptions across significant factors compared to bachelor's and doctoral degree holders, suggesting optimal cybersecurity audit effectiveness perceptions at the master's education level.

### ✓ *Evaluation of Hypothesis H2*

ANOVA results indicate no significant relationships between length of university service and cybersecurity audit effectiveness perceptions across all five factors (p>0.05). This finding suggests that tenure at specific institutions does not significantly influence cybersecurity audit effectiveness perceptions, leading to rejection of H2.

### ✓ *Evaluation of Hypothesis H3*

Analysis revealed no significant differences in cybersecurity audit effectiveness perceptions based on professional experience levels across all factors (p>0.05). This unexpected finding suggests that general internal audit experience may not translate directly to enhanced cybersecurity audit effectiveness perceptions, resulting in H3 rejection.

### ✓ *Evaluation of Hypothesis H4*

Significant relationships emerged between cybersecurity knowledge levels and two factors: Internal Audit and Cybersecurity Perception (F=5.463, p=0.007) and Cyber Risk Management and Perception of Cyber Threats (F=3.551, p=0.036). Post-hoc analysis revealed that participants with adequate cybersecurity training and knowledge demonstrated significantly higher effectiveness perceptions compared to those with insufficient knowledge, confirming the critical importance of specialized cybersecurity competency development.

### 3.4.4. Overall Assessment of Findings

The study provides a thorough assessment of what the authors observed regarding internal audit in cybersecurity issues in the context of Turkish universities. The authors write, while there is an internal audit function in place at the universities, there is a notable lack of cybersecurity-related competency and preparation on the part of the institution. It's important to recognize that the identification of five unique factors that accounted for 78.9% of variance in perceptions when measuring the effectiveness of cybersecurity audit distinguished a clear picture of the nature of this complex relationship.

The authors note the educational background of an internal audit professional as an important factor in determining perceptions of effectiveness in cybersecurity auditing, as those that hold a graduate-level degree held consistently higher perceptions of effectiveness in multiple dimensions. The implications of this finding may signal that investment in higher education may provide the best preparation for understanding complex cybersecurity audit requirements. It is also interesting to note that the authors report the absence of any significant relationships between the perceptions of effectiveness and professional experience, this raises a unique finding that suggests that traditional internal audit experience alone may not be adequate for cybersecurity contexts, implying the specialty of cybersecurity auditing.

Cybersecurity knowledge is critically important, with participants with adequate cybersecurity training demonstrating significantly higher perceptions of effectiveness. This finding emphasizes the urgent need for internal audit professionals to develop cybersecurity competencies in the domain of expertise. The study also highlighted some concerning institutional gaps such as limited discussion by the board on cybersecurity matters, internal audit units failing to identify threats to the institution, and internal auditors acknowledging that they had inadequate knowledge of cybersecurity issues.

In summary, the authors suggest that developing more effective internal audit capabilities in cybersecurity requires specialized training targeting individual auditors' competency development, risk management, and enhanced governance rather than simply relying on experience or time served.

## 5. Conclusion and Recommendations

This study examined internal audit effectiveness perceptions in cybersecurity among auditors at Turkish state and foundation universities. This study addressed a significant gap in understanding how internal audit practices contribute to cybersecurity governance in university environments, where there is a shift in the cybersecurity landscape towards greater sophistication and intensity of cyber threats.

The study revealed that Audit Effectiveness in cybersecurity is constrained by a structural impediment occurring in Turkish universities. The results indicate that only 23.1% of internal audit units possess a level of competency that enables adequate assessment of their institution's cybersecurity processes and controls, thus demonstrating considerable competency gaps. Of most concern was the finding that 80.8% of Audit Units had not identified the nature of the common cyber threats faced by their institution. This represents an overwhelming deficiency in the area of proactive risk management.

Educational background surfaced as a significant variable associated with perceptions of audit effectiveness around cybersecurity. One noteworthy finding was that educational background in cybersecurity was consistently shown to influence perceptions of effectiveness, as master's degree holders consistently earned higher effectiveness perceptions than bachelor's and doctoral degree holders. The most important finding to highlight was that specialized knowledge in cybersecurity was overwhelmingly important, as participants who said they had adequate cybersecurity training had significantly higher perceptions of effectiveness.

Counter to what was anticipated, there were no significant differences in participant perceptions of audit effectiveness based on tenure at the university or overall professional experience, suggesting that ingrained internal audit experience is not necessarily enough to bolster the effectiveness of cybersecurity auditing, which further exemplifies the decidedly specialized nature of cybersecurity auditing.

The research revealed five distinct factors explaining 78.9% of variance in effectiveness perceptions, which presently provides a multi-faceted understanding and model for measuring audit effectiveness in the specific context of higher education. There is an institutional governance gap, given that 44.2% of institutions engaging in institutional governance (board) conversations never include cybersecurity.

It is recommended that universities embed specific cybersecurity training into professional development programming for internal audit staff. In accepting the premise that general audit knowledge and skills can be nuanced by additional specific knowledge of cybersecurity, enhanced education will strengthen and empower university internal auditors with an institutional competence credibility focused on cybersecurity-related risks. It is recommended that university boards in governance of cybersecurity establish regular governance oversight committees focused specifically on cybersecurity matters and disclose adequate expertise to advise all board decisions. It is recommended that institutions establish systematic processes to mitigate cyber threats at the point of potential occurrence, rather than respond after the risk occurs.

This research contributes to the body of literature addressing governance of cybersecurity threats by employing a structured qualitative lens. It offers empirical evidence to demonstrate an identifiable number of antecedent factors influencing the effectiveness of internal audit in specific contexts, such as cybersecurity. Additionally, the study demonstrated that specialized knowledge is exponentially more important than general audit experience in the specific field of cybersecurity auditing.

There were limitations to the study in terms of generalizability. First, the limited sample size, just 52 participants, and the context of universities in Turkey, so it cannot be generalized universally. The research design employed was a cross-sectional design, which was limited in collecting perceptions at a single moment in time. The research also relied on self-reported data, which can be limited by bias. Additionally, this research focused on perceptions, when measures of the effectiveness of performance and cybersecurity were not part of the evaluation.

Future research should address said limitations through longitudinal studies and quantitative studies comparing results from audits of universities in different national contexts. There are future research opportunities to explore the optimal training program for internal auditors who operate directly in a cybersecurity context. Other interesting opportunities for research would be to explore various governance models at universities that achieve success at integrating direct oversight of cybersecurity as a component of overall institutional governance. Given the ever-changing landscape of cyberthreats in the higher education context and how institutions are implementing cybersecurity strategies, it is important to understand how the internal audit function can adapt to mitigate the emerging risks associated with technology.

The research presented in this study lays the foundation to understand more comprehensively, the nature of effectiveness of an internal audit operations practice in the specific context of cybersecurity in higher education, and as such emphasizes the need for higher education institutions to heavily rely on specific knowledge of cybersecurity, appropriate education behind the specific knowledge of cybersecurity, as well as enhancement to governance frameworks to strengthen institutional resilience cybersecurity risks.

## REFERENCES

Arcagök, M. S., & Erüz, E. (2006). Kamu mali yönetimi ve kontrol sistemi. İstanbul: Maliye Hesap Uzmanları Derneği Yayınları.

Aydın, S. K. (2021). Üniversitelerde iç denetim ve misyon sorunu. Ünye İktisadi ve İdari Bilimler Fakültesi Dergisi, 4(2), 9-22. doi:10.31834/uiibfd.959212

Baker Tilly. (2024). Going back to basics: Higher education internal audit challenges, risks and strategies. Retrieved September 15, 2024, from https://acua.org/resource/going-back-to-basics-higher-education-internal-audit-challenges-risks-and-strategies/

Bayrakçı, E., & Demirel, A. (2017). İç denetimin yapısal ve işlevsel sorunlarının Türkiye'deki üniversiteler bağlamında analizi. Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi, 19(33), 52-60. doi:10.18493/kmusekad.400150

BitLyft. (2023, August 18). The state of higher education cybersecurity: Top insights and trends. Retrieved February 12, 2024, from https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

BitSight. (2024, March 6). 7 cybersecurity frameworks to reduce cyber risk in 2024. Retrieved October 15, 2024, from https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

Ceyhan, İ. F. (2010). İç denetim ve kurumsallaşma (Unpublished master's thesis). Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale.

CompTIA. (2024). State of cybersecurity 2024. Retrieved November 8, 2024, from https://www.comptia.org/content/research/state-of-cybersecurity-report

ConnectWise. (2024). Top cybersecurity frameworks for 2024. Retrieved August 22, 2024, from https://www.connectwise.com/blog/cybersecurity/cybersecurity-frameworks

CrossCountry Consulting. (2024, April 15). Internal audit roles and responsibilities in 2024. Retrieved September 28, 2024, from https://www.crosscountry-consulting.com/insights/blog/internal-audit-roles-responsibilities/

Cybersecurity Tribe. (2024, April 15). NIST cited as the most popular security framework for 2024. Retrieved October 5, 2024, from https://www.cybersecuritytribe.com/articles/nist-security-framework-2024

EDUCAUSE. (2023a, October). 8 considerations when establishing cybersecurity in higher education. EDUCAUSE Review. Retrieved January 18, 2024, from https://er.educause.edu/articles/sponsored/2023/10/8-considerations-when-establishing-cybersecurity-in-higher-education

EDUCAUSE. (2023b, December). 3 key solutions to higher education cybersecurity workforce challenges. EDUCAUSE Review. Retrieved March 5, 2024, from https://er.educause.edu/articles/sponsored/2023/12/3-key-solutions-to-higher-education-cybersecurity-workforce-challenges

Forvis Mazars. (2024, April 8). Navigating the updated IIA's global internal audit standards. Retrieved July 20, 2024, from https://www.forvismazars.us/forsights/2024/03/navigating-the-updated-iia-s-global-internal-audit-standards

Güler, A., & Arkın, A. K. (2019). Siber hijyenin sağlanmasında iç denetimin rolü. Denetişim, (19), 17-40.

Gürler, Ö. K., & Demirogları, S. (2020). Determinants of household education expenditures by education level: the case of Turkey. International Journal Of Contemporary Economics And Administrative Sciences, 10(1), 235-258.

Hazaea, S. A., Tabash, M. I., Khatib, S. F. A., Zhu, J., & Al-Kuhali, A. A. (2020). The impact of internal audit quality on financial performance of Yemeni commercial banks: An empirical investigation. Journal of Asian Finance, Economics and Business, 7(11), 867-875. doi:10.13106/jafeb.2020.vol7.no11.867

Hyperproof. (2024). The future of auditing: What to look for in 2024. Retrieved November 12, 2024, from https://hyperproof.io/resource/the-future-of-auditing-2024/

IIA. (2024). Global internal audit standards. Retrieved August 15, 2024, from https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/

Inside Higher Ed. (2024, July 1). University cybersecurity threats remain a concern. Retrieved October 8, 2024, from https://www.insidehighered.com/news/tech-innovation/2024/07/01/university-cybersecurity-threats-remain-concern

ISO. (2022). ISO/IEC 27001:2022 - Information security management systems. Retrieved May 14, 2024, from https://www.iso.org/standard/27001

ISC2. (2023). 2023 cybersecurity workforce study. Booz Allen Hamilton. Retrieved February 25, 2024, from https://www.isc2.org/Research/Workforce-Study

Kalender, İ. (2008). Türk kamu idaresinin yeni yönetim ve denetim sistemleri. Türk İdare Dergisi, (468), 87-103.

KPMG. (2024, January 31). 2024 global internal audit standards. Retrieved June 18, 2024, from https://kpmg.com/us/en/articles/2024/global-internal-audit-standards.html

Korkmaz, U. (2007). Kamuda iç denetim. Bütçe Dünyası Dergisi, 2(25), 4-15.

Malwarebytes Labs. (2023). Ransomware attacks in education sector report. Malwarebytes. Retrieved January 30, 2024, from https://www.malwarebytes.com/resources/files/2024/01/education-sector-ransomware-report

Moody's Investors Service. (2024). Higher education cybersecurity budget analysis. Moody's Corporation. Retrieved September 10, 2024, from https://www.moodys.com/research/higher-education-cybersecurity-budget-analysis

NIST. (2024). Cybersecurity framework 2.0. Retrieved June 25, 2024, from https://www.nist.gov/cyberframework

Ocak, H. S. (2021). İç denetimin gelişen ve değişen dünyasında siber güvenlik ve denetim (Unpublished master's thesis). Marmara Üniversitesi, İstanbul.

OneTrust. (2024). ISO 27001 vs. NIST cybersecurity framework. Retrieved August 8, 2024, from https://www.onetrust.com/blog/iso-27001-vs-nist-cybersecurity-framework/

Öztürk, M. S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. Muhasebe ve Vergi Uygulamaları Dergisi, 11(Özel Sayı), 208-232. doi:10.29067/muvu.340848

Pickett, K. S. (2010). The internal auditing handbook (3rd ed.). New York, NY: John Wiley & Sons.

RSM. (2024). IIA issues 2024 global internal audit standards to guide the profession's future. Retrieved July 5, 2024, from https://rsmus.com/insights/services/risk-fraud-cybersecurity/iia-issues-2024-global-internal-audit-standards-to-guide-future.html

Saruhan, Ş. C., & Özdemirci, A. (2018). Bilim, felsefe ve metodoloji (5th ed.). İstanbul: Beta Basım Yayım Dağıtım A.Ş.

Selimoğlu, S. K., & Saldı, M. H. (2019). İşletmelerde siber risklerin analizinde, haritalanmasında ve değerlendirilmesinde iç denetimin rolü. Muhasebe ve Denetime Bakış, 19(57), 75-92.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. doi:10.1016/j.accinf.2021.100548

StrongDM. (2024, January 22). Cybersecurity audit: The ultimate guide for 2024. Retrieved September 3, 2024, from https://www.strongdm.com/blog/cybersecurity-audit

UpGuard. (2024). How to perform a cybersecurity audit for colleges & universities. Retrieved November 18, 2024, from https://www.upguard.com/blog/how-to-perform-a-cybersecurity-audit-colleges-universities

Uysal, M. C. (2018). Kamu kurumlarında kurumsal risk yönetimi ve risk odaklı iç denetim: İç denetçiler üzerine bir araştırma-II. Denetişim, (18), 35-44.

World Economic Forum. (2024). Global cybersecurity outlook 2024. Geneva: World Economic Forum. Retrieved October 20, 2024, from https://www.weforum.org/reports/global-cybersecurity-outlook-2024/

Yılmaz, O. (2018). Küreselleşme sürecinde dönüşen güvenlik algısı ve siber güvenlik. Cyberpolitik Journal, 2(4), 22-43. doi:10.1234/cyberj.2018.389915

Zorlu, M. (2014). Kâr amacı gütmeyen organizasyonlarda iç kontrol ve iç denetim: Bir devlet üniversitesinde uygulama (Unpublished master's thesis). Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü, Nevşehir.