Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683

Innovative Approaches to Risk Governance Integrating Security Audits with Advanced Cybersecurity Strategies

Sneha Gogineni
USA
gsneha0828@gmail.com

ABSTRACT

This paper's goal is to examine how well cybersecurity internal audits work. For this reason, we set out to create a Cybersecurity Audit Index that covers the bases in terms of preparation, execution, and reporting. We postulate that the likelihood of a successful cyber assault is inversely related to the efficacy of cybersecurity audits and that cyber risk management maturity is favorably related to them. By surveying auditors and chief audit executives from different nations and industries, we were able to test our hypotheses. Our research shows that there is a wide range of Cybersecurity Audit Index scores (58 on a scale from 0 to 100). Cyber risk management effectiveness reporting to the Board of Directors is less strongly tied to the planning and performance stages, despite the high and positive correlation between them. Although it was expected that the Cybersecurity Audit Index would have a positive correlation with maturity, it was surprised to see no correlation with the likelihood of a successful cyber assault. For the first time, this report quantifies the impact of cybersecurity audits on cyber risk management and how effective they are.

Keywords: *Cybersecurity, Audit, Risk Governance*

1. INTRODUCTION

The financial situation, strategic goals, and, most importantly, the trust and credibility that a business has established over the years are all at risk when sensitive data is compromised in a cyberattack [1]. The IT security audit function is tasked with reducing the likelihood and impact of this significant risk. How does it do this? Why, then, should audits of both IT and security be conducted in tandem? By figuring out how to use testing and controls across different frameworks, organisations can save time and effort during audits and get a better picture of their audit, compliance, and security postures all at once.

What Is a Security Audit?

An audit of a company's security measures and computer systems is known as a security audit. By conducting an IT security audit, businesses can uncover the vulnerabilities in their whole IT infrastructure, including networks, devices, and applications.

Organisations can address security weaknesses and achieve compliance using this opportunity [2]. However, security audits are more complex than that. Today, many organisations are subject to many audits as a result of compliance regulations that they must follow. The evaluation process that organisations go through in order to be ready for an audit may be rather daunting.

Why Perform a Security Audit?

Conducting security audits is important for several reasons. Here are six objectives:

1. Locate vulnerabilities, exploits, and security issues in the system.
2. Create a baseline for security that can be used to compare future audits.
3. Follow the security policies of the organisation that are internal.
4. Meet all rules set by external regulators.
5. Evaluate the level of security training.
6. Find resources that aren't needed.

Critical data can be better protected, vulnerabilities can be found, new security rules can be developed, and the efficacy of security tactics can be monitored through security audits. Organisations should have suitable security processes in place, and audits should be scheduled regularly to stimulate the development of procedures to continuously uncover new vulnerabilities.

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683

When Is a Security Audit Needed?

A company's security audit frequency should be proportional to its industry, the complexity of its operations, and the amount of systems and applications that need checking. More regular audits are commonplace for organisations like healthcare providers and financial institutions that deal with large amounts of sensitive data. Security audits can be more easily performed, and even more regularly, by enterprises that employ less than two apps. A number of external factors influence the frequency of audits, including regulatory obligations (such as FEDRAMP, the US Federal Risk and Authorisation Management Program). On the other hand, most businesses probably don't have what it takes to conduct audits on a quarterly or monthly basis [3]. How frequently a company decides to conduct security audits is influenced by the type and relevance of the data stored in such systems as well as the complexity of those systems. Data from vital systems may be audited more often, whereas audits of complex systems that take a lot of time may be inspected less frequently. Organizations are required to conduct specific security audits after certain events, such as data breaches, system upgrades, data migrations, changes to compliance rules, new system implementations, or exceeding user limits. This incident may have introduced security weaknesses, but these one-off inspections can pinpoint exactly where. For example, in the event of a recent data breach, the root cause of the breach can be determined by an audit of the affected systems.

What System Does an Audit Cover?

An organization's systems may be checked for vulnerabilities in specific areas during a security audit, such as:

Network vulnerabilities— By "weakness," auditors imply any area of a network that may be exploited by an attacker to gain unauthorized access, steal data, or cause harm in any other way. Data is especially vulnerable while it is being transferred between different places. Security audits and routine network monitoring capture every single message sent and received over the network, be it an email, instant message, file transfer, or anything else. The audit also includes checking the network availability and accessibility points.

Security controls— In this part of the audit, the auditor checks how well the company's security measures work. In this step, we verify that the organization has adhered to its own policies on the protection of sensitive information and computer systems.

Encryption— The existence of policies and processes to monitor the encryption of critical information is verified in this audit component.

Software systems— It is standard practice to test software systems to make sure they are secure, that the data they provide is correct, and that no one else can access sensitive information. Topics including data processing, software engineering, and IT infrastructure are covered.

Architecture management capabilities— Auditors make sure that the IT management has set up the necessary organizational structures and processes to guarantee a controlled and efficient environment for data processing.

Telecommunications controls— When it comes to telecommunications, auditors make sure that all controls—client, server, and network—are operational.

Systems development audit— Systems in development must adhere to the organization's security goals, and audits in this area ensure they do just that. This section of the audit is necessary for a number of reasons, one of which is to guarantee that all systems in development are compliant.

Information processing— Data processing security procedures are confirmed by these audits.

2. LITERATURE REVIEW

Cybercrime continues to thrive despite widespread awareness of the problem and several technological and procedural precautions. A survey of 579 Chief Audit Executives (CAE) was carried out by the European Confederation of Institutes of Internal Auditors (ECIIA) and was titled "Cybersecurity" [4]. A number of factors have combined to make cyber risk more prevalent since the last pandemic, including the rise of telecommuting, the use of

videoconferencing software at work, and the incorporation of personal devices and private WiFi networks into business systems [5].

Examining the efficacy of cybersecurity audits (CSAs) and their roles in risk management is the driving force behind this research. A lot has changed in the field of CSA in the past several years. The objective of this audit is to collect evidence from an outside source that the company's policies and processes for managing risk, as well as its internal controls, are sufficient to protect assets, proprietary information, and the timely access to that information [6]. With the support of the internal audit function (IAF), the executive managers and the Board of Directors (henceforth the Board) can carry out their responsibilities in the area of CS governance with more confidence [7]. Internal audits have received less attention in the literature on CS risk management and governance [8].

Still lacking, however, is both the idea of what makes a good CSA and proof of its actual implementation. It is difficult to measure the efficacy of CSA and other forms of internal audit (IA). [9] describes IA as a "risk-based concept that helps the organisation achieve its objectives by positively influencing the quality of corporate governance." Regards IA as "doing the right things" and "doing them well" when it comes to effectiveness. In addition, you should go over the various ways that prior research has tried to quantify the efficacy of IA, the pros and cons of each, and then come to the conclusion that no adequate metric has been proposed in the current literature. There appears to be no consensus on how to define or measure the efficacy of IA, according to a recent literature review. The most typical metric is really tracking the level of adoption of the IAF's suggestions and the success of its annual work plan. The IIA Practice guide defines effectiveness as the degree to which IAF's aims are achieved, thus this is consistent with that definition. As one component of effective IA, this research focuses on CSA and its efficacy.

We provide a conceptual framework for its typology and use an index to make it operational. Our measure is based on the process approach, which holds that effective IA requires adherence to the Standards for the Professional Practice of Internal Auditing. Scholars recognize standard compliance as a quality benchmark, and the Common Body of Knowledge utilizes it as a criterion for IA efficacy [10]. Standard 1300 also employs it. We demonstrate how CSA relies on CS frameworks, normative theory, expert recommendations, and best practices, which expands its scope of use.

Since the Board and the IAF have different levels of knowledge and expertise, evaluating CSA solely by how well it satisfies Board expectations would be incomplete. Based on anecdotal data and professional publications, it appears that CSA and other forms of CS risk management are still driven from the bottom up in many organisations. Furthermore, the directors' expectations regarding this matter are vague. Given that IA is considered successful if it leads to "the achievement of a desired condition," we hypothesise that our Index is linked to cyber outcomes and the degree of advancement in CS risk management.

A total of 183 certified enterprise auditors (CEAs) and IT auditors from various nations throughout the world were polled. We were able to recruit participants through the 19 national IIA chapters and 3 ISACA chapters that shared the study's flyer with their members [11]. At 58 out of 100 on the Index scale, our data indicate that CSA is generally high. But we discover that the scores differ greatly amongst sectors. While there is a high association between the planning and performance phases, there is less of a correlation between the two phases and reporting to the Board. As expected, we also discover that CSA has a favourable correlation with CS risk management maturity levels; nonetheless, it fails to reduce the likelihood of cyber attacks. There are a number of useful contributions in the work. We start by creating a typology for CSA efficacy and then we use objective metrics to make it work. At the end, we come up with the Index. By doing so, we contribute to the growth of both the CSA and IA effectiveness literatures, which have been at odds over how to define and quantify objective measures of IA quality. Researchers and professionals in the field are becoming more interested in CSA. But there can be no solid proof of its efficacy or its

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683

influence on other factors until a complete measurement is developed.

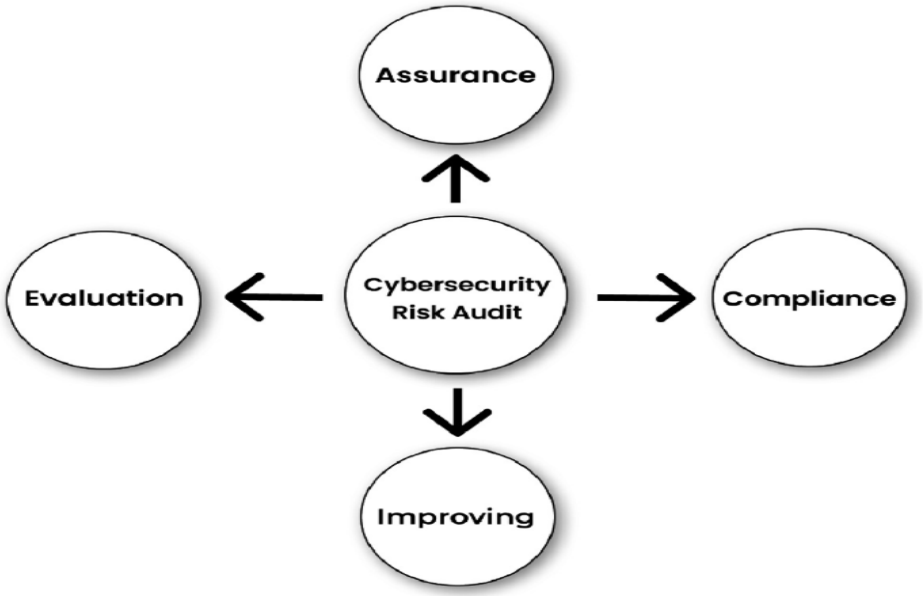


Fig 1: Cybersecurity Risk Audit

Assurance - Situated above the word "Cybersecurity Risk Audit," a downward-pointing arrow leads to it.

Compliance - Located as the arrow points to the left from "Cybersecurity Risk Audit," on the right-hand side.

Improving - Located under the heading "Cybersecurity Risk Audit," with a directional arrow leading up to it.

Evaluation - Next to "Cybersecurity Risk Audit," on the left side of the screen, with an arrow pointing in its direction.

Within the framework of cybersecurity risk auditing, this arrangement implies a recursive or linked process involving these components.

Secondly, the paper adds to the literature on the effectiveness of information assurance by offering new evidence on the relationship between CSA and cyber outcomes, specifically CS risk management maturity and the likelihood of a cyber attack. This research fills a gap in the existing literature by providing original evidence on this relationship. More practically, our results help internal auditors, many of whom have trouble gauging the efficacy of their CSA, improve their methods. The internal auditors can utilise our instrument, which is included in the appendix, as a tool for periodic assessments. In doing so, we respond to the demand that IA research should be more in line with practical issues that matter [12]. Our research aims to provide the IIA chapters throughout the globe with information about the current state of the subject so that they can keep providing publications and training to their members.

Previous research on CSA is limited. In addition, you should summarise thirteen works on CSA to demonstrate that this field is still in its infancy. The efficacy of CSA has not been defined or operationalised in any of the research. The study suggests a number of features of an efficient CSA in [13], however these are rather general and based on principles. Organisations can achieve an adequate degree of information security while keeping costs down, according to this theory, which focusses on the interplay between internal audit and information security operations. Since it is the sole empirical study to examine the scope of CS audit, the work in [14] provides valuable insight. By averaging seven items regarding IT auditing from the Common Body of Knowledge (CBOK) survey, the authors determine the amount of CSA [15]. The CBOK

survey is an all-encompassing look at internal audit methods; it only briefly mentions IT auditing, which is CSA in its own right.

The project aims to propose an 18-domain CSA model in [16] to assist organizations and nation states. The article cannot be relied upon for the current study due to its failure to explain subdomains of domains, its absence of controls, and its provision of a guideline assessment that is exclusive to nation states. When the second line, the CISO, and the third line, the IAF, work together, it improves cybersecurity significantly, according to research in [17]. Five IT auditors/CAEs and one CS consultant participated in semi-structured exploratory interviews to provide their insights on the CSA effectiveness typology.

Our professional network served as a recruiting tool for the interviewees [18]. Every single person we spoke with works in the banking or academic sectors, two of the most vulnerable to cyberattacks. On average, these five individuals—four men and a woman—had worked as information auditors for 15.4 years and as cyber auditors for 10.8 years. Their nationalities were as follows: (3) Slovenian, (1) Croatian, and (1) Australian [19]. A director of a Big Four corporation and a consultant in CS risk management round out their roles. They are IT auditors and CAEs. The research got the green light from the University of Queensland's ethics committee. To facilitate a more in-depth exploration of the topics at hand, the interviews were semi-structured and adaptable according to the interview procedure. There was no intention of using them as a source of direct expert assistance during the instrument's development. Our thought model was informed by qualitative interview data [20].

3. STRENGTHENING COLLABORATION BETWEEN INTERNAL AUDIT AND IT

Prevention, detection, and remediation are the three pillars upon which a strong cybersecurity strategy rests. The primary function of internal auditing is to identify control flaws and cybersecurity gaps, and to prevent significant cyberthreats and risk by conducting regular audits and making suggestions. None of these goals can be achieved without constant communication and cooperation with the IT department. When internal audit and IT work together effectively, everyone wins. For instance, the IT team can improve the controls they've already built or address areas they might have missed thanks to internal audit's impartial and independent assessment of information security frameworks and controls. In order to make sure that management is on board with security policies and that staff are taking their security compliance duties seriously, the IT team is working with internal audit to accomplish these goals.

Consequently, the audit committee and internal audit should have frequent meetings with the CIO and CISO to go over important cybersecurity matters, share insights on new vulnerabilities, threats, and regulations, and answer any questions that may arise. Having an open-source mapping tool (like Secure Controls Framework [SCF]) that facilitates team communication and coordination of audit tasks is also crucial.

Adopting an Integrated Approach to IT and Security Auditing

Maintaining consistent reporting and communication of risk, threats, and controls is the single most important component of any cybersecurity program. If the company wants to establish a unified vocabulary around risk, it needs audits to assist with that. With the use of tools that simplify security data aggregation, communication, and analysis, audit teams should establish standardised libraries of risk factors and controls. Maintaining, accessing, and sharing critical data should be a breeze using a central repository that both the audit and IT teams can utilise. In addition, groups can plot potential points of security breach against auditable entities, IT assets, policies, and laws. Audit and IT teams should be able to use this tightly linked data model to anticipate the effects of cybersecurity risks and ineffective controls on the business and offer proactive solutions.

Because evidence can be tested once and used across appropriate frameworks that share scope, audit integration also reduces strain on audit teams and IT/engineering professionals, as opposed to obtaining it at different times of the year. When you gain efficiency by cross-testing shared controls, you

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683

can stop being in permanent audit mode all year long and put that energy into day-to-day operations.

First things first when planning an integrated audit: ensure sure the testing environments' scopes are going to be comparable for all the relevant frameworks. As soon as the scope is specified, businesses can begin to investigate enterprise-wide controls that are comparable. Prior to considering technical testing of network systems for additional efficiency gains, many organisations begin with security policies and procedures, since these typically apply to the entire organisation.

Frameworks for Integration

It is possible to approach practically any framework in an integrated way. Making sure that scopes are as aligned as feasible is the most crucial part. Standard Operating Procedures (SOPs) 2 Type 2, the Payment Card Industry's Report on Compliance (ROC), HIPAA, and the International Organisation for Standardisation (ISO) standard ISO 27001 are among the most often integrated frameworks, standards, and laws. An organisation that offers billing services to the healthcare industry is one that may use the frameworks outlined earlier. Given its relationship with healthcare providers, the organisation would be obligated to comply with HIPAA. It would also need to comply with the payment card industry as it accepts credit cards as a payment method. Finally, due to internal security demands, the organisation would need to undergo ISO and SOC 2 Type 2 audits to test its processes and systems. An organization's testing efficiency, overall security posture, and compliance duties can be better understood when the scope is aligned with these standards, frameworks, and legislation.

Measurement of CSA Index

Using Diamantopoulos's methodology for index building as a guide, we modified it to create the CSA Index. Our metric for this formative variable was a composite one. We have already provided a conceptual explanation of the construct and its pieces up above, and now we will connect them to the real indicators in this section. This is the first stage in building the index. Step two is to identify the feature of interest and then create a set of dimensions to represent it; in this case, Planning, Performing, and Reporting. The final step in evaluating the items' suitability for measuring the constructs is to check their content validity. To ensure the index was content-valid, we checked it against academic literature, professional norms, and pilot interviews. Defining a formal measuring model is the fourth stage, which is detailed below. Indicators for the IAF's risk assessment, CS frameworks used, and proactive planning make up the first part of the CSA Index's Planning component. As far as preparation goes, the first set of nine questions gauges the IAF's initiative and focus on strategy.

The actions taken by the IAF in relation to risk-based planning are captured in the second group of four elements. The final inquiry pertains to the application of CS frameworks. As previously mentioned, we believe that any CS framework, because to its systematic mapping of processes, is more successful than none at all. Table 1 shows the Planning dimension, which we created by combining the three sets of indicators and assigning weights to each set based on our assessment of their relative relevance.

4. METHOD

Table 1: The Planning dimension

Abbreviation	Planning	Weight	Description
PROACT	IAF's proactiveness in planning	0.3	Nine items are used to assess the IAF's proactive planning, with 1 being not at all, 2 somewhat, 3 substantially, 4 very lot, and 5 fully.
RISK	IAF's risk assessment	0.3	Provide your ranking of four items related to the IAF's actual risk assessment activities using a Likert scale where 1 is not present, 2 is somewhat present, 3 is moderately present, 4 is very much, and 5 is absolutely absent.
FRAMEW	CS frameworks used	0.4	If participants employ a framework, the value is 1; otherwise, it is 0.

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683

Performing, also known as the execution of CSA, is the second dimension and it includes two sets of indicators. There are twelve CS categories that are audited in each cycle: program management, data protection, identity and access management, infrastructure, cloud and software security, third party and workforce management, threat and vulnerability management, monitoring, crisis management, and enterprise resilience. The first group of metrics assesses compliance with ISA 500: Audit evidence by tracking the application of particular audit methods including inquiry, observation, inspection, analytical procedures, and reperformance.

To a significant extent, they conform to the standard CS models. We set a maximum score for three or more operations and a greater score for additional procedures because we know that testing areas effectively requires a mix of processes. There are certain processes that naturally yield better results than others. Reperformance is the gold standard of audit procedures since it allows the auditor to independently test the entity's internal controls. Consequently, full credit was given for this method alone.

Sample

Information technology auditors and CAEs make up the target demographic for this research. Our goal in seeking for participants was to include a wide range of industries, sizes of organisations, and nations. In all, 36 IIAs were contacted, spanning from the European Community (ECIIA) to Israel, Australia, and New Zealand. We contacted thirteen European ISACA Charters, one American charter, five Australian charters, and three New Zealand charters in an effort to increase our access to IT auditors. We employed a random sampling technique to maximize the utility of our survey and guarantee that our results are applicable to a large audience. The selection of nations is critical due to the wide range of locations and CS development levels. Nineteen IIA Affiliates in Europe, one ISACA Chapter in the United States (Las Vegas), and three ISACA Chapters in Europe (Milan, Austria, and Slovenia) have shown interest in taking part. The poll was distributed to all members of the mentioned groups through their monthly newsletters. In an effort to boost the response rate, each national IIA can choose to translate the survey into their local language, based on their best judgment. The six IIAs who made the decision were the Polish, Hungarian, Croatian, Serbian, Czech, and Bulgarian voices. The translation was reviewed again by each IIA's IT staff. Before its release, the survey was proofread by five IT auditors and two CS experts to ensure it was error-free and easy to understand.

Two of them skipped out on the first round of interviews. Some questions on the instrument were revised slightly to make them easier to understand.

5. RESULTS AND STUDY

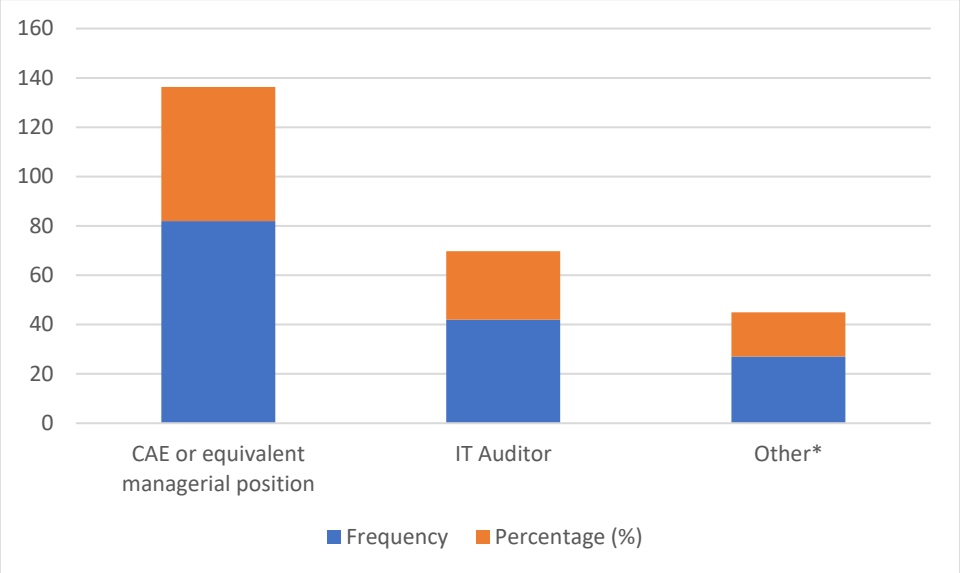
Table 2 Descriptive statistics.

Panel A: Respondents Demographics

Employment Role Distribution (n = 151)

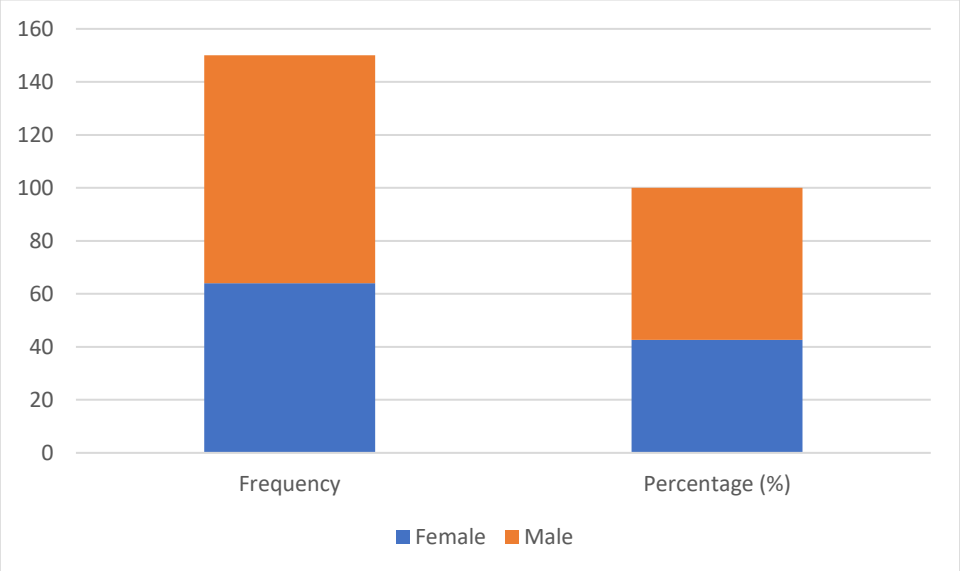
Role	Frequency	Percentage (%)
CAE or equivalent managerial position	82	54.30
IT Auditor	42	27.80
Other*	27	17.90

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683



Gender Distribution (n = 150)

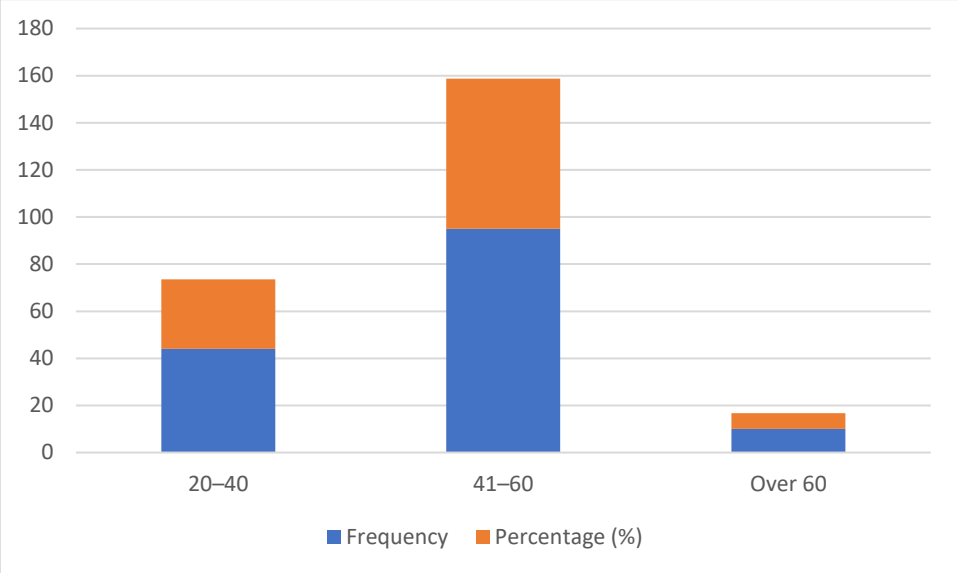
Gender	Frequency	Percentage (%)
Female	64	42.7
Male	86	57.3



Age Distribution (n = 149)

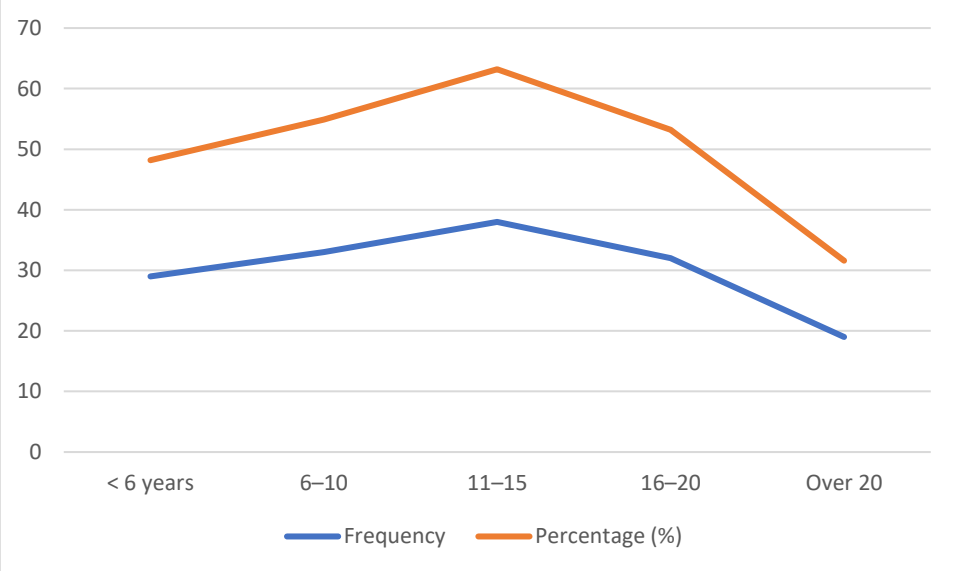
Age Group	Frequency	Percentage (%)
20–40	44	29.5
41–60	95	63.8
Over 60	10	6.7

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683



Work Experience as Internal Auditor (n = 151)

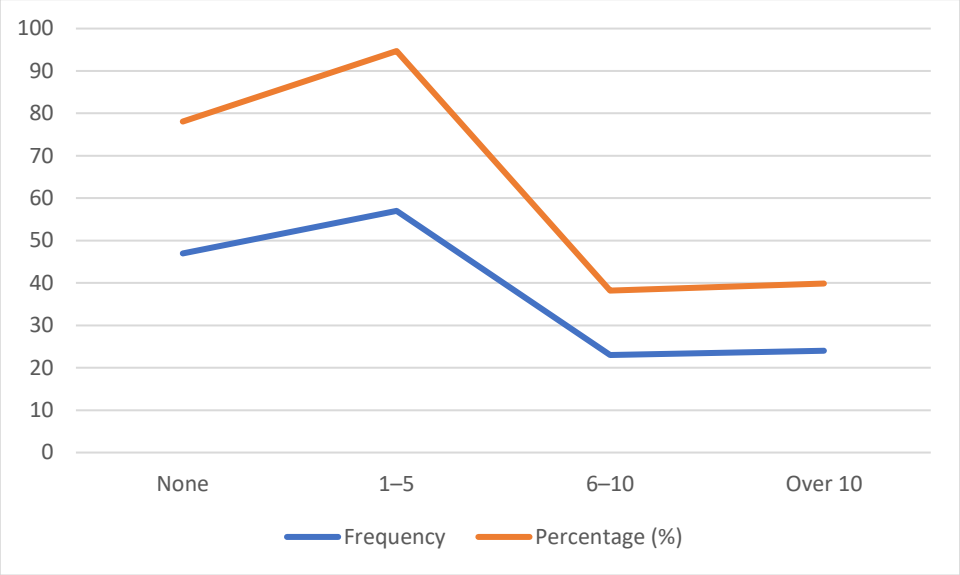
Experience (Years)	Frequency	Percentage (%)
< 6 years	29	19.2
6–10	33	21.9
11–15	38	25.2
16–20	32	21.2
Over 20	19	12.6



Work Experience in the Area of CS (n = 151)

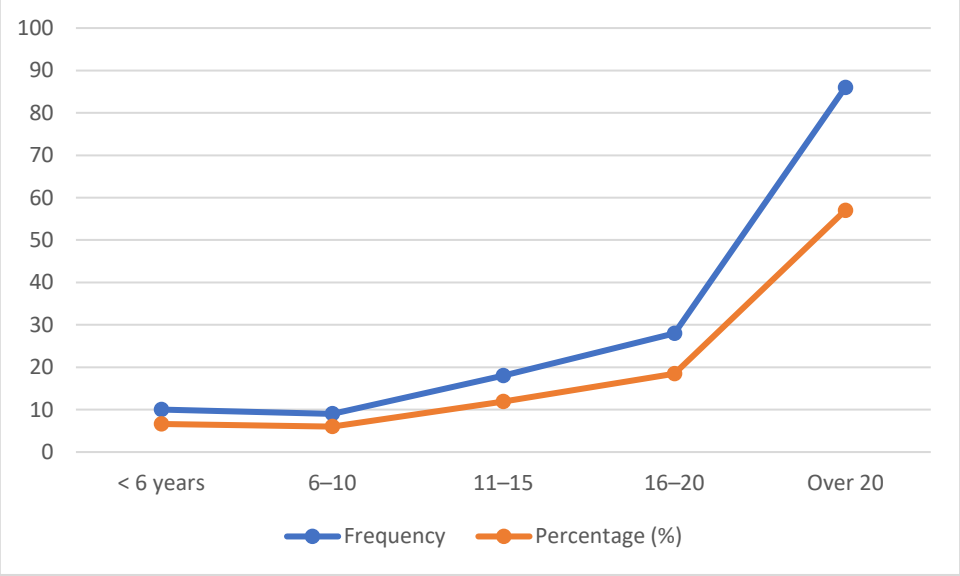
Experience (Years)	Frequency	Percentage (%)
None	47	31.1
1–5	57	37.7
6–10	23	15.2
Over 10	24	15.9

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683



Total Work Experience (n = 151)

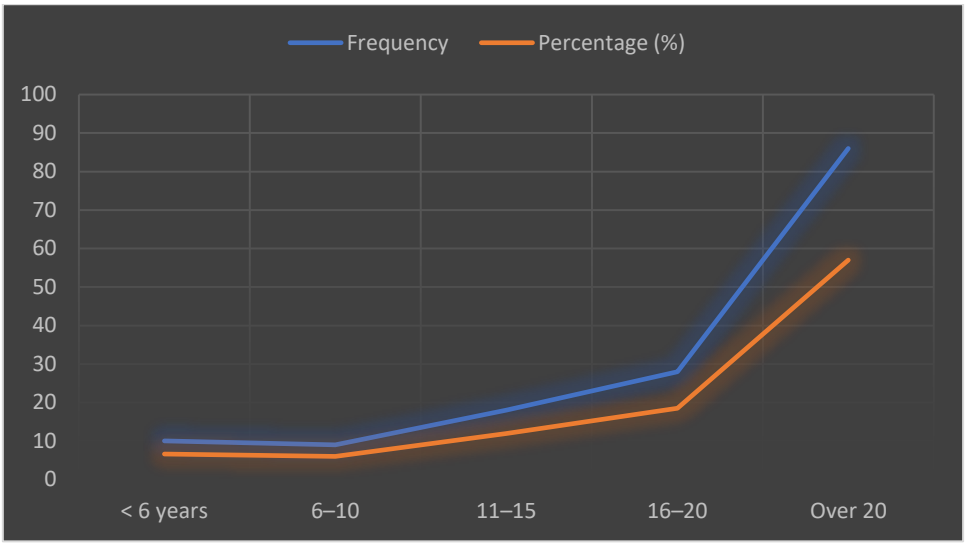
Experience (Years)	Frequency	Percentage (%)
< 6 years	10	6.6
6–10	9	6.0
11–15	18	11.9
16–20	28	18.5
Over 20	86	57.0



IT or CS Certification Possessed (n = 175)

Certifications	Frequency	Percentage (%)
None	72	41.10
One	56	32.01
Two	28	16.01
Three	10	5.70
Over Three	9	5.10

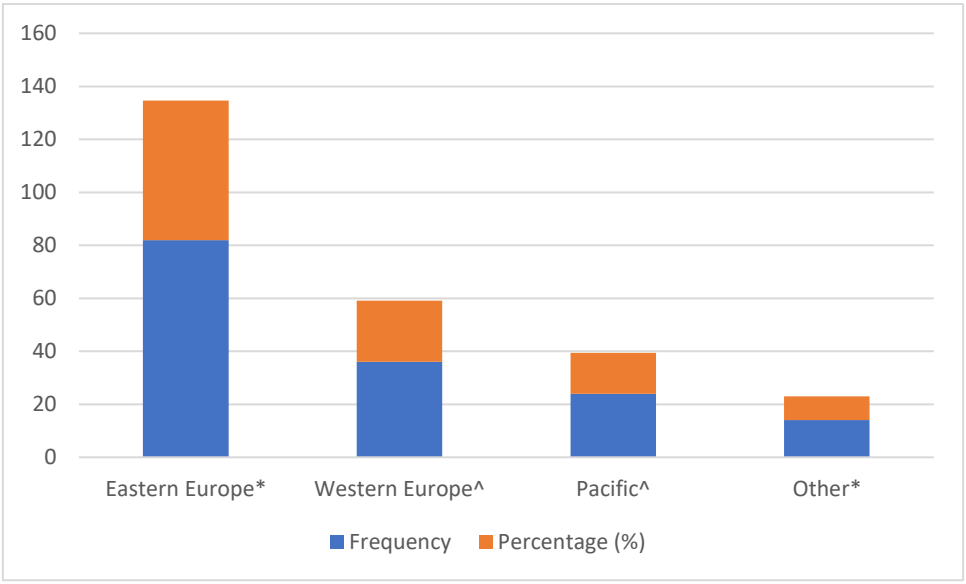
Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683



Panel B: Organizational Characteristics

Regional Distribution (n = 156)

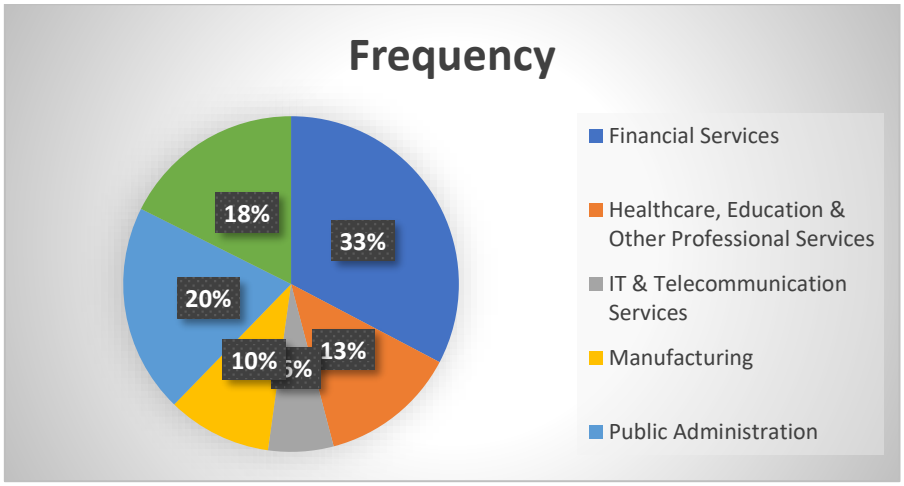
Region	Frequency	Percentage (%)
Eastern Europe*	82	52.60
Western Europe^	36	23.10
Pacific^	24	15.40
Other*	14	9.01



Industry Distribution (n = 159)

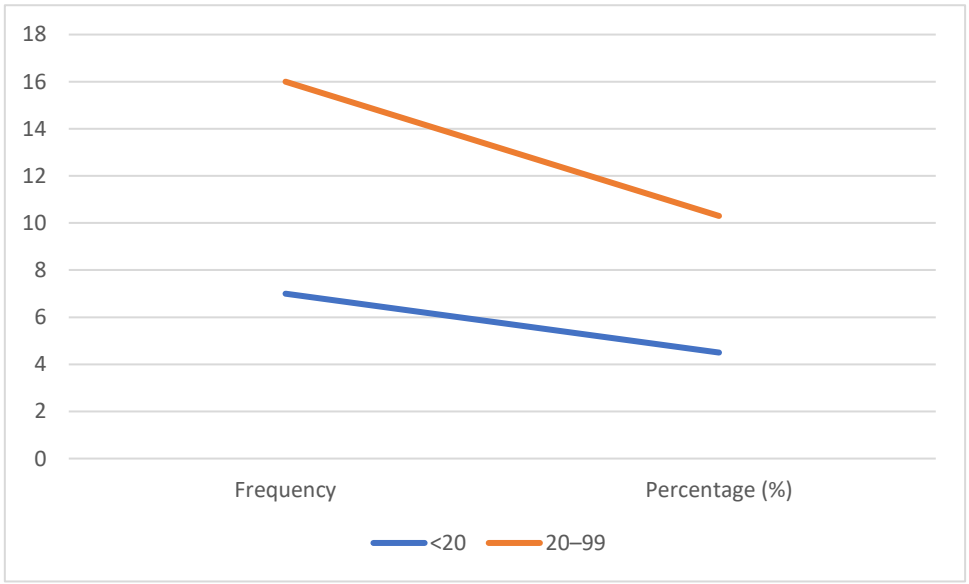
Industry	Frequency	Percentage (%)
Financial Services	52	32.70
Healthcare, Education & Other Professional Services	21	13.20
IT & Telecommunication Services	10	6.30
Manufacturing	16	10.10
Public Administration	32	20.10
Other*	28	17.60

Economic Sciences
https://economic-sciences.com
ES (2023) 19(1), 29-42 | ISSN:1505-4683



Company Size by Number of Employees (n = 156)

Company Size (Employees)	Frequency	Percentage (%)
<20	7	4.5
20–99	9	5.8



CONCLUSION

The option to employ any weights at all, or none at all, is subjective, and it affects the scores because of the weights we used to build the Index. In response to a worry that subjective weights would skew the results, we ran the same studies using raw indicators only, excluding the weights, and got the same overall picture. There have been some intriguing discoveries made via descriptive statistics. In our sample, CSA appears to have a relatively high effectiveness. As we intended for the Index to be difficult to acquire a high score—the maximum score could only be attained by firms with first- and second-line comprehensive CS processes, high IA competencies, and enough resources—this result is very encouraging. Nevertheless, it is important to use caution when drawing broad conclusions from

this discovery, as it is possible that some respondents were deterred from completing the survey due to the Index's complexity. In addition to the financial industry, other highly vulnerable businesses including health, education, professional services, and IT & telecommunications accounted for 20% of the participants (Audit Analytics, 2021). Nevertheless, there is a notable amount of diversity in the sample. Using co-sourcing or outsourcing assurance to third parties seems to make up for the incompetence of IAFs. Tighter alignment of the three phases is necessary due to the weak association between Planning and Reporting and Performing and Reporting. It appears that certain IAF are still able to give the Board a general view on CS risk management despite their low Planning and Performing effectiveness.

REFERENCES

1. Abdullatif, M., Kawuq, S., 2015. The role of internal auditing in risk management: evidence from banks in Jordan. J. Econ. Admin. Sci. 31 (1), 30–50. https://doi.org/ 10.1108/JEAS-08-2013-0025.
2. Arena, M., Azzone, G., 2009. Identifying organizational drivers of internal audit effectiveness. Int. J. Auditing 13, 43–60.
3. Association of Healthcare Internal Auditors (AHIA) and Deloitte (2017), "Cyber assurance: How internal audit, compliance and information technology can fight the good fight together?", available at: https://ahia.org/assets/Uploads/pdfUpload/WhitePapers/CyberAssuranceWhitePaper.pdf (accessed 15 June 2020).
4. Audit Analytics (2021), "Trend in Cybersecurity Breaches", available at: https://go.auditanalytics.com/cybersecurityreport (accessed 10 March 2021).
5. Australian National Audit Office (2002), "Benchmarking the Internal Audit Function", available at: https://www.anao.gov.au/sites/default/files/anao_report_2002- 2003_13.pdf (accessed 10 March 2021).
6. Bailey, K.D., 1994. Typologies and taxonomies: An introduction to classification techniques. Sage, Thousand Oaks, CA.
7. Beasley, M., Clune, R., Hermanson, D.R., 2005. Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. J. Account. Public Policy 24 (6), 521–531.
8. Bodeau, D., Graubart, R., 2016. Cyber resilience metrics: Key observations. The MITRE Corporation.
9. Boehm, J., Curcio N., Merrath, P., Shenton, L., St¨ ahle, T., 2019. The risk-based approach to cybersecurity. McKinsey's Our Insights, available at: https://www. mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity# (accessed 10 June 2020).
10. Brown, C.E., Wong, J.A., Baldwin, A.A., 2007. A review and analysis of the existing research streams in continuous auditing. J. Emerg. Technol. Account. 4 (1), 1–28. https://doi.org/10.2308/jeta.2007.4.1.1.
11. Busenbark, J.R., Yoon, H., Gamache, D.L., Withers, M.C., 2021. Omitted Variable Bias: Examining Management Research With the Impact Threshold of a Confounding Variable (ITCV). J. Manage. 01492063211006458.
12. Byrnes, P.E., Ames, B., Vasarhelyi, M.A., 2015. The current state of continuous auditing and continuous monitoring. In Audit Analytics and Continuous Audit: Looking Toward the Future, available at: https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Downloadable Documents/AuditAnalytics_ LookingTowardFuture.pdf (accessed 10 September 2020).
13. Carias, J. F., Labaka, L., Sarriegi, J. M., and Hernantes, J. (2018), "An approach to the modeling of cyber resilience management". In 2018 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.
14. Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. (2004), "The economic impact of cyber-attacks", available at: https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf (accessed 20 March 2021).
15. Chambers, A., 1992. Effective Internal Audits. Pitman Publishing, How to Plan and Implement. Chambers, R. (2014), "From Good to Great: Strategic Planning Can Define an Internal Audit Function", available at: https://iaonline.theiia.org/blogs/chambers/2014/Pages/From-Good-to-Great—Strategic-Planning-Can-Define-an-Internal-Audit-Function.aspx (accessed 11 April 2021).

16. Chartered Institute of Internal Auditors (2020), "How to gather and evaluate information Chartered Institute of Internal Auditors", available at: file:///C:/Users/ matejd/AppData/Local/Temp/How%20 to%20gather%20and%20evaluate%20information-1.pdf (accessed 20 June 2020).
17. European Confederation of Institutes of Internal Auditors (2020), "Risk in focus 2021. Hot topics for internal auditors", available at: https://www.eciia.eu/wpcontent/uploads/2020/09/100242-RISK-IN-FOCUS-2021-52PP-ECIIA-Online-V2.pdf (accessed 20 October 2020).
18. EY (2019), "How financial services organizations manage cyber risk", available at: https://www.ey.com/en_gl/consulting/how-financial-services-organizations-canmanage-cyber-risk. (accessed 11 August 2020).
19. Fadzil, F.H., Haron, H., Jantan, M., 2005. Internal auditing practices and internal control system. Managerial Audit. J. 20 (8), 844–866.
20. Federation of European Risk Management Associations (FERMA) (2019), "At the junction of corporate governance & cybersecurity", available at: https://www.eciia. eu/wp-content/uploads/ 2019/02/FERMA-Perspectives-Cyber-risk-governance-09.10.2018_0.pdf (accessed 16 March 2020).
21. Rahul Kalva. Revolutionizing healthcare cybersecurity a generative AI-Driven MLOps framework for proactive threat detection and mitigation, World Journal of Advanced Research and Reviews, v. 13, n. 3, p. 577-582, 2022.
22. Ankush Reddy Sugureddy. Enhancing data governance frameworks with AI/ML: strategies for modern enterprises. International Journal of Data Analytics (IJDA), 2(1), 2022, pp. 12-22.
23. Ankush Reddy Sugureddy. Utilizing generative AI for real-time data governance and privacy solutions. International Journal of Artificial Intelligence & Machine Learning (IJAIML), 1(1), 2022, pp. 92-101.
24. Sudeesh Goriparthi. Leveraging AIML for advanced data governance enhancing data quality and compliance monitoring. International Journal of Data Analytics (IJDA), 2(1), 2022, pp. 1-11
25. Sudeesh Goriparthi. Implementing robust data governance frameworks: the role of AI/ML in ensuring data integrity and compliance. International Journal of Artificial Intelligence & Machine Learning (IJAIML), 1(1), 2022, pp. 83-91.