UNIVERSITI TEKNOLOGI MARA | Cawangan Terengganu Kampus Dungun

FIELD REPORT

PAC 671

FACULTY OF ACCOUNTANCY

NAME	**NURMAISARAH BINTI MOHD JOHARI**
STUDENT ID	**2020495658**
CLASS	**TAC2208A**
PREPARED FOR	**PUAN NORLINDA ZAINAL ABDUL**

TABLE OF CONTENT

SECTION A **PAGE**

SECTION B

SECTION A

1.0 Introduction

Mohamed Asri & Co is a firm that was established in November 1996, in Temerloh Pahang and one branch in Kuantan, Pahang. The services offered at this firm are audit, taxation consultancy, accounting, management consultancy, mergers and acquisitions. There are more than 300 private and government companies managed by Mohamed Asri & Co at the Kuantan branch. I chose to be practical here because of the firm's extensive experience in related fields. I was assigned to audit department.

This firm is authorized to audit companies and cooperative accounts regardless of whether they are small or large, giving an independent opinion on the financial statements submitted. A firm that audits financial statements may also evaluate the efficiency of the accounting system, client reports, and budgets, and they can recommend new procedures to ensure that the business operates more profitably while minimising expenses. Here I can train myself in the skills of becoming an external audit person. Various knowledge and techniques taught by the employees at this firm.

The employees at Mohamed Asri n Co are very cooperative when a student like me asks something I don't understand in this audit job. They also gave me the opportunity and experience to do a field audit. This has made me better understand how audit work is done and how audit works in business. While studying, I didn't understand what audit work was, but when I went through it, I understood better what audit work was like and made me a little interested in continuing my work as an audit.

2.0 Summary of Work Done

So basically, Mohammed Asri & Co audits is companies and cooperative accounts regardless of whether they are small or large by providing an independent opinion on the financial statements presented. When auditing a financial statement, the Company can check the effectiveness of the accounting system, reports and budgets of clients and recommend new methods so that business can be run more smoothly. I was placed in the accounting department. At first my job was just to help my supervisor. I do a statutory audit, cross reference or double check the audit work made by my supervisor in terms of spelling, numbers are the same as financial statements and vocabulary. In the middle of month 3, I along with my two seniors went to audit the client firm. There I was taught how to make audit vouching and collect crucial vouching as proof for audit.

In addition, I have also been given the opportunity to audit two large companies, which is Raub District Council and Jerantut District Council. I was given the task to audit the expenses section of the financial statements. During my outstation at the two councils, I was also able to learn to see the assets purchased by the Council in the current year as physical evidence of their purchase, making audit vouching and communicate skill with clients. In addition, I have been given the trust to audit a small company alone but with a little help from my supervisor. When doing this audit task, I just saw and understood how the audit job works since the company I work for is more of an external audit. So, there are a lot of external clients that we need to audit.

3.0 Strengths & Weaknesses of Training

During my internship at Mohamed Asri & Co, I gained a variety of auditing experiences. I was exposed to various auditing tasks such as statutory audit, cross reference and vouching which played an important role in developing practical skills. My involvement in both large and small businesses provide valuable insight into different scales of operations. Participating in field audits provides practical experience, improves understanding of auditing expenses, reviews physical assets and gathers important evidence. The supportive environment at Mohamed Asri & Co also plays an important role in the learning process. The Collaborative nature of the employees ensures that I can seek guidance and ask questions when needed, allowing me to learn directly from more experienced professionals.

This experience was further enriched when the Company gave me a Trust to audit a small Company by myself, demonstrating the firm's confidence in my abilities and fostering Work Skills. Throughout the training, I was able to develop important skills such as communicating with clients, understanding the accounting system and mastering audit procedures. The company's benefits include paid time off (PTO); however, as students, we do not receive annual leave. Nevertheless, if we have MC and are unwell, our allowance remains intact and will be counted as working days. Furthermore, others company's benefits include hands-on experience. As a practical student, I had the opportunity to get real-world experience as an external auditor. I need to write a working paper audit with other auditors in the company I work for, which will allow me to apply academic knowledge and acquire practical skills for my future profession.

Even with the wealth of expertise accumulated in the audit division, Mohamed Asri & Co's training programme has several shortcomings. The audit department is the exclusive area of exposure, meaning that working in other fields like taxation consulting, management consulting, or mergers and acquisitions—which might offer a more complete experience—is not possible. My initial work consisted primarily of supportive tasks, such as assisting managers with spelling and maths corrections, however not very difficult or engaging. Only in the middle of the third month did significant fieldwork experience start, indicating that more regular fieldwork chances during training can improve the development of practical skills.

Next, employers are anxious to get new trainees on the work quickly in order to maximise the use of resources, thus charitable training is sometimes a hurried affair. This haste can have serious negative effects, such as the early development of ambiguity and misunderstanding. Pushing through the training process too fast might leave trainees with a lack of confidence in their skills as well as an incomplete understanding of crucial ideas and procedures. Their performance may suffer, but it may also have a negative impact on their general job happiness and long-term professional growth. The urge to expedite training also leads to partial or superficial learning, in which students are exposed to the bare minimum without developing a thorough comprehension of the activities that are required of them.

Furthermore, when trainees are expected to engage in projects and learn the process at the same time, low productivity can become a serious problem. This method can be laborious since it necessitates explaining each stage of the activity to the trainee before permitting them to go, which may cause the task to take longer to complete. Because of this, the time of both the trainer and the trainee is wasted, which may have an adverse effect on the project's overall productivity. Such delays may result in late deliveries, which may have a detrimental impact on the project's performance and the organization's reputation. They may also cause low work satisfaction and unfavourable ratings.

4.0 Self-Reflection

Reflecting on my training at Mohamed Asri & Co, Chartered Accountants, I see how critical it is that we comprehend how dynamic the workplace is. At first, there was a lot of idle time during the off-peak season due to the lack of job. It's a difficult time for me since I need to figure out how to continue being enthusiastic at work. The several proactive strategies I employ to request additional work and a reduced burden leading to intense ennui and a feeling of immobility. I learned from this experience how crucial it is to be self-motivated and to make the most of your downtime—two abilities that are crucial in every workplace.

As my practice increased, I realized how important it was to be flexible and patient. More possibilities for practical practice, like reviewing financial statements, filling out audit vouchers, and interacting with clients, will be available in the upcoming months. These assignments help me develop not just my technical abilities but also my teamwork and client-facing communication skills. Understanding the procedures and difficulties of auditing in the actual world is provided by experience auditing major organisations. All things considered, my internship has been a worthwhile educational experience that has highlighted the significance of tenacity, flexibility, and proactive involvement in career advancement.

SECTION B – ENHANCING ACCOUNTING SYSTEMS IN AN ERA OF CYBER THREAT

1.0 INTRODUCTION

In an era of unprecedented technological progress, the accounting industry has experienced significant transformations. A company's digitization of operations to increase productivity and optimize workflows will introduce a number of cyberthreats into the accounting system, including the possibility of data loss, inaccurate data entry, and misuse of private information. Without a question, these developments have made communication and information sharing more effective. Data and information can now be shared widely and effortlessly thanks to significant technological advancements. In order to guarantee that account system security becomes a top concern for many businesses in the age of cyber threats, it is imperative that the system be improved.

The integration of technology into accounting processes creates unprecedented opportunity for innovation and growth, but it also exposes firms to new risks. However, by embracing sophisticated technology and implementing strong cyber security measures, a company can not only lower the danger caused by cyber threats, but also increase the efficiency, accuracy, and dependability of its accounting procedures. Furthermore, the possibility of restructuring an enterprise's accounting department by reassigning the operational duties of accounting specialists to enterprise cyber security is investigated. provides suggestions to base the creation of cyber security regulations on enterprise accounting policies and the internal regulations that go along with them. It is obvious that accounting and corporate control operations require frequent security assessments. Information barriers and real risks to the efficient functioning of economic entities can be prevented, avoided, and eliminated by an enterprise by having an external expert from an audit company or an internal controller of the account monitor and test the cyber security system.

2.0 Issue and Problem Statement

2.1 Data Breaches

A data breach is the deliberate or accidental disclosure of confidential information to an unauthorized party. In today's digital age, data has become one of the most critical components in an Enterprise. A data leak can cause serious damage to organizations, including significant reputational damage and financial loss. Cybersecurity incidents are thought to pose a thousand of dollar threat to some individuals. Significant data breaches caused by cyberattacks can have devastating impact on account systems and even businesses. In addition to posing a serious risk to confidence and reputation, a data breach may also result in lost revenue or a drop in the share price of a company that is publicly traded.

Accounting information systems are vulnerable to a number of risks, particularly when they connect with the internet. Scientists, auditors, and management accountants should be concerned about this issue. Researchers provide sufficient consideration to identifying hazards and potential threats to the security of accounting data. Popivniak M. highlights a number of issues, including the use of flimsy methods to authenticate users of accounting information, the disregard for workplace computer security regulations or other access-control measures, and the disregard for accounting data preservation guidelines. Systems being compromised by irresponsible persons is one of the issues linked to data breaches. For instance, a number of computers were used to steal client and employee information from an accounting firm that was compromised.

Regretfully, there is no encryption on this data. A few consumers filed claims for damages after being victims to identity theft. In addition, the firm also had to bear the significant cost of notifying all affected customers and employees by providing two years of monitoring service credit. Organisations are at serious risk from data breaches, which may have disastrous effects on accounting systems. Cyberattacks that have the potential to cause large financial losses, harm to one's reputation, and legal repercussions frequently cause these breaches. The revelation of private data, including financial records and individual customer information, can erode confidence and lead to a decline in sales and a decrease in shareholder value. In addition, a data breach may create delay and lost productivity while systems are being rebuilt and safeguarded.

2.2 Employee Training and Awareness

The promotion of training programmes and staff knowledge is the second concern to strengthen the account system against cyberattacks. This is to encourage staff members to be security-ready so they can safeguard the organization's sensitive data, including the accounting system. Why is the training and awareness is required? Human mistake is the primary cause. In cybersecurity, employees are frequently the weakest link. Serious security breaches can result from human mistake, such as falling for phishing schemes or managing sensitive data incorrectly. Employees may unintentionally end up being the weakest point in a company's defence against cyberattacks if they are not properly trained. This flaw may result in data leaks, big financial losses, and illegal access to financial details. Employees lacking proper training may unintentionally bring malware or ransomware into systems, which can seriously interrupt corporate operations and need expensive cleanup efforts.

Small firms sometimes operate with little resources and may not prioritise cybersecurity as a critical component of their operations. Unlike major firms, which can afford specialised cybersecurity teams and sophisticated defence mechanisms, small businesses sometimes lack the financial means to invest in a strong cybersecurity infrastructure. This presents a weakness that hackers may exploit since they know that firms may have inadequate defences and security procedures. In 2019, 80% of cybercrimes targeted small businesses via public services, social media, and postal services, according to the Internet Security Threats report. The absence of departments and specialists to maintain cyber security is the primary cause of cyberattacks targeting small organisations. As a result, there is a greater likelihood that these cyberattacks will be effective against these companies.

In today's increasingly linked and digital world, the need of safeguarding accounting systems from cyber threats cannot be overstated. While Malaysia does not currently face as serious a cyber threat as other areas, the global nature of cybercrime implies that there are no huge organisations. As hackers' strategies improve, Malaysia's small and medium companies (SMEs) must be proactive in planning for any cyber events. However, in order to prevent unintended events, we must be ready. Organisations may greatly bolster their defences against cyberattacks, safeguard confidential data, and foster an organisational cyber security culture by investing in thorough staff training and initiative awareness is critical in this respect.

3.0 Literature Review

Numerous scientists have studied the issue of accounting data security in light of current macro- and micro-level cyberthreats. Specifically, Yu. Maroz and Yu. Tsal-Tsalko define cyber security in detail from an accounting perspective. They draw it in as a danger to the enterprise's vital interests, including those related to people and intellectual property, trade secrets, proprietary technology, profit, added value, and markets; information generated by the accounting system and made available by particular laws; economics; organisational controls; and technical [2, page 9]. The fundamental guidelines for handling the cyber security of accounting data were established by S. Viter and I. Vitlyshyn. These guidelines included software support, safeguarding private information, individual accountability, secrecy, completeness, and control over who may access accounting data. [3, page 501].

The majority of scientists link the growing advancements in computer and communication technologies to the necessity of cyber security on both a micro and global scale. The rise of internet and the digitalization of socioeconomic processes have led to an increase in criminal activity with the intention of causing harm in addition to illegitimate financial gain. Recent international research has debunked the theory that increased use of information processing technology in social and commercial activities necessitates more proactive cyber security. By examining the correlation between the advancement of ICT and the degree of cyber security, we can determine that several nations exhibit an imbalance in these metrics. Put another way, the degree of digitalization of socio-economic activities in this nation has no direct bearing on the evolution of the cyber security system. Therefore, potential barriers and informational dangers rather than the degree of digitalization of socioeconomic operations are what are driving the advancement of cyber security.

.

4.0 Recommendation

4.1 Network Security Protocols

Data breaches are a huge threat to organizations, resulting in financial losses, reputational harm, and potential legal consequences. These breaches are frequently the result of network security flaws such as poor encryption, insufficient access controls, and unpatched software. To reduce this danger, organizations must have strong network security protocols that protect data confidentiality, integrity and availability. The purpose of network security protocols is to guarantee the confidentiality and integrity of data transferred via network connections. The type of data being protected and the network connection determine the precise network security protocol to be utilized.

Every protocol outlines the methods and practices needed to safeguard network data from harmful or unauthorized work to read or extract information. Organisations that apply these regulations can lower the risk of data interception and unauthorised access. In addition to implementing this protocol, organisations should create a detailed software usage policy. This policy must require frequent updates and patches for all software, including operating systems, applications, and firmware, in order to defend against known vulnerabilities. Ensuring software authenticity through appropriate licencing and avoiding counterfeit goods is critical to a safe environment. Synchronising security systems, such as firewalls and antivirus programmes, enables uniform protection across networks, minimising possible attacker access points.

Effective access control is an important part of defending against data breaches. Implementing role-based access control (RBAC) helps guarantee that workers only have access to information necessary for their job tasks, hence limiting possible insider threats. Furthermore, multi-factor authentication (MBA) will increase security by demanding various forms of authentication before giving access to critical data and systems. Limiting the usage of an organization's software and hardware for personal reasons helps to avoid unauthorised access and potential security breaches. Combining these Steps with continuing staff training on cybersecurity best practices promotes a security-conscious culture, decreases the possibility of human error, and strengthens the organization's data breach defences.

4.2 Empowering Employees

Employee training and awareness are crucial for improving an organization's defences against data breaches and other cyber security risks. Despite strong security measures, human error remains a major threat. To address this, organisations should create comprehensive training programmes that cover basic safety concepts, industry-specific hazards, and practical risk-reduction measures. Employees should also get training and workshops to ensure they are aware of the most recent cyber risks and understand their role in maintaining security. Training should be required for all staff, including new recruits, as part of their onboarding process. In other words, cyber security solutions do not ensure that the company will be adequately protected against all threats. Cyber security systems may have detection flaws, necessitating security audit services.

Internal accounting specialists may be given permission to undertake continuous security audits, or this job may be delegated to external independent auditors and consulting organisations. A security audit's primary goal is to offer a complete, systematic assessment of information risks that impact the Enterprise's economic operations and cyber security. An accounting specialist should monitor the effectiveness of firewalls, antivirus software, the state of updating computer programmes, particularly to the latest version, and the use of strong passwords by employees to protect confidential information, a comprehensive combination. These abilities and expertise will aid security auditors in detecting internal and external risks. Testing the company's information systems is an efficient approach of monitoring cyber security.

The most time-consuming aspect of the security audit is screening the Company's employees for potential breaches of valuable information. Phishing mailing lists can help security auditors discover corporate employees who are prone to cyber dangers and eager to share personal sensitive information. It is also critical to evaluate certain cyber threat software and computer antivirus programmes' abilities to identify different sorts of infections. To hire internal and external security auditing professionals, as well as accounting specialists. An organisation should sacrifice money and give advantages to its personnel in order to seek new information and contribute to the organization's overall safety. Establishing a comprehensive programme for employee training and awareness lowers the risk of data breaches and other cyber dangers while also empowering staff to defend the company and themselves.

5.0 Conclusion

In conclusion, integrating cutting-edge technology into the accounting system is necessary to increase its security against cyberw2crime and to provide a host of benefits related to productivity, efficiency, and creativity. The growing use of advanced technology and processes by enterprises will make potential cyber threats like ransomware, phishing attempts, and data breaches more noticeable. Serious repercussions, such as monetary loss, harm to one's reputation, and compromised data integrity, may result from these attacks. Thus, in order to guard against a variety of hazardous threats, it is critical for an organisation to give strengthening their accounting system top priority.

A multipronged strategy with strong network security standards and extensive personnel training and awareness initiatives is needed to counter these cyberthreats. The danger of unauthorised access and serious data breaches may be decreased by putting strong encryption techniques, frequent software upgrades, and efficient access restrictions into place. In addition, training staff members on current threats and cybersecurity best practices may assist lower human error rates, which are frequently the weakest link in an organization's security protocol. Organisations may build a strong defence against cyber threats by advocating for security awareness among staff members and making sure they have the requisite knowledge and abilities.

Ultimately, developing an integrated security framework that integrates technology, policy, and people is just as important for enhancing accounting systems in this age of cyber dangers as using the newest technological advancements. Frequent internal and external security audits can help firms keep ahead of new threats by offering insightful information about possible weaknesses. We can safeguard sensitive financial data and maintain the trust and confidence of our stakeholders by making significant investments in a comprehensive cyber security system and encouraging a proactive approach to business security. This will create more opportunities for sustainable growth and innovation in the digital age.

References

1. Lehenchuk, S., Vygivska, M., & Hryhorevska, O. (2022). Protection of accounting information in the conditions of cyber security. *Problemi Teorìï Ta Metodologìï Buhgalters'kogo Oblìku, Kontrolû Ì Analìzu*, *2(52)*, 40–46

https://www.researchgate.net/publication/366050111_Protection_of_accounting_information_in_the_conditions_of_cyber_security

2. Mat, B., Pero, S. D. M., Wahid, R., & Shuib, M. S. (2020). Cyber Security Threats to Malaysia: A Small State Security Discourse. *ResearchGate*

https://www.researchgate.net/publication/349881373_Cyber_Security_Threats_to_Malaysia_A_Small_State_Security_Discourse.

3. Zadorozhnyi, Z., Muravskyi., & Shevchuk, O. (2020). The Accounting System as The Basic for Organising Enterprise Cybersecurity.

https://www.researchgate.net/publication/346745367_THE_ACCOUNTING_SYSTEM_AS_THE_BASIS_FOR_ORGANISING_ENTERPRISE_CYBERSECURITY

4. Cheng, L., Liu F., & Yao, D. (2017). Enterprise data breach : causes, challenges, preventation and future directions. *Wiley Interdisciplinary Reviews. Data mining and Knowledge Discovery*

https://www.researchgate.net/publication/318152978_Enterprise_data_breach_causes_challenges_prevention_and_future_directions_Enterprise_data_breach

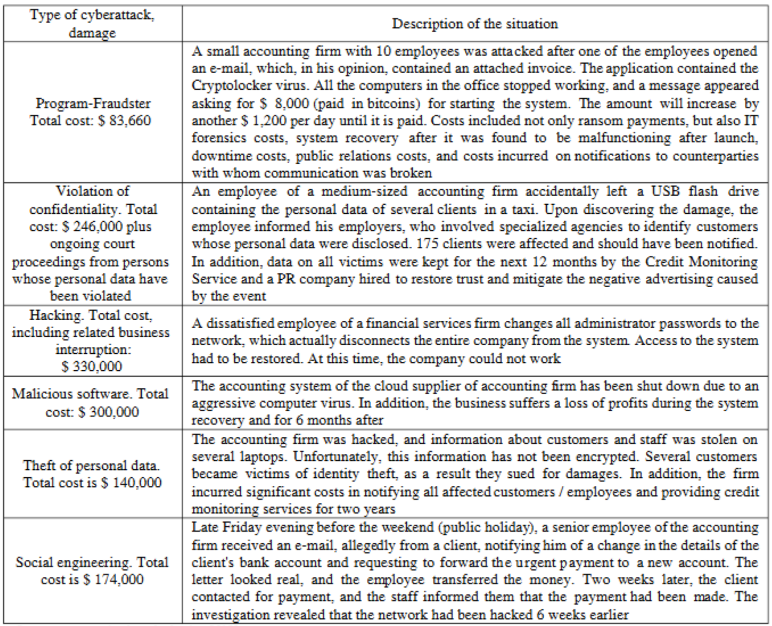
5. Dileep, K., Venkatesh, R., Kumar, B., Rao, U., & Kshatra, P. (2020). Analysis of Data Breaches and Its impact on Organizations. *International Journal of Emerging Trends in Engineering Research.*

(PDF) Analysis of Data Breaches and Its impact on Organizations (researchgate.net)

Appendix

Table 2

Examples of the impact of cyberattacks on the accounting system and related costs (on the example of outsourcing companies in Australia)



Type of cyberattack, damage	Description of the situation
Program-Fraudster Total cost: $ 83,660	A small accounting firm with 10 employees was attacked after one of the employees opened an e-mail, which, in his opinion, contained an attached invoice. The application contained the Cryptolocker virus. All the computers in the office stopped working, and a message appeared asking for $ 8,000 (paid in bitcoins) for starting the system. The amount will increase by another $ 1,200 per day until it is paid. Costs included not only ransom payments, but also IT forensics costs, system recovery after it was found to be malfunctioning after launch, downtime costs, public relations costs, and costs incurred on notifications to counterparties with whom communication was broken
Violation of confidentiality. Total cost: $ 246,000 plus ongoing court proceedings from persons whose personal data have been violated	An employee of a medium-sized accounting firm accidentally left a USB flash drive containing the personal data of several clients in a taxi. Upon discovering the damage, the employee informed his employers, who involved specialized agencies to identify customers whose personal data were disclosed. 175 clients were affected and should have been notified. In addition, data on all victims were kept for the next 12 months by the Credit Monitoring Service and a PR company hired to restore trust and mitigate the negative advertising caused by the event
Hacking. Total cost, including related business interruption: $ 330,000	A dissatisfied employee of a financial services firm changes all administrator passwords to the network, which actually disconnects the entire company from the system. Access to the system had to be restored. At this time, the company could not work
Malicious software. Total cost: $ 300,000	The accounting system of the cloud supplier of accounting firm has been shut down due to an aggressive computer virus. In addition, the business suffers a loss of profits during the system recovery and for 6 months after
Theft of personal data. Total cost is $ 140,000	The accounting firm was hacked, and information about customers and staff was stolen on several laptops. Unfortunately, this information has not been encrypted. Several customers became victims of identity theft, as a result they sued for damages. In addition, the firm incurred significant costs in notifying all affected customers / employees and providing credit monitoring services for two years
Social engineering. Total cost is $ 174,000	Late Friday evening before the weekend (public holiday), a senior employee of the accounting firm received an e-mail, allegedly from a client, notifying him of a change in the details of the client's bank account and requesting to forward the urgent payment to a new account. The letter looked real, and the employee transferred the money. Two weeks later, the client contacted for payment, and the staff informed them that the payment had been made. The investigation revealed that the network had been hacked 6 weeks earlier

Source: systematized on the basis of [13]

FINANCIAL AND CREDIT ACTIVITIES: PROBLEMS OF THEORY AND PRACTICE 2020 № 3 (34)

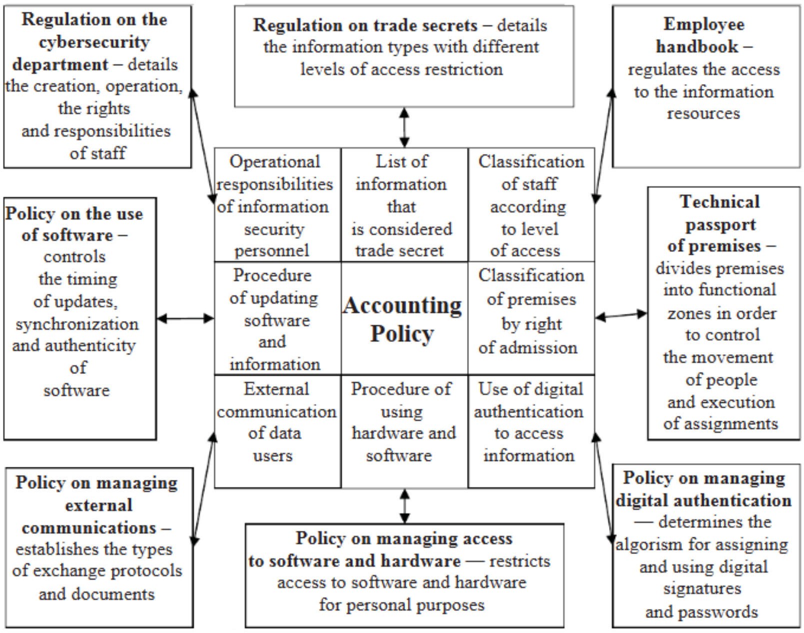

Regulation on the cybersecurity department – details the creation, operation, the rights and responsibilities of staff
Regulation on trade secrets – details the information types with different levels of access restriction
Employee handbook – regulates the access to the information resources
Operational responsibilities of information security personnel
List of information that is considered trade secret
Classification of staff according to level of access
Policy on the use of software – controls the timing of updates, synchronization and authenticity of software
Technical passport of premises – divides premises into functional zones in order to control the movement of people and execution of assignments
Procedure of updating software and information
Accounting Policy
Classification of premises by right of admission
External communication of data users
Procedure of using hardware and software
Use of digital authentication to access information
Policy on managing external communications – establishes the types of exchange protocols and documents
Policy on managing access to software and hardware — restricts access to software and hardware for personal purposes
Policy on managing digital authentication — determines the algorism for assigning and using digital signatures and passwords

Fig. **Security protocols documented in the enterprise accounting policy and internal regulations**