UNIVERSITI TEKNOLOGI MARA

Fakulti Perakaunan

FIELD REPORT

PAC 671

FACULTY OF ACCOUNTANCY

UNIVERSITI TEKNOLOGI MARA

UiTM CAWANGAN TERENGGANU

NAME : NUR KHAIRUNNISA BINTI SAHUDIN

STUDENT ID : 2020834576

SUPERVISOR (UiTM) : EN. SYAFIQ BIN ABDUL HARIS HALMI

TABLE OF CONTENTS

PART A

1.0 INTRODUCTION

AC220 Bachelor of Accountancy students at Universiti Teknologi MARA (UiTM) must complete Industrial Training (PAC671). This internship program offers students the chance to gain real-world experience and learn new skills. It provides excellent opportunities for students to apply their knowledge and abilities in the appropriate sector. We were allowed to examine employment options based on our bachelor's degree. Accounting students can pick from several occupations, including auditor, accountant, tax consultant, and many more. The exposure of each career varies depending on the organization or corporation we select.

I am now completing my internship program with Prestige One Stop Advisory PLT in Sekinchan, Selangor, from March 4th to August 30th, 2024. Prestige One Stop Advisory PLT, established with a commitment to excellence in 2014, specializes in providing comprehensive financial services including accounting, taxation, and secretarial services. Prestige caters to a diverse clientele ranging from small and medium-sized enterprises (SMEs) to multinational corporations (MNCs) across various industries such as manufacturing, retail, technology, healthcare, and professional services. Prestige's core services encompass meticulous bookkeeping, financial statement preparation, budgeting, and cash flow management, ensuring accurate and timely financial reporting to support informed decision-making by our clients. In taxation, our seasoned professionals offer strategic guidance on tax compliance, optimization, and planning, aimed at minimizing liabilities and maximizing savings. Additionally, our secretarial services encompass company incorporation, maintenance of statutory registers, and filing of annual returns, meticulously ensuring compliance with regulatory obligations

2.0 SUMMARY OF WORK DONE

i. Recording The Transactions

Recording transactions is a fundamental task in the field of accounting, essential for maintaining accurate and trustworthy financial records for businesses and organisations. At its foundation, this procedure is methodically collecting and documenting numerous financial transactions that take place within the company. One of the key responsibilities of a bookkeeper is to keep complete records of all financial activities. This includes but is not limited to, recording sales transactions in which products or services are sold to consumers, documenting purchases from suppliers or vendors, recording payments made to settle obligations or costs, and recording revenues from customers or other sources of income.

ii. Classification and Categorization

The classification and categorizing of financial transactions is an important part of accounting that ensures exact and transparent financial reporting inside organizations. This procedure entails carefully organizing and allocating transactions to specified accounts by established accounting rules such as Generally Accepted Accounting rules (GAAP) or International Financial Reporting Standards (IFRS). At its foundation, correct categorization is critical in presenting an organization's genuine financial status and performance. Each transaction must be thoroughly categorized into relevant accounts, such as income, costs, assets, liabilities, and equity. Revenue accounts record money from fundamental company operations such as sales of products or services, interest earned, and rental income. Expense accounts include costs spent during business operations, such as salary, rent, utilities, and administrative fees. Asset accounts reflect the organization's resources, such as cash, accounts receivable, inventory, property, plant, and equipment. Liabilities accounts indicate the organization's responsibilities, such as accounts payable, loans, accrued costs, and delayed revenues.

iii. Bank Reconciliation

Bank reconciliation is an important step in bookkeeping that ensures the correctness and dependability of financial records, particularly when dealing with credit card transactions and electronic payment systems such as Touch 'n Go. This procedure entails comparing and matching transactions recorded in the company's accounting system to those indicated on bank statements from financial institutions.

To resolve disputes in credit card transactions, bookkeepers methodically review charges and credits against the company's records. Similarly, transactions done with electronic payment methods are reconciled to ensure that all expenditures and payments are correctly recorded. It can identify and carefully investigates inconsistencies such as missing transactions, erroneous sums, and unauthorised payments. This investigation procedure involves checking supporting paperwork, contacting financial institutions or vendors for clarification, and swiftly correcting problems. Bank reconciliation helps to avoid financial misstatements and unauthorised operations, protecting the organization's assets and guaranteeing regulatory compliance.

3.0 STRENGTHS & WEAKNESSES OF TRAINING

3.1 Strengths

i. Strengthen Essential Technical Skills

Training at an accounting business gives me a thorough chance to hone my important technical skills, which are critical for success in accounting and financial management positions. Through organized programs, I gain competency in critical areas such as utilizing accounting software for effective financial data management and reporting. I also obtain a complete grasp of financial documents, such as balance sheets and income statements, which allows for correct analysis of financial performance. These technical abilities enable professionals to efficiently conduct day-to-day accounting operations, offer correct financial reporting, and give useful insights that assist organisational decision-making.

ii. Supportive Teamwork and Collaboration

Teamwork and cooperation are essential characteristics in the dynamic and linked world of accounting businesses. These organisations thrive on their teams' aggregate experience and work together to provide full financial services and advisory assistance to their clients. Accounting businesses' training programmes are carefully intended to build and improve people's vital abilities. Effective cooperation in an accounting business includes more than simply working together; it also entails combining varied talents and views to achieve common goals. Training enables people to acquire excellent interpersonal skills, which create open communication and mutual respect among team members. Individuals in a collaborative setting are encouraged to use their unique abilities and experience to help the team achieve its

goals. Individuals acquire exposure to all aspects of accounting practice through collaborative projects and assignments, which enhance their professional talents and instill confidence in their ability to achieve outcomes as part of a cohesive team.

iii. Work-Life Balance

Maintaining a healthy work-life balance while training at an accounting company is critical for both personal and professional growth. Accounting training is typically tough, requiring professionals to properly handle strict schedules and obligations. To preserve a sense of balance, prioritise time management tactics that allow for devoted personal time in addition to business responsibilities. Setting clear boundaries between work and personal life might help you avoid burnout and retain mental clarity. Taking regular pauses during the day boosts productivity and decreases stress, while prioritising physical health via exercise, right diet, and enough rest improves overall vitality. Furthermore, cultivating hobbies, personal interests, and relaxation activities outside of work helps to promote a well-rounded lifestyle.

3.2 Weaknesses

i. Dependence On Key Personnel.

Dependency on key persons is a major worry for many accounting businesses, since the knowledge, client contacts, and leadership of a few key individuals may have a considerable influence on the firm's stability and development trajectory. These individuals frequently have considerable industry expertise, strong client relationships developed over years of service, and a strategic vision that propels the business forward. One of the most significant hazards connected with such reliance is the possible disruption produced by the departure or retirement of these essential persons. Their departure might leave a hole that is difficult to replace quickly, leading to uncertainty among clients, employees, and stakeholders. Client relationships based on trust and personal rapport may suffer, since clients may prefer to work with known faces who understand their individual needs.

4.0 SELF-REFLECTION

During my internship at Prestige One Stop Advisory Plt, I engaged myself in the dynamic world of accounting, getting invaluable hands-on experience that went beyond the scope of textbook study. I dug into the complexities of accounting methods, seeing firsthand how accountants methodically handle and reconcile financial information. One of the most meaningful things I learned was the need for fundamental and technical abilities in the accounting profession. Beyond academic knowledge, I strengthened my practical abilities in financial analysis, reporting, and auditing. These abilities are more than simply academic exercises; they are crucial tools that accountants use daily to guarantee correctness and compliance. Furthermore, my experience demonstrated the need of excellent communication across account teams. Collaborating with colleagues highlighted the need of clear, succinct communication in presenting financial results and suggestions. This competence is essential for both internal cooperation and developing great client connections. Speaking about clients, I got the opportunity to work with a wide range of firms during my internship. This experience broadened my awareness of various accounting approaches and techniques designed for different businesses.

PART B

Protecting Accounting Data and Information with Strong Cybersecurity Is Essential.

1.0 INTRODUCTION

Cybersecurity is an essential safeguard for organizations and economies throughout the world, protecting sensitive data and maintaining operational integrity. Definition of Cyber Security: Gaps and Overlaps in Standardisation (ENISA, 2016). It is critical in ensuring financial transparency, enabling informed decision-making, and preserving regulatory compliance across a wide range of industries, including banking, healthcare, manufacturing, technology, retail, and agriculture. Cybersecurity is viewed as a major issue for all types of companies. (Mangelsdorf, 2017), either private or public. As the digital world evolves, so does the value of cybersecurity. Technological advancements have revolutionized cybersecurity practices, including cutting-edge technologies such as blockchain, artificial intelligence (AI), big data analytics, and cloud computing. These enhancements not only increase the efficiency of cybersecurity measures, but they also defend organizations against sophisticated cyber-attacks. In today's digital era, cybersecurity specialists are increasingly responsible for developing robust defences against data breaches, unauthorized access, and other cyber dangers. The proactive deployment of current cybersecurity technology not only decreases risks but also ensures that company operations remain resilient in the face of escalating cyber threats. Looking ahead, cybersecurity will continue to play an important role in determining the future of corporate operations and economic stability. As organisations traverse the intricacies of the digital world, investing in strong cybersecurity frameworks becomes critical for protecting valuable assets, retaining stakeholder confidence, and achieving long-term success in an interconnected global economy.

During my internship at Prestige One Stop Advisory Plt, I learned that, while data and information are critical components of accounting operations, their value is balanced by the broader skills and abilities necessary in the sector. While knowledge of financial data is essential, the company also prioritised practical skills such as financial analysis, reporting, auditing, and good communication within teams and with clients. This sophisticated approach showed that, while correct data management is the foundation of accounting practices, the application of insights and strategic knowledge produced from this data is what actually delivers value for clients and guides business decision-making processes. As a result, while data management remained important, the internship highlighted the complementing significance of interpretive abilities.

2.0 ISSUES

2.1 Technological Advancement

Technology advancements in cybersecurity have significantly addressed basic issues in accounting operations. These enhancements include the implementation of advanced data encryption techniques, which secure sensitive financial information by encrypting it in a way that unauthorized parties cannot decipher. Biometric identification technologies, such as fingerprint scanning and facial recognition, have also been used to enhance security. These technologies correctly validate user identities, lowering the risk of identity theft and unauthorized access. Automated cybersecurity solutions based on AI and machine learning algorithms may experience false positives and negatives. False positives, which falsely detect harmless behavior as a danger, can lead to unnecessary alerts and operational inefficiencies. False negatives, or failing to identify true dangers, can jeopardize accounting firms. As happened with Capital One, outside persons got unauthorized access and received some sort of personal information concerning Capital One credit card users and those who applied for our credit card products (Capital One, 2019) .

False positives occur when the system incorrectly identifies innocuous behavior as a potential threat. This might result in unnecessary alarms being triggered for actions that pose no true threat to the accounting firm's security. When false positives occur frequently, cybersecurity teams may develop alert fatigue, allowing significant dangers to be overlooked in a sea of irrelevant signals. False negatives occur when the system fails to detect a legitimate threat. This is particularly dangerous since it suggests that illicit behavior may go unnoticed, jeopardizing the security of important financial data. A missed detection of a serious threat might result in data breaches, financial losses, brand damage, and regulatory ramifications for the accounting industry.

2.2 Phishing and social engineering

Phishing and social engineering are important cybersecurity threats for accounting firms because they exploit psychological manipulation and deception to attack human vulnerabilities rather than technological ones. Attackers conduct extensive research about their targets to properly personalize phishing emails. They typically exploit information from public sources or previous breaches to construct communications that appear authentic and timely. Attackers exploit accounting professionals' trust relationships with other parties by impersonating legitimate entities such as clients, coworkers, or financial institutions. Phishing emails frequently contain deceptive content designed to fool recipients into engaging in specific behaviors. For example, they may seek sensitive financial information such as login credentials, account numbers, or tax information to meet urgent updates or compliance needs. Alternatively, emails may instruct recipients to download seemingly innocent files or to click on links to fraudulent websites that appear to provide legitimate services. The target receives a blank email with the subject line "price revision" (Stu Sjouwerman, 2020). It can happen when the accounting carelessly reads the email whether it is from clients or phishing.

Its attacks are designed to induce psychological responses in recipients. They typically communicate a sense of urgency, such as alerts about impending financial loss, account suspension, or missed opportunities. Urgency pushes recipients to act quickly without first determining the request's validity. Similarly, attackers arouse victims' curiosity by sending them enticing offers, unusual information, or purportedly important updates that persuade them to click on links or download files. Threats of legal action, penalties, or reputational loss can be used to coerce receivers into disclosing sensitive information or complying with fraudulent requests.

2.3 Ransomware of Cybersecurity in Accounting and Information

Ransomware is malicious software that encrypts files on computers and networks, making them unavailable to users. Attackers demand a ransom payment, typically in cryptocurrency, in return for decrypting the files and providing access. This type of attack can disrupt accounting systems by encrypting bank records, client data, and sensitive information needed for daily operations. It is often spread by phishing emails containing malicious files or links, exploit kits that target software or operating system vulnerabilities, or hijacked remote desktop protocol (RDP) credentials. When ransomware enters a network, it swiftly encrypts files on all available devices, including servers and backup systems, to maximize its impact and increase the probability of ransom payment. Hackers take possession of systems or information and only release it when the victim pays a ransom. In recent years, bad actors have increased their use of this form of assault (*Arjun Kharpal*, 2023). Furthermore, releasing sensitive material undermines the trust and reputation that have been carefully built with clients and regulatory organizations. The effects of such breaches extend beyond immediate financial losses to long-term damage to the company's credibility and status in the industry. Restoring confidence and recovering from these reputational hits may be a tough and resource-intensive undertaking that necessitates open communication, committed remedial efforts, and proactive steps to avoid future incidents.

In essence, ransomware assaults endanger not just immediate operational concerns, but also the basic trust and trustworthiness on which accounting firms rely. Mitigating these dangers requires robust cybersecurity measures, meticulous planning, and an unshakable commitment to safeguarding sensitive data and client trust.

2.4 Insider Threat

Internal cybersecurity hazards in accounting are described as threats posed by employees within the organisation who have authorised access to sensitive data. These hazards might be intentional or unintentional, and they encompass a variety of conditions that jeopardise data integrity, confidentiality, or availability. Employees that engage in purposeful activities with malicious intent constitute a significant internal threat. This might include unauthorised access to financial information, consumer data theft, or sabotage designed to disrupt operations. Malicious insiders may exploit their knowledge of internal systems and procedures to go around security measures and evade detection.

Internal cybersecurity issues inside accounting firms can frequently come from unsatisfied employees or outsiders driven by external causes. These insider threats offer a significant risk because they may lead to intentional activities that harm the organisation. Such scenarios usually use complicated techniques and may encompass a wide range of damaging behaviours that jeopardise cybersecurity and information integrity. It happened once to one of the big firms that KPMG and PCAOB were former staffers at the Public Company Accounting Oversight Board (PCAOB) and former senior officials at KPMG LLP - arising from their participation in a scheme to misappropriate and use confidential information relating to the PCAOB's planned inspections of KPMG (“US Public Auditing Reforms May Follow 2020 | Emerald Insight,” 2020).

While these collaborations are crucial for business continuity and efficiency, they can raise significant cybersecurity problems if the third parties do not adhere to the same stringent security criteria as the organization. One of the primary concerns is the possibility of data breaches or unauthorized access through third-party networks. This might be the result of weak encryption techniques, lax access controls, or faults in their IT architecture.

2.5 Cloud Security

Cloud computing is a concept of giving access (via the internet from anywhere) to a shared pool of customizable computing resources (e.g. networks, servers, storage, applications, and services) on demand (Peter and Tim, 2011). Entrusting sensitive financial information to another entity requires a leap of faith. While most cloud companies spend much on security, a successful attack on their infrastructure might compromise your data. Furthermore, their security procedures may not always be perfectly matched with your organization's specific needs. A limited understanding of their security practices might be troublesome. While major cloud providers like Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) invest much in security and infrastructure, the possibility of a successful cyberattack cannot be eliminated. These breaches might involve cyber incidents, insider threats within the organization, or physical security weaknesses in data facilities. A compromise at the provider level may have far-reaching repercussions, exposing your organization's data alongside that of other clients.

Cloud companies offer defined security measures and capabilities. While powerful, they may not entirely fulfill the organization's specific financial data security needs. For example, industrial standards may necessitate additional security measures beyond what the primary cloud service provides. They will need to examine if the cloud provider has the necessary customization options to meet regulatory standards.

3.0 MITIGATION

3.1 Job Displacement

The future of work presents numerous potentials for technology breakthroughs, which may affect the amount, quality, and stability of jobs; generate new occupations of varying skill and income levels; and radically disrupt whole sectors (Chia-Chia Chang, 2022). To manage the challenges of job displacement, organizations should deliberately pivot towards improving their personnel through systematic upskilling and reskilling projects. A critical step is to spend heavily on bespoke training programs that provide existing staff with the fundamental abilities needed to effectively connect with modern technology, such as data analysis, automation tools, and cloud computing solutions. This proactive strategy not only improves organizational agility but also protects the workforce from the disruptive effects of technological innovations.

Furthermore, a focus on boosting human knowledge in conjunction with technology integration is critical. This approach is shown by hybrid jobs that synergistically combine technical capabilities and human expertise. For example, incorporating AI-powered tools into accounting operations while keeping human oversight for complex jobs highlights efficiency improvements without sacrificing the precision and qualitative insights that human judgment and problem-solving abilities offer.

Ethical integrity is crucial during this transforming journey. Adherence to severe data privacy rules, such as GDPR and CCPA, guarantees the safe management of customer information, fostering confidence and protecting against any liabilities. Transparent communication with customers about data collection, storage, and permission processes increases responsibility and strengthens client relationships. Organizations may successfully negotiate the problems of job displacement by designing programs around four pillars—strategic upskilling, precise cost management, and unshakable ethical standards. This strategy not only puts them at the forefront of technical innovation, but it also develops a robust and adaptable workforce capable of prospering in an ever-changing digital world.

3.2 User awareness and training

Only top management (organization) and external challenges have a substantial positive link with user knowledge of the application of accrual accounting (Nurul Nadiah Ahmad,2024). As to improve organizational resilience against cyber risks, comprehensive solutions that include both behavioral and technological measures are required. Beginning with frequent phishing simulations, organizations may systematically assess and improve their workers' capacity to detect and avoid phishing attacks. These simulated assaults are important instructional tools because they raise awareness and provide workers with the knowledge they need to accurately spot phishing red flags. Concurrently, constant security awareness training is essential. Employees benefit from such training efforts, which teach them core cybersecurity principles such as how to identify phishing tactics, social engineering maneuvers, and rules for protecting sensitive information.

A deep grasp of the psychology underlying social engineering is also required. Employees should be trained to recognize common social engineering ploys that use emotions such as haste, fear, or appeals to authority. Organizations may considerably reduce the danger of unintentionally disclosing personal information or falling victim to fraudulent links by arming their staff against these manipulative methods.

Fostering a culture that fosters quick reporting of suspicious activity enhances defenses even further. Creating a climate in which workers feel empowered to identify possible risks without fear of retaliation promotes early identification and rapid mitigation of security breaches, hence preventing potential harm to organizational integrity. On the technological front, strong security measures are an essential line of defense. Implementing effective email filtering and anti-phishing software is critical. These systems use advanced algorithms to proactively identify and intercept suspect emails before they reach employee inboxes, reducing exposure to phishing.

Furthermore, the concept of least privilege helps to restrict access to sensitive data to only authorized individuals. This pre-emptive strategy mitigates the possible consequences of successful phishing or social engineering attacksBy combining these multiple techniques, organizations can build a robust cybersecurity framework that not only guards against current threats but also creates a watchful and knowledgeable workforce capable of effectively protecting key assets.

3.3 Collaboration and Partnerships

Collaboration and collaborations with cybersecurity professionals, industry colleagues, and law enforcement agencies are critical for organisations looking to strengthen their resistance against ransomware threats. Cyber and finance are partnering on technological initiatives as organizations increase the efficiency and security of their financial procedures and systems (ICAEW Insights,2024). By actively engaging with these stakeholders, organizations can access invaluable expertise, insights, and resources that contribute to a more robust cybersecurity posture.

Cybersecurity specialists have specialized expertise and experience in detecting, analyzing, and managing ransomware attacks. Their counsel assists organizations in staying current on changing ransomware strategies, weaknesses, and viable solutions. This partnership enables organizations to execute proactive solutions that are adapted to their unique risks and operational situations. Industry peers play an important role in knowledge sharing and collective defense against ransomware. Participation in industry forums, working groups, or consortiums enables organizations to share threat intelligence, incident response best practices, and lessons gained from previous experiences. Organizations may enhance their defenses and improve their incident response skills by learning from the achievements and problems of their peers. Law enforcement agencies play an important role in countering ransomware through their legal knowledge, investigative powers, and coordination of cybercrime response activities.

Participation in information-sharing forums, such as Information Sharing and Analysis Centres (ISACs) or sector-specific cybersecurity groups, allows for real-time threat intelligence exchange. These forums provide organisations with early alerts about new ransomware tactics, indications of compromise, and successful mitigation techniques. Organizations may use collective intelligence to proactively change their defenses and reduce ransomware attacks before they develop.

In conclusion, engagement and collaborations with cybersecurity professionals, industry colleagues, and law enforcement authorities enable organisations to increase their defenses against ransomware. Organizations may improve their ability to identify, mitigate, and recover from ransomware outbreaks by sharing information, collaborating on projects, and responding in a coordinated manner. Embracing a collaborative strategy not only strengthens individual organisations but also adds to a larger effort to battle ransomware threats across sectors and industries.

3.4 Control and Access Management:

To improve cybersecurity measures in accounting and information systems, organizations should follow a systematic framework that includes least privilege principles, tight access controls, robust authentication methods, proactive monitoring, and thorough education campaigns. The idea of least privilege states that workers should only be given the bare minimum of access required to carry out their job tasks. Limiting access permissions helps organizations reduce the possible consequences of compromised credentials or abuse, decreasing the breadth of harm in the case of a security breach. When combined with strong password rules requiring complicated passwords and regular updates, organisations improve the robustness of their authentication systems to brute-force attacks and unauthorised access attempts. Implementing multi-factor authentication strengthens defences by requiring a verification element other than passwords, such as a code from a mobile application. This added layer of protection is especially important for accounts that handle sensitive financial data, as it considerably reduces the danger of unauthorised access even when login credentials are compromised.

User access credentials are reviewed on a regular basis to ensure that they are in line with current job positions and responsibilities. Conducting these evaluations on a regular basis enables organisations to quickly remove access for individuals who no longer require it, minimising the probability of insider threats or unauthorised access following personnel changes. Furthermore, session management strategies like session timeouts and automated locking of inactive sessions reduce the danger of unauthorised access via unattended devices. Data encryption, both at rest and in transit, protects sensitive information from unauthorised access, preserving confidentiality even when accessed by insiders with malevolent intent. In addition to these protections, detection and monitoring techniques such as user activity monitoring and data loss prevention technologies allow for the proactive identification of questionable behaviour or data exfiltration efforts.

Clear exit processes guarantee the quick termination of access privileges and retrieval of corporate equipment and credentials when employees leave the organisation, reducing the risks connected with dissatisfied former employees. Segregation of tasks within financial processes improves transparency and accountability by eliminating single points of failure and discovering fraudulent activity early on. By incorporating these concepts and practices into a comprehensive cybersecurity plan, businesses may successfully manage risks within their accounting and information systems, protect sensitive data, and preserve operational continuity in the face of changing threats.

3.5 Protection Of Sensitive Financial Information

Mitigating cloud security threats necessitates a systematic strategy to ensuring the security of sensitive financial data entrusted to third-party cloud providers. Data protection is critical to securing sensitive financial information (Cloud Accounting Security: What You Need to Know - Cloud Accountant, 2024). While cloud service providers such as Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) make significant investments in security and infrastructure, organisations must supplement these measures with tailored strategies that address their specific security requirements and compliance standards. To begin, organisations must realise that, while large cloud providers use powerful security mechanisms, they are not immune to intrusions. Hacking events, insider threats, and physical security flaws in data centres all have the potential to jeopardise critical cloud data. A security compromise at the provider level can have far-reaching consequences, potentially exposing not just one organization's data but also that of other clients that share the infrastructure.

To successfully mitigate these risks, organisations should do extensive due research before picking a cloud provider. This involves evaluating the provider's security methods, certifications, and compliance with industry standards for financial data protection. Understanding the provider's security architecture and incident response skills is critical in determining their capacity to mitigate and respond to possible attacks.

Furthermore, organisations should consider adding extra security measures that go beyond what cloud providers typically offer. This includes identifying and implementing additional security controls, encryption techniques, and access management rules that are suited to specific industry standards and organisational security requirements. For example, companies with severe compliance requirements may demand specific security configurations that go beyond the cloud service's baseline security capabilities.

Regular audits and inspections of the cloud environment, together with constant monitoring of access logs and data activities, aid in the early detection of abnormalities and potential security breaches. Implementing data encryption at rest and in transit provides an additional degree of security, guaranteeing that critical financial information remains unreadable to unauthorised users even if accessed illegally. Although cloud services provide scalability and efficiency benefits, protecting sensitive financial data necessitates a cautious and tailored strategy. By augmenting basic cloud security measures with personalised solutions, organisations may successfully limit risks while maintaining the confidentiality, integrity, and availability of their financial information in the cloud.

4.0 CONCLUSION

Finally, cybersecurity is a critical component in protecting sensitive financial information within accounting businesses. As technology innovations continue to reshape operating environments, the significance of strong cybersecurity frameworks becomes more apparent. Organisations must traverse a dynamic world rife with emerging threats such as phishing, ransomware, insider threats, and cloud vulnerabilities. Mitigating these hazards requires a diverse strategy. It starts with proactive initiatives like strategic upskilling and reskilling of personnel, which ensures they are ready to efficiently exploit technology while keeping ethical integrity and data protection standards. Enhanced user awareness and training programmes help staff recognise and avoid social engineering methods and phishing efforts, building a watchful organisational culture that values cybersecurity. Collaboration and collaborations with cybersecurity specialists, industry peers, and law enforcement agencies improve organisational resilience to ransomware attacks by enabling information exchange and joint defence actions. Meanwhile, strict access restrictions, strong authentication methods, and encryption protocols strengthen accounting and information systems' defences, protecting sensitive financial data from unauthorised access and breaches.

Adopting these measures not only improves cybersecurity, but also maintains client trust, operational continuity, and regulatory compliance. As businesses navigate the complexities of the digital age, investing in comprehensive cybersecurity measures ensures they are well-prepared to confront emerging threats and capitalise on technology's transformative potential, securing a resilient future in an interconnected global economy.

5.0 REFERENCES

Cybersecurity in accounting research | Emerald Insight. (2018). *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108//MAJ

2019 Capital One Cyber Incident | What Happened | Capital One. (2019). Capital One. https://www.capitalone.com/digital/facts2019/

Stu Sjouwerman. (2020). *New BEC Phishing Attack Steals Office 365 Credentials and Bypasses MFA*. Knowbe4.com. https://blog.knowbe4.com/new-bec-phishing-attack-steals-office-365-credentials-and-bypasses-mfa

Arjun Kharpal. (2023, November 10). *China's ICBC, the world's biggest bank, hit by cyberattack that reportedly disrupted Treasury markets*. CNBC; CNBC. https://www.cnbc.com/2023/11/10/icbc-the-worlds-biggest-bank-hit-by-ransomware-cyberattack.html

Definition of Cybersecurity - Gaps and overlaps in standardisation. (2016). ENISA. https://www.enisa.europa.eu/publications/definition-of-cybersecurity

SEC.gov | Six Accountants Charged with Using Leaked Confidential PCAOB Data in Quest to Improve Inspection Results for KPMG. (2018). Sec.gov. https://www.sec.gov/newsroom/press-releases/2018-6

US public auditing reforms may follow 2020 | Emerald Insight. (2020). Emerald Expert Briefings, oxan-db(oxan-db), -. https://doi.org/10.1108//OXAN

The Role of Technological Job Displacement in the Future of Work | Blogs | CDC. (2022, February 15). Cdc.gov. https://blogs.cdc.gov/niosh-science-blog/2022/02/15/tjd-fow/

Why collaboration is key to better cyber security. (2024). Icaew.com. https://www.icaew.com/insights/viewpoints-on-the-news/2023/oct-2023/cyber-month-why-collaboration-is-key-to-security

Cloud Accounting Security: What you Need to Know - Cloud Accountant. (2024, February 20). Cloudaccountant.co.uk. https://www.cloudaccountant.co.uk/blog/cloud-accounting-security-what-you-need-to-know/#:

View of Key Critical Factors Of The Users' Awareness Towards Migration Of Accounting Practices. (2024). Mohe.gov.my. https://myjms.mohe.gov.my/index.php/jrpam/article/view/21621/11626