FIELD REPORT

PAC 671

FACULTY OF ACCOUNTANCY

UNIVERSITI TEKNOLOGI MARA

UiTM CAWANGAN TERENGGANU

NAME : NUR IFFAH LIYANA BINTI MOHD SOHAIMI

STUDENT ID : 2020615344

SUPERVISOR (UiTM) : NORLINDA ZAINAL ABDUL

TABLE OF CONTENT

SECTION A

1. INTRODUCTION

SYAM & CO
CHARTERED ACCOUNTANTS

Syam & Co Chartered Accountants is an audit firm offering a comprehensive range of accounting, tax, audit, corporate advisory, and financial services. The firm's mission is to help businesses thrive by providing expert guidance and strategic solutions, ensuring clients can focus on what they do best in running their business. Syam & Co has its headquarters located in Bandar Baru Bangi, with a branch in Cyberjaya.

Syam & Co provides accounting services, including bookkeeping, financial statement preparation, and management accounting. These services are tailored to help businesses maintain accurate financial records and make informed decisions. Other than that, the firm also offers tax services such as tax planning, compliance, and advisory. Their expertise ensures clients optimize their tax obligations and remain compliant with the latest tax laws and regulations. Syam & Co conducts thorough audits to assess the accuracy and fairness of financial statements which help clients identify areas for improvement and maintain stakeholder confidence. The corporate advisory services at Syam & Co include business consulting, mergers and acquisitions, and corporate restructuring. These services are designed to support clients in strategic planning and enhancing business performance.

This company's mission is to provide desired service in accounting, auditing, corporate secretarial, taxation and business consultancy in meeting the client's expectation. As for the vision, Syam & Co is to provide an integrated assurance and advisory solution that satisfies the demands of all sectors of Malaysian corporate society and sub-societies, with a focus on Semi-Medium Industries (SME). Below are the organization charts of Syam & Co:

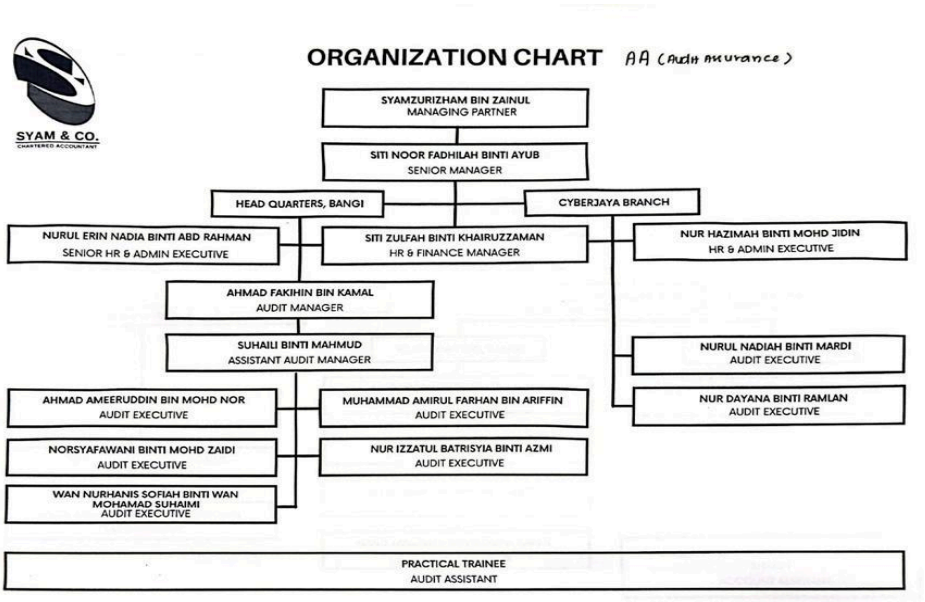

Figure 1.0: Organizational Chart

2. SUMMARY OF WORK DONE

2.0) Reliability Test

At the beginning of the internship period, we were exposed to the reliability test (RT). This reliability test is done in the first step before doing the audit work. The objective of doing this RT is to perform a test to ensure that the financial statements received by the client are ready for audit planning at the end of a particular financial year. This test can only be performed after the auditor has received a full set of financial statements with Trial Balances, Ledgers and Notes to the Financial Statements. To complete the test, there are several steps to complete and if any of the steps fail, I must write a letter to the client to notify them of the discrepancies found. Upon receiving revised financial statements, all steps must be repeated until all steps are successfully completed.

2.1) Audit Job (Abot)

On March 6, we began our first auditing assignment using the Abot system. The system has two main sections. The "By Client" section includes four steps which are Data Preparation (uploading and entering client data), Corporate Info (inputting company details), Account

Summary (consolidating key account information), and Financial Report (ensuring accuracy for the audit report). Each step is crucial for the accuracy and integrity of the audit process.

The "By Auditor" section starts with audit planning, which involves checking for conflicts of interest, assessing fraud risk, evaluating business continuity, and reviewing related parties. During audit execution, all supporting documents must be uploaded, including tax computations from the tax agent, which are vital for determining the client's tax liability.

Audit completion involves finalizing all audit steps, obtaining confirmations from the audit manager and principal, and producing paperwork for client signatures. Once verified, I email the draft audit report to the client for approval, then obtain a commissioner's stamp. The final audit report is assembled into six copies for various recipients. This process will be repeated for each client throughout the internship

3. STRENGTH AND WEAKNESS

3.1 Strength

3.1.1 Great Work surrounding

During my time interning at Syam & Co, I got to work closely with the folks in the audit department. What really stood out to me was how they were both professional and caring. They didn't just give me tasks and leave me on my own, they were always there to help and support me. Whenever I had a problem or didn't understand something, they were patient and took the time to explain it to me. Every time they explained something, it felt like I was getting a really good lesson, not just on how to do the task, but also on why we were doing it that way. Their instructions were really clear and easy to follow, which made it a lot easier for me to do my job. Being in such a helpful environment made learning new things much easier, and it gave me the confidence to tackle tough challenges.

3.1.2 Gain a lot of knowledge

I had a significant learning experience that broadened my understanding of the accounting field. Before this internship, I had only studied audit theory in the classroom, but I lacked practical knowledge of how it applied in a real-world work setting. This opportunity allowed me to bridge that gap between theory and practice. By working alongside professionals in the audit department, I gained firsthand experience in applying the concepts and principles I had learned

in my coursework. I was able to see how audit theory translated into actual audit procedures and practices within the company. This exposure not only deepened my understanding of accounting but also gave me insights into the day-to-day operations of a professional accounting firm. Overall, my internship provided me with invaluable exposure to the practical aspects of accounting, complementing my theoretical knowledge and better preparing me for a career in the field.

3.1.3 Work life balance

At Syam & Co, my internship experience has been quite unique compared to other companies. One standout aspect is the excellent work-life balance they offer. Unlike some places where weekends and holidays are often disturbed by work-related calls or emails, here, we get to truly enjoy our time off. The company respects our personal time, and there's no expectation to work outside of regular hours. Furthemore, the work schedule is very reasonable, from 9 to 5:30, and overtime is only required when absolutely necessary. Additionally, the company organizes events during working hours, giving us opportunities to unwind, destress, and build stronger bonds with colleagues. This not only fosters a positive work environment but also contributes to our overall well-being. Importantly, the workload is manageable, allowing us to maintain a healthy balance between work and personal life without feeling overwhelmed.

3.2 Weakness

3.2.1. Limited Duration

One downside of my internship experience is the limited duration of the program, typically around six months. This timeframe poses a challenge because it takes me about a month or more to audit a company effectively, especially since I'm still in the learning process. This limited time doesn't leave much room for adjustment. As a result, I often feel rushed to complete audit tasks within tight deadlines, which can sometimes compromise the thoroughness of my work. Another drawback is the restricted number of companies I can audit within the internship period. With the limited time available, I'm unable to gain exposure to a wide variety of companies across different industries. This lack of diversity in my audit experiences means that I may miss out on valuable learning opportunities and insights that come from working with a range of companies with unique challenges and operations.

3.2.2. Using Personal Laptop

Another potential weakness of my internship experience is the reliance on my personal laptop for audit tasks. While using my own device offers familiarity and convenience, it also presents challenges. One major issue is the mixing of work-related audit documents with my personal files, which can affect my laptop's storage space. Audits often involve handling a large volume of documents, increasing the likelihood of system slowdowns or crashes due to the strain on my device's resources. Furthermore, the performance limitations of my personal laptop, such as slower processing speeds or insufficient memory, can hinder productivity and efficiency during audit tasks. This reliance on personal hardware may also pose compatibility issues with certain audit software or tools, leading to potential disruptions or delays in completing tasks.

3.2.3. Limited Direct Client Communication

One area of weakness in my internship experience is the lack of direct communication with clients. Throughout my internship, I primarily interacted with clients indirectly through email and through my supervisor. While this approach provided some exposure to client communication, the absence of direct interaction limited my ability to develop strong interpersonal and client management skills.

Direct client communication is essential in the audit profession for several reasons. It allows interns to gain firsthand experience in understanding client needs, clarifying audit requirements, and addressing any concerns or questions in real-time. By communicating through my supervisor, I may have missed opportunities to independently handle client queries, build rapport, and demonstrate my understanding of audit processes directly to clients.

4. SELF REFLECTIONS

During my internship at Syam & Co, I went through a big learning experience that made me see just how different it is to work compared to being a student. This time was like my first step into the real working world, where I learned really important things about being responsible and working hard. As an auditor, I quickly realized that being honest and professional are super important. I saw how crucial it is to stick to what's right, even when there's pressure from outside to do something different. It taught me that the integrity of audit work is something that can't be messed with.

This internship turned out to be a major confidence boost for me, especially in formal situations like meetings and presentations. It was a whole new world for me since it was my first job ever, so I wasn't used to dealing with such professional scenarios. However, as time went on, I found myself becoming more and more comfortable handling them. Working as an auditor wasn't just about improving my technical skills, it also helped me become much better at communicating with others. I found myself talking to my coworkers a lot about work-related stuff, and that really helped me become more articulate and effective in my communication.

The challenge I faced during this internship was adapting to the professional work environment, which was a completely new experience for me. Despite having some theoretical knowledge of auditing from university, applying it in a real-world context proved to be difficult and complex. However, over time, I managed to adapt to the working life and gain some knowledge from all the staff. Overall, I am very grateful and satisfied with my internship at Syam and Co, as the team consistently provided guidance and advice that significantly enhanced my understanding and skills in the field of accounting.

SECTION B

Title

IMPLICATIONS OF WEAK DATA SECURITY

In today's fast-paced era, advancements in technology have revolutionized many aspects of our lives, including the accounting industry. The shift from traditional, manual accounting methods to advanced online systems has greatly improved the efficiency and accuracy of data recording and management. With the widespread use of the internet, accounting firms have adopted digital platforms to streamline their operations, making data entry, storage, and retrieval more efficient and less prone to human error. This digital change not only allows for handling larger amounts of data but also enables real-time updates and access to financial information from anywhere in the world. The use of advanced technologies such as cloud computing, AI, and blockchain further enhances the capabilities of online accounting systems, allowing firms to automate routine tasks, generate insightful reports, and ensure compliance with constantly changing regulations.

However, with the increased reliance on online systems comes the critical responsibility of protecting sensitive financial data. Data security has become a major concern for accounting firms, as they deal with highly confidential information that, if compromised, can lead to severe financial and reputational damage. Implementing strong data security measures is essential to protect digital data from unauthorized access, tampering, and cyber threats. This includes using encryption techniques, multi-factor authentication, and regular security audits to ensure the integrity and confidentiality of accounting data. By prioritizing data security, firms can prevent unauthorized changes, ensure the accuracy of financial records, and maintain the trust of their clients. Effective data security not only protects against external threats but also reduces risks from internal breaches, thereby upholding the firm's commitment to protecting all account data information. However, there are now various risks of attacks on account security data that will have a negative impact on the company. These include cyber attacks, data breaches, and security misconfigurations, which can harm the company's reputation in the eyes of the public.

One of the main reasons for data security weaknesses in the accounting system is the use of outdated systems that are not in line with current technological advancements (Gudhenia & Johri, 2024). These outdated systems often have weak security features, making them easy targets for hackers and unauthorized parties. Hackers can use these opportunities to gain

access to sensitive financial information, leading to significant financial and reputational damage for the company. Additionally, outdated systems are more prone to frequent network interruptions because they are not designed to handle the large volumes of accounting data generated in today's digital world which can lead to operational inefficiencies and data loss. Moreover, outdated systems are more exposed to viruses and other forms of malware, which can corrupt data and disrupt business operations. The problem is due to companies that do not take proactive steps to protect client data by updating their systems in line with current technology. These companies often fail to implement the latest security patches and upgrades, leaving their systems vulnerable to attacks. This negligence provides an opportunity for unauthorized organization to access the data for their own benefit, potentially leading to identity theft, financial fraud, and other illegal activities.

1. DISCUSSION

Issue 1: Cyberattacks

One of the most significant consequences of weak data security is the vulnerability to various cyber attacks. Cyber attacks are unlawful activities conducted by individuals seeking to exploit data for personal gain, which can severely impact sensitive financial information and disrupt a company's financial operations. Data breaches are a common example of such attacks, involving unauthorized access to confidential data by any unauthorized organizations (Kafi & Akter, 2023). These breaches exploit weaknesses in an organization's data protection measures, which can occur in several ways. For instance, when companies adopt cloud accounting and allow Bring Your Own Device (BYOD) policies, employees may use personal devices like laptops to access company data remotely. While this practice can enhance productivity, it also introduces risks if adequate security measures are not in place. Employees may unintentionally or intentionally cause data breaches by mishandling sensitive information or failing to follow security protocols. For example, they might copy confidential documents to personal folders, potentially exposing them to unauthorized access or theft. This is shown that the access privileges can lead to significant data compromises and pose serious threats to the integrity and confidentiality of financial records.

Other than that, using personal laptops for work will expose data to significant risks of malware attacks. Malware is a short form for malicious software, which can harm computers or servers. Personal laptops typically lack the robust security measures found in corporate environments,

such as comprehensive antivirus software. This weak data security can lead to malware attacks, which can compromise sensitive data and disrupt operations. Moreover, personal laptops often serve dual purposes for both work and personal activities. This dual use introduces additional security vulnerabilities. For instance, individuals may unknowingly expose their laptops to malware by visiting any unauthorized websites or clicking on malicious links in phishing emails. Unlike corporate devices that are subject to strict security policies and regular updates, personal laptops may not have the latest security protocols in place. Therefore it is proven that this weak data security will increase the risk of malware and the occurrence of cyberattacks.

Based on (Kafi & Akter, 2023) the example of a data breach caused by weak security is the JPMorgan Chase cyber attack that occurred in 2014. In this incident, hackers believed to be from Russia successfully hacked into the bank's network due to vulnerabilities in the bank's website security. As a result, the hackers infiltrated the bank's systems and accessed sensitive data, including customer information. This breach highlighted the importance of strong security measures and the potential consequences of inadequate data protection. It serves as a reminder of the need for continuous improvement in cybersecurity practices to prevent similar incidents in the future.

Issue 2: Financial Loss

Weak data security will cause a lot of fraud and cyber attacks. This will cause the company to be involved in various problems involving finances. A weak security system will expose the company to hackers because it is easy to hack the system and steal the data and money in the company's account overnight. In the article there is an example where an accounting firm was hacked where the thief stole the client's personal data that was not encrypted (Lehenchuk et al., 2022). This causes the anger of customers who are victims where data is stolen by hackers and the affected clients filed lawsuits against the firm, holding it accountable for failing to protect their confidential data adequately. The total cost that the company had to bear is around $140,000. This legal action not only led to substantial financial liabilities in the form of settlements and legal fees but also damaged the firm's reputation and client trust.

In another case, a company was compromised due to an employee clicking on a phishing link disguised as an invoice. This action triggered a malware attack that paralyzed the company's systems and had to pay compensation to the scammer. This will lead to the company having to bear the cost of system recovery, downtime cost that cost $83.660. These examples illustrate that weak security systems can make it easier for hackers to exploit vulnerabilities, leading to severe consequences such as financial losses.

The occurrence of a cybersecurity incident caused by weak data security can severely damage a company's reputation due to negative media coverage highlighting the breach of confidential information. This bad publicity fosters public distrust and incites clients to seek more secure alternatives, fearing repeated incidents due to the company's insufficient data security measures. Consequently, the loss of customers directly affects the company's revenue streams, leading to long-term financial instability as the company struggles to regain trust and attract new clients while addressing the financial impact of the breach.

2. **RECOMMENDATION**:

2.1. Data Encryption

There are various ways to strengthen security data to reduce the occurrence of cyber crimes as discussed. Advancement technology plays a very important role in increasing the security of accounting data (Temitayo Oluwaseun Abrahams et al., 2023). There are various advanced technologies that will strengthen data security, one of which is encryption. This encryption is one of the main techniques used to protect sensitive account data by changing the original text to a code that cannot be read by some algorithms where it is usually known as ciphertext (Yang et al., 2020). This code is so difficult that unauthorized parties cannot know the contents of the data. This is because unauthorized parties cannot interpret the code without the appropriate decryption key. It is proven that by using this encryption technology, it can ensure that financial data remains confidential and secure, even in the face of advanced cyber threats.

Encryption Algorithm (Cipher) is a mathematical function that transforms plaintext into ciphertext and it is divided into 2 types namely symmetric encryption and asymmetric encryption. Symmetric encryption uses the same key to encrypt and decrypt data. It means to encrypt the data, the original data or text will be combined with the key using a symmetric encryption algorithm to produce ciphertext. And to decrypt the data, the ciphertext is combined with the same secret key using the same algorithm to revert to the original plaintext. While, for

Asymmetric Encryption, for encrypting the data, the plaintext is encrypted with the recipient's public key, producing ciphertext. However, to decrypt the data, the recipient uses their private key to decrypt the ciphertext back into the original plaintext. In conclusion, data encryption is a modern form of cybersecurity that plays a very important role in strengthening data security to protect confidential data from being hacked and accessed by unauthorized parties. Therefore, the company should take smart steps to apply it in an effort to strengthen security data for the sake of data safety in the long term.

2.2. Communicate Transparency

Based on (Kang & Hustvedt, 2013), transparency is one of the fundamental requirements for developing a good relationship between customers and businesses is transparency, which is fostered through CSR initiatives. The relationship that is fostered by brand trust is based in large part on communication, perceived good citizenship, and transparency. When a company experiences unwanted events like data breaches or cyber attacks due to weak security, it's crucial to inform customers right away. Keeping these incidents secret will only worsen the situation and cause customers to lose trust in the company. Transparency between the company and customers is essential. If a company hides important information, it shows a lack of honesty and can damage the relationship with customers. By being open about the issue, the company can demonstrate its responsibility and commitment to fixing the problem. This openness can help maintain customer trust, as customers will appreciate the company's honesty and effort to resolve the issue. Additionally, the company should explain the steps they are taking to address the problem and improve security. This shows that the company is taking the situation seriously and is committed to protecting customer data better in the future. Clear communication and transparency can strengthen the trust customers have in the company, even during difficult times. After being honest about the problem, the company should regularly update customers on the status of the data breaches and the improvements being made. This ongoing communication allows customers to see the company’s efforts firsthand and reinforces their confidence that the company is taking serious action, not just making empty promises. Regular updates show that the company is committed to resolving the issue and improving security measures to prevent similar incidents in the future.

Frequent updates are essential because they show the company's commitment to addressing issues and improving data security. By demonstrating proactive efforts to solve problems, the company can attract attention and potentially gain new customers. This

commitment not only helps regain trust but also enhances the company's reputation, which can lead to increased revenue and offset losses caused by the cybersecurity incident. In essence, transparent communication and consistent updates can play a crucial role in rebuilding trust, attracting new business, and ultimately recovering financially from the impacts of a data breach.

2.3. Employee Training

In addition to improving data security, the company should conduct training for employees. Sometimes, data breaches happen because employees make mistakes or don’t know enough about keeping data safe. If employees don’t understand how important good data security is, they can be easily tricked by outsiders who want to steal the company’s data. By providing awareness training, employees will become more knowledgeable and efficient at maintaining data security. This training will help them understand the importance of protecting sensitive information and teach them how to avoid common security pitfalls. When employees are well-trained and skilled in data security, it becomes much harder for unauthorized people to hack into the company’s systems. Trained employees will be more aware of the risks and better prepared to handle potential threats. They will know how to recognize suspicious activity and take appropriate actions to protect the company's financial data.

Additionally, employees who are informed about the latest security practices will be more confident in their roles, which contributes to a stronger and more secure workplace. By investing in regular training sessions, the company can ensure that its employees are always up-to-date with the best practices in data security, thereby significantly reducing the risk of future breaches. This approach not only strengthens the company's defenses but also shows a commitment to protecting both the company's and customers' data.

4. CONCLUSION

To wrap up all the things that have been discussed, while technology has revolutionized the accounting industry by enhancing efficiency and accuracy, it has also brought significant challenges in data security. The shift to digital systems necessitates robust measures to protect sensitive financial information from cyberattacks, breaches, and other security threats. Companies must adopt advanced technologies like encryption, keep their systems updated, and regularly conduct security audits to safeguard data integrity and confidentiality.

Transparency with clients during security incidents is crucial in maintaining trust and demonstrating accountability. Open communication about the measures being taken to address breaches reassures clients of the company's commitment to their data's security. Additionally, ongoing employee training is vital to ensure staff are well-informed about the latest security practices and can effectively mitigate risks associated with human error.

Ultimately, the balance between leveraging technological advancements and ensuring robust data security is essential for accounting firms to thrive in the digital age. By prioritizing advanced security measures, fostering transparency, and continuously educating employees, firms can protect their financial data, uphold client trust, and confidently navigate the evolving digital landscape.

5. REFERENCES

Md Abdullahel Kafi, & Akter, N. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. *American Journal of Trade and Policy*, *10*(1), 15–26. https://doi.org/10.18034/ajtp.v10i1.659

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, *8*, 131723–131740. https://doi.org/10.1109/access.2020.3009876

Gudhenia, P., & Johri, S. (2024). Increased Use of Data Security in Accounting. *IJFMR240216562*,*6*(2). https://pdfs.semanticscholar.org/50f2/e53631057dec07989074c484ea180c6e1c73.pdf?_gl=1

Temitayo Oluwaseun Abrahams, Sarah Kuzankah Ewuga, Kaggwa, S., Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, & Samuel Onimisi Dawodu. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews*, *20*(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691

S.F. Lehenchuk, I.M. Vygivska, & O.O. Hryhorevska. (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://doi.org/10.26642/pbo-2022-2(52)-40-46

Kang, J., & Hustvedt, G. (2013). Building Trust Between Consumers and Corporations: The Role of Consumer Perceptions of Transparency and Social Responsibility. *Journal of Business Ethics*, *125*(2), 253–265. https://doi.org/10.1007/s10551-013-1916-7

6. APPENDICES

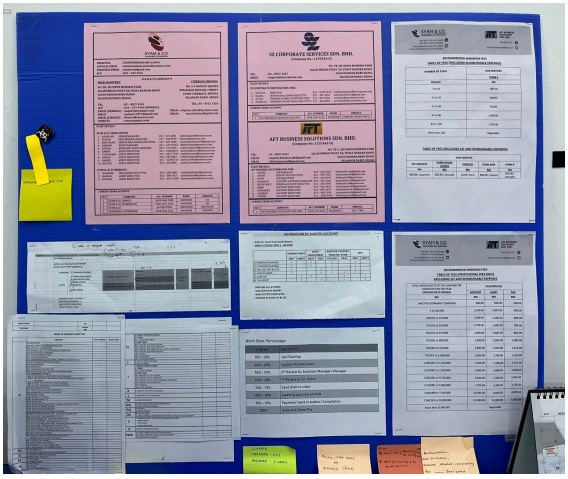

Figure 1.1: Information on the board

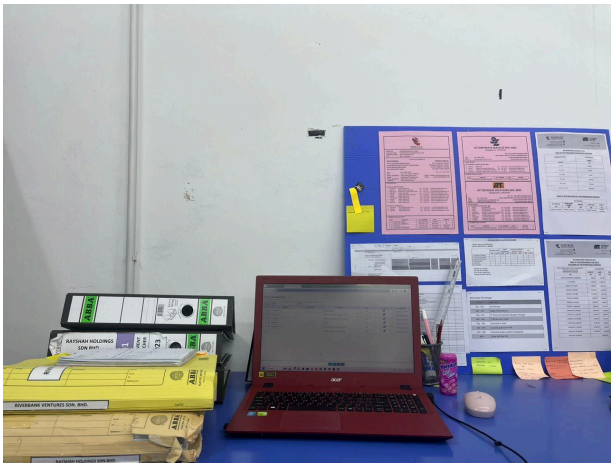

Figure 1.2: Environment on the table

Figure 1.3: Completed files places

Figure 1.4: Environment of the workplace