Report On
A preview of Compliance and Quality Control Strategy in context of Software as a Service Company, Therap Services

By

Nafis Al Bari
20364030

An internship report submitted to the Graduate School of Management in partial fulfillment of the requirements for the degree of
Master's in Business Administration.

BRAC Business School
BRAC University
June 2023

Declaration

It is hereby declared that,

1. The internship report submitted is my own original work while completing a degree at Brac University.
2. The report does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The report does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I have acknowledged all main sources of help.

Student's Full Name & Signature:

Nafis Al Bari
20364030

Supervisor's Full Name & Signature:

Dr. Syed Mahbubur Rahman
Associate Professor, BRAC Business School
BRAC University

Letter of Transmittal

Dr. Syed Mahbubur Rahman
Associate Professor,
BRAC Business School
BRAC University
66 Mohakhali, Dhaka-1212

Subject: Submission of Internship Report

Dear Sir,

I, hereby, submit my internship report, titled "A preview of Compliance and Quality Control Strategy in context of Software as a Service Company, Therap Services" which is a partial requirement for completing my MBA program. I have attempted my best to finish the report with essential data and recommended my suggestions in a comprehensive manner utilizing my gathered knowledge and experience.

I trust that the report will meet the desires.

Sincerely yours,

Nafis Al Bari
20364030
BRAC Business School
BRAC University
Date: June 11, 2023

Acknowledgement

Firstly, I would like to thank Almighty Allah for giving me the opportunity to complete my internship report regardless of all the complications and difficulties that occurred. Then I want to acknowledge Dr. Syed Mahbubur Rahman, my internship supervisor for his guidance, advice and being a constant encouragement during this period. All of these helped me to complete my report properly. Furthermore, I would like to show respect to Ms. Malisa Mahjabeen and Ms. Iffat Arzuman my on-field supervisors in Therap (BD) Ltd. who relentlessly guided me every day. Lastly, I am grateful for everyone's input to this report and my remarkable journey towards the completion of the MBA Program.

Executive Summary

Therap is a US-based Software as a Service company operating since 2003. It provides documentation software to the providers and agencies who support individuals with intellectual and developmental disabilities. It also provides Home and Community Based Services and Long-Term Support and Services to the individuals with special needs and their family. As an organization Therap has very enriched management principles, marketing strategies, HR processes, operation management and information technology. Being the industry leader in the healthcare industry of US Therap has to follow several state and federal mandates like HIPAA. To ensure this compliance it has its own compliance and quality control activities which ensure compliance with the regulatory body mitigating any legal penalties and liabilities. This report contains a brief overview of the company, company's management processes and activities, and its compliance and quality control activities which streamlines the regulatory compliance process.

Keywords: SaaS; Sensitive Information; Information System; Healthcare Industry; Documentation; Regulation; Mandates

Table of Contents

List of Figures

List of Acronyms

HIPAA	Health Insurance Portability and Accountability Act
PHI	Protected Health Information
PII	Personally Identifiable Information
IDD	Intellectual and Developmental Disability
AICPA	Association of International Certified Professional Accountants
SOC	Service Organization Control
GAPP	Generally Accepted Principles and Practices
FedRAMP	Federal Risk and Authorization Management Program
StateRAMP	State Risk and Authorization Management Program
MARS-E	Minimum Acceptable Risk Standards for Exchange
HCBS	Home and Community Based Services
LTSS	Long-Term Services and Support

Chapter 1

Overview of Internship

1.1 Student Information

Name: Nafis Al Bari

Student ID: 20364030

Program: Master of Business Administration

Major: Operational Management

1.2 Internship Information

1.2.1 Employment Details

Duration: August 2022 - Present

Designation: Associate Compliance and Quality Control Specialist

Department: Compliance and Quality Control

Organization Name: Therap (BD) Ltd.

Address: House 47, Road 4, Block C, Banani, Dhaka 1213, Bangladesh

1.2.2 Supervisor Information

- Malisa Mahjabeen

  Lead Compliance and Quality Control Specialist

- Iffat Arzuman

  Lead Compliance & Quality Control Specialist

1.2.3 Job Description

- Prepare and maintain documentations required for audit purposes.
- Create, Modify, Update policies, standards and plans based on specific settings and requirements.
- Research to gather information required to comply with different regulations.
- Maintain the quality of internal processes and training.
- Interdepartmental communication to gather various audit related requirements and information.
- Assisting the internal audit of several organization processes.

1.3 Outcomes

1.3.1 Student's Contribution to the Company

I work on preparing, modifying standards and policy documents required for complying with regulatory body requirements as well as maintaining security of the information system. Additionally, I have worked on sorting the third-party vendors/software information, auditing the list of company provided device inventory, researching on some potential vendors, doing monthly internal audit of visitor access to the company premises.

1.3.2 Benefits to the Student

Therap provided me the platform to learn how the organization is providing software as a service as a form of documentation. It also helped me to learn how internal audit is conducted and how a company meets the requirements for the external audit to comply with the industry's regulatory requirements. All these experiences have taught me how to face real-time challenges and make fast decisions giving the company's interest first priority whilst brushing off the complexity of the situation.

1.3.3 Problems/Difficulties

During the period of my report making for MBA program completion both of my supervisors were very helpful and supportive. This really helped to complete the report properly. As, the organization is based in the US, apart from the designated working hours employees are often required to stay available even after the office hours end and and attend regular meetings. However, as it gets communicated beforehand, it did not create any complication during the preparation of this report.

Chapter 2

Organization Part

2.1 Company Overview

Therap (BD) Ltd. is a US based software company that registered in Bangladesh in 2004. The head office of Therap is in Connecticut. Therap has been operating since 2003 in the US. It provides Software as a Service (SaaS) to the government and private organizations globally that serve people with Intellectual and Developmental Disability. Since 2003 the mission of Therap has been to enhance the lives of individuals who have intellectual and developmental disability and need constant support by the service organizations. Therap does it by providing the tools that the service provider agencies require to bring a meaningful outcome for the people they serve. The administrators of Therap have decades of experience in the IDD industry who possess a dedication in creating efficiency and streamlining process. This enables the company to securely connect people through information exchange and integrating all aspects of service delivery while keeping the individuals, their families and professionals who support them, in focus. The company's name of the SaaS is 'Therap'. The software is HIPAA compliant meaning it adheres to the privacy and security regulations of the Health Insurance Portability and Accountability Act, 1996 of the US. HIPAA protects any information, or a set of information stored in electronic or printed form that can be used to identify an individual. The HIPAA law was created to ensure that the health care delivery is more efficient and there is no fraudulent activity, by limiting the access to individuals' Protected Health Information (PHI). Therap provides its software to the agencies and entities that serve people with intellectual and developmental disabilities. For this Therap has to be HIPAA compliant as it documents PHI of the people whom the agencies serve. Therap is also SOC2 compliant. SOC2 compliance refers to compliance with the five trust service principles of AICPA that ensures security, privacy, availability, integrity of the data company stores, transmits, and receives.

Therap provides comprehensive information management system and documentation software for HCBS/LTSS service providers, state and government agencies, and individuals & families. Therap has 70+ modules in the application that supports,

- Intellectual and Developmental Disabilities
- Community Employment & Vocational Rehabilitation
- Special Education and School Health Services
- Aging and Home Health
- Autism Program

Moreover, Therap has extensive experience in meeting several state required regulations. With the help of this documentation software Therap has made the service provided to the individuals better, easier, and more efficient.

2.2 Management Practices

2.2.1 Leadership Style

The leadership style of Therap is focused on a collaborative work environment that emphasizes employee empowerment through teamwork. The work environment is open and dynamic that is free from any kind of political and government interference and involvement. The employees are always encouraged to have an open and transparent communication with the head of the department and the management. The management values transparency, trust, and accountability and encourages the employees to take responsibility for their work. Thus, the leadership style can be characterized as somewhat democratic. Every decision does not necessarily come straight from the top. Decisions are made based on discussion with proper authorities, responsible personnel, and team members as appropriate. Every team lead of the company encourages a collaborative work environment, engaging in open communication and seeks constant feedback and input from their team members. The team leads also provides constant guidance to the members while also training them so that they can make impromptu decisions on critical situations and take responsibility for their work as needed.

The leadership style of the company also supports individual growth and development on personal and professional levels, and it is open for training and development that will help their career and the company at the same time. Overall, the company maintains such a leadership style that is engaging to the employees and creates a positive impact in their work environment. It helps the employees feel valued, supported, and empowered and encourages them to contribute more to the company's success.

2.2.2 Recruitment and Selection Process

The Recruitment and selection process in Therap starts with the job posting and advertising. All the job vacancies and the job description are posted in detail under Therap career website. Applicants can apply through the career page of the website. Apart from the Therap career page job posting, the company also pays visits to various career fairs organized by the universities and collects resumes from there as well.

The next process after collecting the resumes, is screening. Mainly the applicants initial screening is done by respective department's senior member and/or heads. After passing through the initial screening the applicants are called for the multi-phase recruitment process.

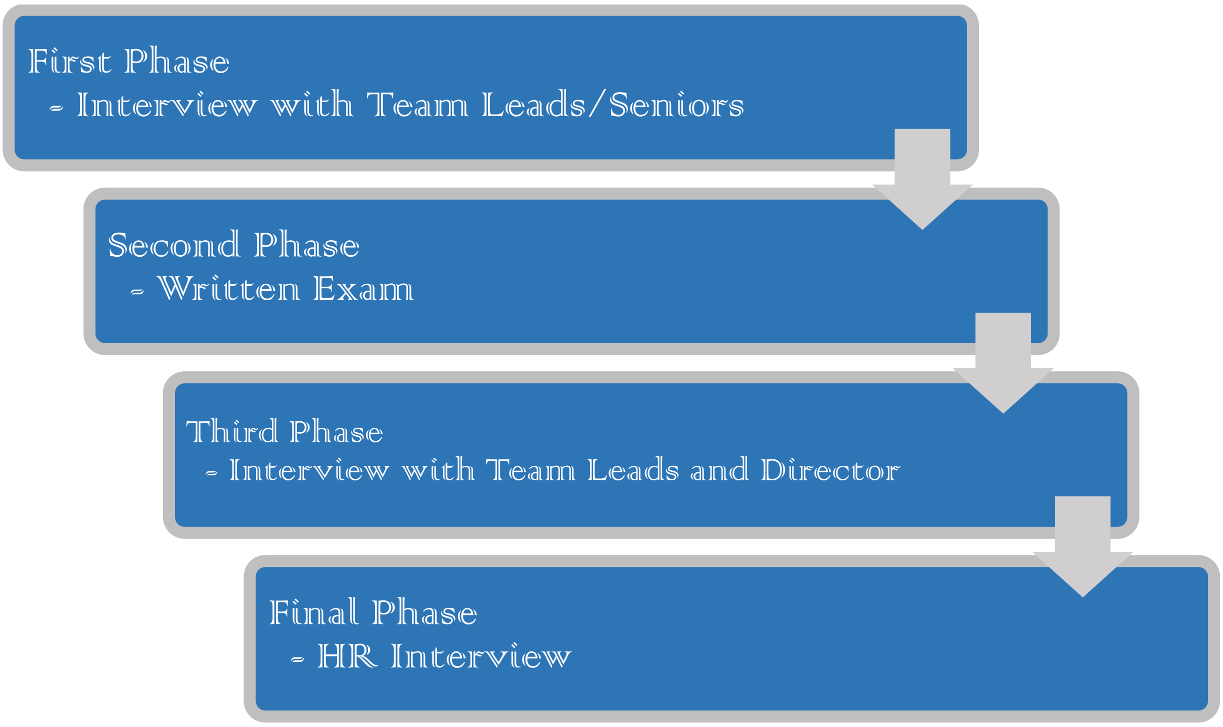
First Phase
- Interview with Team Leads/Seniors
Second Phase
- Written Exam
Third Phase
- Interview with Team Leads and Director
Final Phase
- HR Interview

Figure 1: Recruiting Process

In the first phase of the recruitment process the applicants are called for an interview. This is the initial phase of the interview where the company gets to know about the basics of the applicant. For example, details of educational background, applicants' knowledge about the company and the position that they applied for, goals and future vision of the applicants.

If the applicants get passed in the first phase of the interview, then they are called for the next phase which is usually a written test. The written test consists of conceptual questions, scenario-based questions, and aptitude tests. In the written phase the applicants are judged based on scenarios relevant to their job responsibility.

After passing the 2nd phase, the applicants are called for another face-to-face interview with the department heads of the corresponding department and higher-level authorities of the company such as the director. The candidates are given several scenario-based situations and get evaluated to see whether they are suitable for the post or not and whether they have the mental capability to handle pressure or not.

The next phase of the interview is with the head of HR. Here the applicant’s backgrounds get checked and the final call is being made whether the applicant will get hired or not.

As Therap is a software company the selection process and the steps/phases of the recruitment for various teams vary based on the job responsibility. For example, for the recruitment of technical job position, there are additional phases where the applicant needs to face an implication-based interview. However, the basic four phases remain almost the same for all the team. After finalizing the recruiting the candidates are asked to submit the verified copies of their educational documents and documents of verified proof of identity.

2.2.3 Training and Development

The company always encourages personal growth of each employee which will eventually contribute more to the company’s success. After getting recruited the first few months is the probationary period where the employees get trained for their day-to-day tasks. Constant training is given in person and online to make sure that the employees can learn efficiently about what they will be doing in future. As the company deals with sensitive health information the norms and ways of doing day to day tasks at the office are different. To comply with the regulatory mandates all the employees are given Security training upon joining the company where they are taught how to handle sensitive information, how to escalate any potential issues, what and what not to do in order to make sure the information is safe. Job related training is also given to make employees accustomed with the processes and norms of the company work culture.

Moreover, the employees are encouraged to take several courses which are related to their job responsibility and will add to their performance for the team. Before taking up any course or training it needs to be approved by the department heads and higher management.

2.2.4 Performance Appraisal System

Therap maintains a performance evaluation system which is always fair and transparent to the employees. The work culture is such that the seniors and the leads always provide feedback on the employees work so that they can improve and develop. The performance appraisal system is based solely on how an individual employee performs. Here the employee gets constant feedback of their completed tasks that helps to identify the area of growth and improvement. Throughout the year the team provides ongoing feedback of the employees' work, helps them to complete their tasks and address the performance issues if any arise. Every year the team leads with higher authorities evaluate the performance of the employee, conducts a performance review, and based on this performance review the employees get evaluated.

2.3 Marketing Practices

2.3.1 Target Customers

Therap serves in the niche market of the US healthcare industry. The market is focused on only government organizations and NGOs that serve people with Intellectual and Developmental Disabilities. Therap is the largest Software as a Service Provider of Electronic Health Record solutions in this market.

The target customer/ user of Therap are the providers of health care services to the people with Autism Spectrum Disorder, Down Syndrome, and other intellectual disabilities, Aging and Home Health Service Providers, and Special education & School Health Services providers, and many more. As Therap is the leader in this segment of the industry, the biggest marketing channel is spreading brand reputation through the word of mouth.

2.3.2 Marketing Strategy

Mass Emailing/ Email Marketing: Therap serves in the niche market of healthcare industry in the US. One of the marketing strategies for the company is mass emailing. Therap sends out mass email to all the users of all states to notify them about any feature update, service update, upcoming webinars, and conferences.

As a marketing strategy Therap also uses user-based niche emailing. As Therap application is configurable upon specific requests and its features vary from state to state, some newly added features might be only state specific. To communicate these state specific new updates, feature updates, webinars, events, and conferences specific to individual states, Therap sends out state specific mass email to notify the user.

Using mass emailing system Therap also communicates the new releases of its application. Each year the application undergoes several new releases where new features, services, updates are added. Therap sends release-based emails to its customer to communicate the new release, change updates and its user guide.

Social Media marketing: Therap uses social media as a part of marketing practices. Use of social media includes Facebook posts, LinkedIn updates, YouTube videos etc. Therap posts on social media platforms such as Facebook and LinkedIn about its upcoming in-person events, webinar, conferences to communicate with its users and followers. In Facebook, Therap also publishes post in solidarity with specific national events like Black History Month in US and many more. These sorts of posts are made in LinkedIn as well. Also, Therap publishes posts during the celebration of religious events like Christmas, Eid etc., National Events like National Independence Day, International Mother Language Day etc., and so on.

Trainings: Therap uses the training materials as a marketing element as well. Therap creates system specific training, to teach about the system to its user and describe the new advantages and uses of new features and updates in the system. Therap also conducts webinars and events specific to states to guide the users. In these events and webinars, the user gets training on how to use the system, what are the features of the system, and how new features can help their agencies. These events are only for describing the system to its user. Through this informative training approach Therap markets its application and grabs the attention of potential users.

Blogs & Press Release: Therap published blogs and press releases which also acts like a marketing strategy for the company. Therap publishes blogs about its upcoming updates and current achievements. Through the blogs and press releases the company shares the view of the customers about the company that creates brand awareness and helps to promote the service.

Print Materials: Therap organizes several events which are for state specific users to guide them how to use the software and let the new users get acquainted with the software. Moreover, Therap participates several events like this as an exhibitor. In these events the company hands out catalog, flyers to the attendees and there are also banners on the booth and around the booth which helps to promote the brand and grab the attention of any new potential user.

2.4 Operations Management and Information System Practices

2.4.1 Use of Information Systems in the Company

The use of Information System plays a vital role in the company's overall business process and business growth. Therap is a software company that provides Software as a Service. So, the company has to maintain an information system to provide service to its customers. The software is used to document the individual's sensitive information and health data digitally. To run this software Therap uses colocation providers where the servers and networking equipment resides. Therap also has a cloud platform to manage data and run software globally. Therap software is also compatible with mobile devices for providing some features which allows to document individual data while providing home-based services.

Therap application also supports the customer with data analysis by using Business Intelligence technology. Using this the customers are able to see the trend of information about each individual over a period of time which helps to provide more meaningful service to them.

Therap application also supports 24x7 customer support and has a dedicated feature for providing this service in the software. It helps the customer to communicate with the company regarding various issues or problems they face while using the software.

Inside the company Therap has its own workspace accounts. All the employees are given access to their individual workspace accounts using which they can communicate with the other employees and customers as well. All internal procedures are mostly done using the workspace profile.

When a company relies on an information system heavily for all of its work, it is necessary to ensure the security of the information system. Moreover, as Therap deals with sensitive data it is mandatory for the company to maintain the federally mandated security protocols for its information system. Server Security and Data Encryption is one of them. Therap encrypts all of its data which includes data stored in the database and data transfer used for communication. To ensure server security, Therap follows strict protocols and provides least privilege for server access. Only authorized personnel are authorized to access the server room. Also, to maintain the overall security of the information the access to the information system and its data is limited to need basis only. Therap follows least privilege access and need based privilege access so that access to the information system can be limited and the security of the overall information system can be ensured.

2.5 Industry and Competitive Analysis

2.5.1 Porter's Five Forces Analysis

Porter's Fives Forces model helps to identify the 5 competitive forces for any business which helps to identify how much competitive advantage they have in their running industry. It also helps to determine the company's strengths and weaknesses so that the company can plan their business accordingly ahead of time to gain competitive advantage in the market. The porter's five forces are,

1. Threat of New Entry
2. Threat of Substitutes
3. Bargaining Power of the Buyer
4. Bargaining Power of the Supplier and,

5. Industry Rivalry

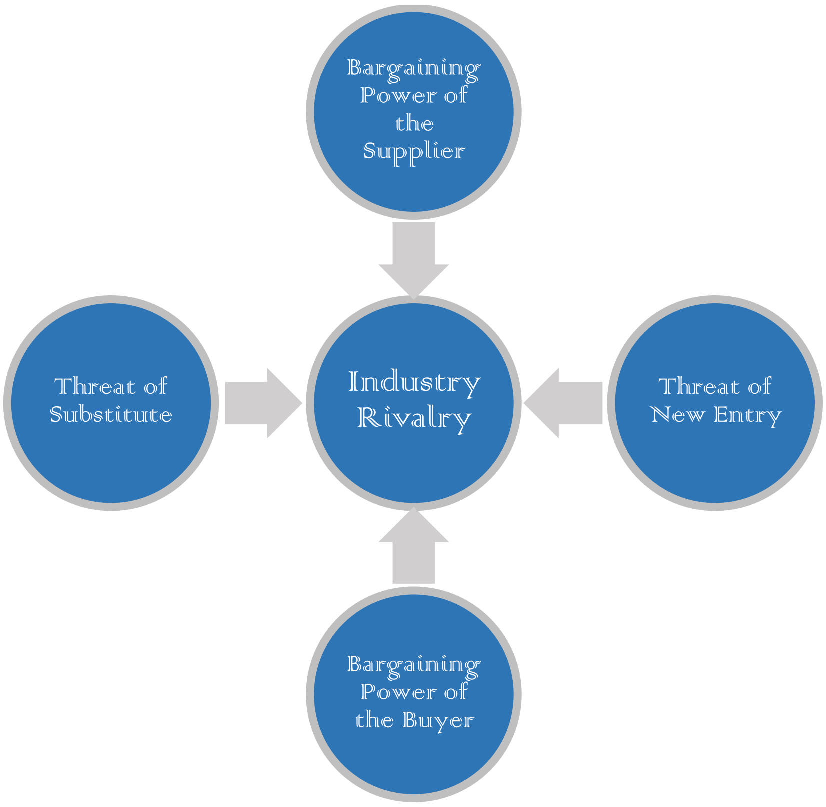
Bargaining Power of the Supplier
Threat of Substitute
Industry Rivalry
Threat of New Entry
Bargaining Power of the Buyer

Figure 2: Porter's Five Forces

Threat of New Entry: A company's competitive advantage depends highly on the potential new competitor in the industry as new entrants possess new threats to the existing players in the market. The less the cost of entry is the less is the barrier to enter and the higher is the threat of new entry. Therap technically serves in the healthcare industry of the US. To enter in the healthcare industry, it requires a lot of research, investment, and compliance of regulatory bodies. The hardest part is getting compliant with the government and federal mandates like HIPAA. It also requires expertise in software development, information security practices which gets more solid over years of experience. Moreover, Therap has been in the market for many years and over the years with experience and use of technology it has become the leader of the industry which makes it difficult for the new entrants to establish in this market.

Considering these facts Therap has strong brand recognition and market reputation. For this, the threat of new entrants for Therap is very low.

Threat of Substitute: Substitutes poses threat to the company in the industry as it can potentially replace the products or services of the company in no time. In the healthcare industry, especially in the Electronic Health Record segment, there are number of substitutes. However, Therap offers configurable software which the customer can configure upon request So, even if customers find an alternative in the market, they will not be able to provide the same quality service as Therap. Moreover, there will also be a switching cost for the customers as they will need to shift entirely from an information system to another. This makes the threat of substitute of Therap low in the industry.

Bargaining Power of the Buyer: Bargaining power of the buyer or customer arises when there are several competitors in the industry who serve the same quality product/services in the market. The more the competitors in the market the higher is the bargaining power. As mentioned earlier in the industry there are several competitors of Therap. However, being the industry leader Therap has competitive advantage in the market. Therap also has advantages when it comes to providing quality service, security, software usability and configurability. Due to these factors the bargaining power of the buyer/customers can be considered moderate.

Bargaining Power of the Supplier: If in the industry where the company is serving the suppliers are prominent and rare, they can demand more value for themselves and charge higher prices for the services they provide. This increases the power of bargaining for the suppliers. As mentioned, Therap serves in the industry where the sensitivity of information is very high which makes the security and privacy of information a concern which should be taken care of with utmost priority. To ensure the information security of the system, Therap only uses prominent vendors of the industry who are trusted, whose quality of service is impeccable and are compliant with government and federal mandates for providing the service. Also, to ensure the service quality Therap has to use top vendors for servers and networking equipment, colocation providers, backup service providers and database providers. As Therap deals with only the vendors that are industry leaders in each of their individual sectors the bargaining power of the supplier is moderate for the company. However, Therap has been in the market since 2003 and during this time the company has made several strategic partnerships with the key vendors and suppliers which helps to mitigate the risk of the bargaining power of suppliers for Therap.

Industry Rivalry: The industry rivalry and competitiveness depend on the number of competitors in the industry who provide a similar kind of service that can be a better or equal alternative for the company's product. In the US this market is quite attractive, and this makes the nature of the market quite competitive. Moreover, in this industry where Therap serves there are several alternatives. For example, for the Electronic Health Record sector there are several alternatives. However, over the years Therap has become the industry leader and has built up a well-known reputation and brand image in the industry. Therap also has established a commitment towards the continuous improvement of its software through adding new features and customer satisfaction. It has a potential impact in the market as it differentiates Therap from its other competitors and makes the industry rivalry low for the company.

2.5.2 SWOT Analysis

SWOT analysis is the strategic analysis of business objective and performance internally and externally. Using SWOT analysis, a company gets to know what it does the best, where it needs to improve, and what are the scope of future improvements. SWOT analysis tools analyze the business in two ways internally and externally. SWOT stands for,

- Strengths
- Weaknesses
- Opportunities &
- Threats

The main purpose of SWOT analysis is to identify and approach new opportunities using the company’s strength and work on the improvements of its weaknesses to mitigate the potential future threats.

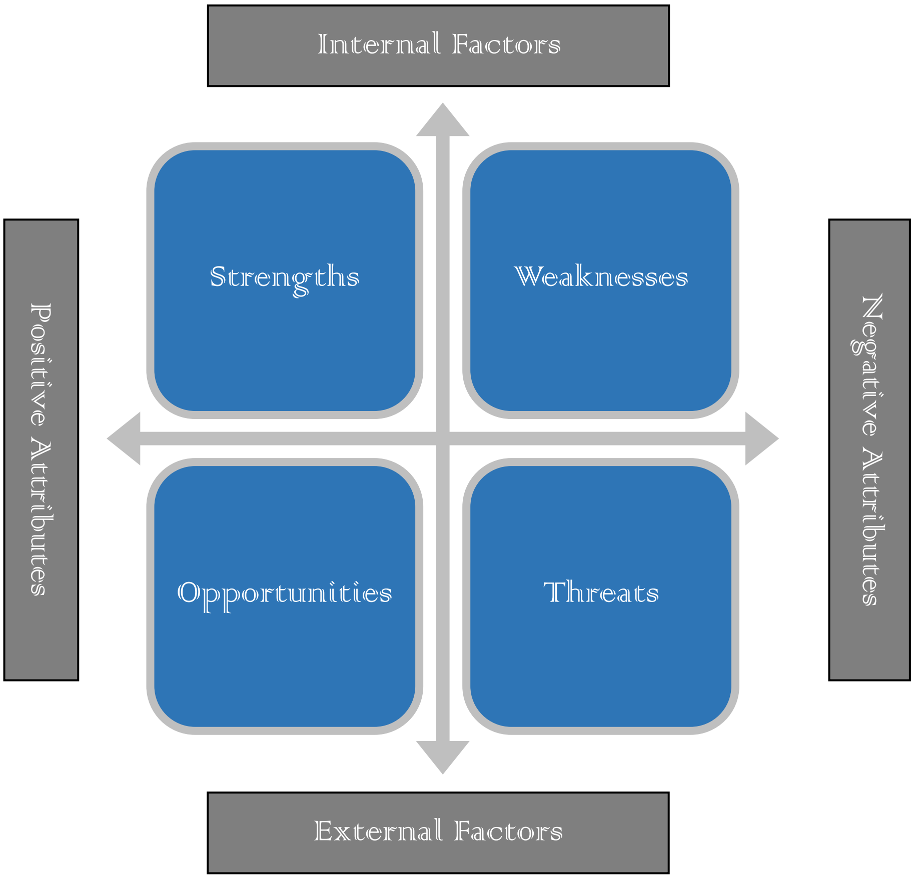

Figure 3: SWOT Analysis for Therap

Strengths: The followings can be identified as strength of the company:

- Therap has built a strong brand value, brand reputation in the healthcare industry.
- Therap software is configurable (upon request) based on provider needs. In the US different states have different requirements, regulations and mandates. The providers or agencies who are the users of the software can request to configure the software based on their needs and their state regulatory and mandates.
- Since the establishment of the company, Therap has had a strong focus on the continuous improvement to its software, enhancing customer satisfaction through state-of-the-art technology.
- Built in tools for trend analysis. Therap has tools within the software that can be used to analyze the individual's data who are being served. By analyzing this data service

provider can tailor their service based on individual necessities. This helps the provider to bring a better outcome.

- Over the years Therap has built a good partnership with some of its key suppliers like Oracle, Ancor, HL7 etc.
- The company has built up its brand image as a leader in the industry.
- A greater challenge for the companies who serve in the healthcare industry is complying with the regulations governed and mandated by states and/or federal governments. Whenever there is an update or change in the regulations the company has to change or update its information system accordingly. As Therap is HIPAA compliant and also compliant with several regulatory bodies it gives the company an upper edge competing in the market.
- Pricing varies from customer to customer based on the service provider wants from the company. The customers will need to pay for only the number of modules they want to use.
- A single software can server many sectors of healthcare industry. For example, IDD, Aging and Home Health Services, Special Education and School Health Services, Autism program etc.

Weaknesses: The following can be identified as the weakness of the company

- Majority of the service is provided in the US market and the global reach is still limited.
- The promotion of the application is mainly based on word of mouth or customer referrals.

Opportunities:

- Expanding global reach based on the rising demand of the electronic health record system.
- Growing demand of the electronic health record system within the US industry.
- Emergence of technology and people embracing the new technologies over the time.
- In the era of Machine learning and IoT, Therap can also integrate with ML and IoT to enter another market segment which will make the electronic health record system and documentation a lot easier.

Threats:

- As Therap provides Software as a Service in the healthcare industry, it has to deal with a lot of sensitive information. Most of this information can be used to trace back the identity of an individual. In the information system industry, PIIs are prone to cybersecurity risk. For this the biggest threat for the company is the unforeseen cyber-attack.
- Possibility of new entrants in the market as the industry is lucrative and the demand for electronic health record systems is increasing in the US market.
- Possibility of technological disruption due to unavoidable circumstances.

2.6 Summary and Conclusion

Therap started its journey in 2003 through providing Software as a Service to the agencies and providers who give support to the individuals with special needs. Since then, it has come a long way achieving successful implementation of its product and customer satisfaction. In the niche market of IDD industry of healthcare industry over the time Therap has become the market leader. Therap achieved evolution in documenting the health record system by shifting it from paper based to fully electronic records. As an organization Therap practices democratic leadership styles which encourages the employees to add value to the company decision and it encourages employee's empowerment and collaboration. The company uses various marketing tools to promote the software. Due to the high brand value and customer reputation word of mouth referral plays a vital role in promoting the product it serves. As an information system company Therap has to rely heavily on information system technology for all of its work and security of the system. The company also has its own strengths and weaknesses; however, it overcomes all its challenges and threats through ongoing strategic planning and adaptation. Overall, Therap has become the industry leader in this market serving in all the states of the US and expanding its operation globally. It has a well-established technology with strong commitment to serve its customers better and excel further in the industry.

Chapter 3

Project Part

3.1 Introduction

Compliance and Quality control is a crucial part of an information system organization specially for the ones who provide SaaS. Therap serves in the healthcare industry of the US, and the US healthcare industry has a lot of state and federal regulatory requirements. Also, the quality control ensures that the product meets the highest customer satisfaction.

Any SaaS company must adhere to the regulatory mandates applicable for the company. As Therap serves in the healthcare industry it has to comply with many state and federal mandates to do business and get customers. These state and federal mandated regulations also ensure that the SaaS is secure to use. For example, in the US any organization that serves in the healthcare market must adhere to HIPAA compliance which is a federal law that protects patient's identity and security. It also ensures the privacy and security of an individual's sensitive health information. Ensuring this kind of compliance is also necessary as any violation under any of these regulations will result in penalties. Any violation may also lead to legal liabilities which will eventually hamper the company reputation. Apart from regulatory compliances the company also needs to follow industry best practices to maintain the information system and ensure its data security. The quality control helps to ensure that the software is being developed keeping in mind the need and expectation of the customers.

Moreover, through compliance and quality control companies can also ensure data security to protect the sensitive information of individuals. Data security is the highest priority for the company and Therap ensures data security through availability, integrity and confidentiality. Data security can be ensured by conducting regular audits, encrypting the information system and its data transfer, and monitoring the access controls to the information system. For this, compliance and quality control acts as an essential part for a SaaS company. It helps the company to build customer value, avoid any legal issues related to regulatory compliance and to run business in a successful way by meeting the customer needs and satisfaction.

3.1.1 Objective

The main objective of this chapter is to understand the primary activities of a SaaS company that ensures compliance for the company in context of Therap.

3.1.2. Significance

The scope of the study primarily focuses on the activities of the Compliance and Quality control department to make it understand how compliance and quality control activities can be conducted in a SaaS company to ensure the compliance of internal and external regulation in the context of Therap. Since, Therap has been in the market from 2003, the processes are well established. However, these go through continuous improvement to ensure the most efficiency of the process and handle the new challenges that come along the way.

3.1.3. Limitation of Study

Therap Services, LLC deals with sensitive health information of individuals in the US. There are several state and federal mandates due to which access to information is very limited. Due to this less data are presented for being confidential and/or proprietary information of Therap.

3.2 Methodology

To complete this report the primary sources of information was,

- The work experience and knowledge gained from the company.
- Conversation with employees, and
- In person training

The secondary source of information was.

- Therap BD website
- Therap US website
- Journals and publications of industry best practices

3.3 Findings and Analysis

Being a SaaS company Therap gets audited every year against some set of controls. Against these controls the company needs to submit all the available documents, policies, procedures, and activities. For the SaaS company it is necessary to ensure that all the internal controls are in place to ensure Information System Security. Types of internal controls are,

- Preventive Controls that should be in place to prevent incidents.
- Corrective Controls that should be in place to take steps in times when there is an incident.
- Detective Controls that should be in place to provide evidence for error and traces of access to the information system.

Therap has all these types of controls in place to ensure compliance and quality control.

3.3.1 Organizational Document Review

Organization’s internal document review is an important process to ensure the compliance with regulatory bodies. Reviewing the documents includes all the organizational policies, procedures, documents to any operational activities. Reviewing the documents ensures that the documents are up-to-date, compliant with regulatory laws, reflect accurate organizational activities, information, and procedures. The following are the steps of the organizational document review process:

- The first step of the process is identifying the documents that need to be reviewed. The documents include policies, procedures, and the related procedural documents. Every document has its own review frequency. Based on the review frequency the documents are identified that need review.
- The next step involves identifying the person who will review the document and conduct the review.
- Updating the document as applicable, based on new regulations, changes in company activity and policy, updates in industry best practices.
- The final step involves approving the document by the document owner. Generally, C-suite executives are the document owner and approver of any changes made in the document.

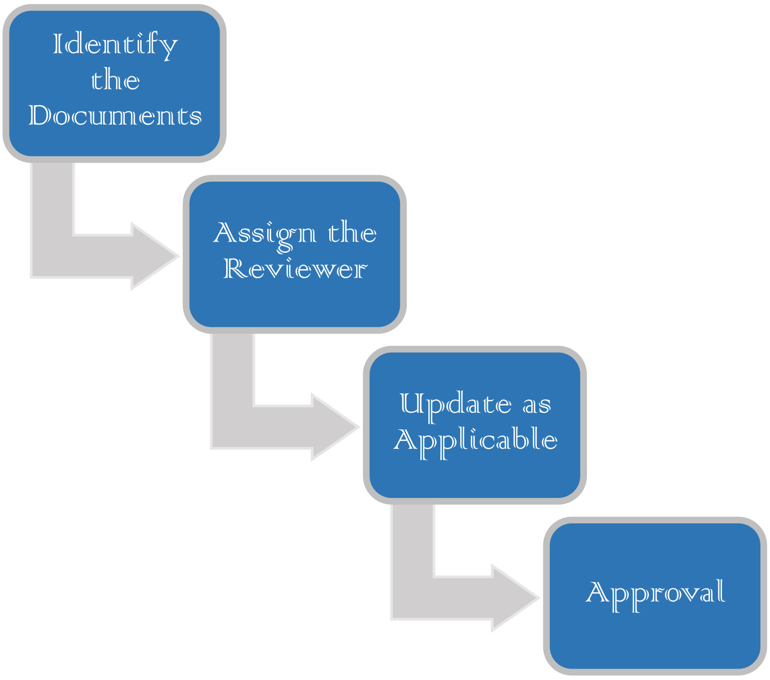

Figure 4: Document Review Process

3.3.2. Internal Audit

To ensure the compliance and quality control requirements of the company, internal audit is a necessary tool. It helps to identify the potential risks, improve the internal process, promote transparency and accountability, and it also helps to mitigate the legal liabilities by ensuring compliance with the regulatory authoritative bodies. As a part of the internal audit the following things are done

- Review of information system resources like server security check, database security check, data security check, data encryption check, system vulnerability check, and audit of networking devices etc. Through these resources review, it is ensured that the industry best practices are followed to ensure security and availability of the system, and it also gets reviewed that all the necessary state and federal mandates are being followed while running the SaaS.

- Critical vendors review. Any software and hardware used to provide the service of the company falls under this vendor criteria. This review ensures that all the critical vendors are certified to provide their services to the company and all the critical and non-critical vendors have all the security components needed for the SaaS, and those are safe to use.
- Audit check of office inventory.
- Review of access control to the information system.
- Review of employee access enforcement and revocation upon joining and termination.
- Review of physical safety of the employees and information system assets from unforeseen hazards. For example, Fire safety, Earthquake etc.

3.3.3 External Audit

External audit provides the scope of independent assessment of the company resources and its security. It improves the credibility of the assessments and provides a comprehensive report of the assessment through the evaluation of the internal processes of the company. Apart from ensuring compliance it also gives a different perspective into identifying the company weaknesses, lacking, and vulnerabilities. To make sure the regulatory compliance Therap currently undergoes the following external audits:

- HIPAA Audit
- SOC2 Audit

HIPAA Audit: Through the HIPAA audit the company gets the certification of HIPAA compliance. As per the HIPAA law the organization must adhere to the Privacy Rule, Security

Rule and Breach Notification Rule to get HIPAA compliance. The auditor checks against the following criteria for HIPAA audit:

- Privacy rule requirements such as protection of individually identifiable health information, patient's/individual's right over their health information, permissible use and disclosure of PHI, company privacy practices, privacy training and awareness programs.
- Security rule checks such as the secure transfer, storing, and reception of PHI data, access controls to the PHI data, role-based access control to the information system etc.
- Security breach notification requirements.
- Other Administrative Requirements such as unique health identifiers, transaction rules, code set standards etc.

SOC2 Audit: SOC2 certification is also an independent auditor's assessment. SOC2 audit conducted against the five Trust Service Criteria set by AICPA. Here it is assessed how much the company complies with those five trust principles based on the information system processes.

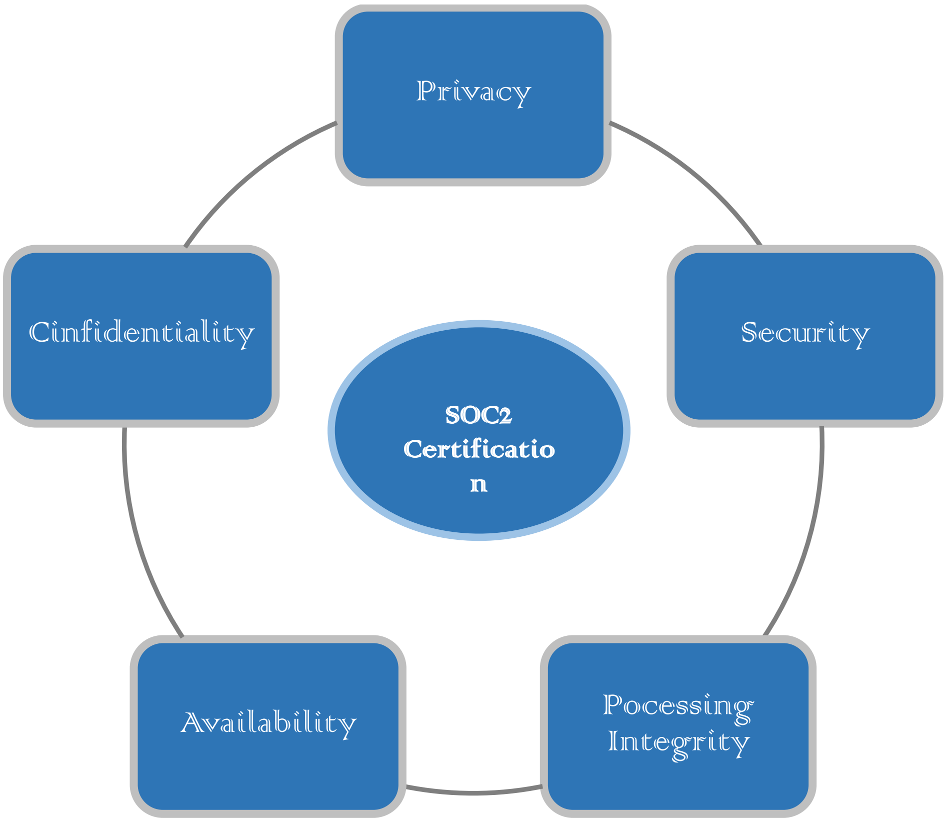

Figure 5: SOC2 Audit & Five Trust Principles

- **Privacy:** Privacy principle controls the use, retention, transfer, disclosure, and disposal of the sensitive information as per the AICPA's Generally Accepted Privacy Principles (GAPP). Against the privacy control for SOC2 general audit checklists for a SaaS company providing service in the healthcare industry are,
  - Access to the information system and PHI
  - Two factor authentications
  - Data encryption
- **Security:** Security rules controls the protection mechanism of the information system to prevent any unauthorized access. For the security control the general checklist consists of

  - Network/application firewall
  - Two factor authentication
  - Intrusion detection

- **Availability:** This control refers to availability of the system as per the business agreement. General checklist for this control is:
  - Performance monitoring
  - Disaster handling
  - Security Incident Handling

- **Processing Integrity:** This control addresses the data processing integrity of the information system through:
  - Performance Monitoring
  - Quality Assurance

- **Confidentiality:** Confidentiality refers if the access to the information system and sensitive information is restricted to specific set of personnel in the organization. Checklist for this consists of:
  - Encryption
  - Network and Application firewall setting
  - Access control

3.3.4 Training and Awareness Program

Therap as a SaaS has to deal with a lot of sensitive PII/PHI. As a part of ensuring compliance, the employees get awareness training on several cyber security scenarios so that they can learn how to stay aware and protect information from these cyber-attacks. The training includes,

- Awareness training on phishing attack.
- Awareness training on social engineering.
- Awareness training on spam.
- Awareness training on data security.
- Awareness training on device security.
- Awareness training on handling sensitive data.

Moreover, training on regulatory compliance are given so that the employees can understand their roles and responsibilities in terms of company compliance and promote safe work culture to ensure the security of the information they are working on.

3.4 Summary and Conclusion

The compliance and quality control activities of Therap ensures the overall security of the application. It also helps the company to follow the state and federal mandates and comply with those. For a SaaS company compliance and quality control is necessary as it can reduce the risk of non-compliance and quality issues. This can help to increase the brand reputation, the credibility of the service, and to create customer goodwill. The SaaS company also needs to review and update its compliance framework, internal documents regularly so that it can stay updated with the newest regulations, mandates, and industry best practices. To ensure the security of the information system audit form independent assessors also helps the company to identify its weaknesses in the current process and enhance the credibility of its service through providing a comprehensive report of all the processes. In a nutshell, compliance and quality control activities should be an integral part of a SaaS company and by prioritizing it the company can gain competitive advantage in the market ensuring the information security, customer satisfaction and gain long term success.

3.5 Recommendation

- To enhance the credibility of the service Therap can get more certification on some other federal regulations like FedRAMP, StateRAMP, MARS-E.
- To expand the business globally especially in the European region going for GDPR compliance.
- Increasing the frequency of internal audit to ensure more transparency, accountability, and security.
- Provide more security awareness training so that the employees can learn the best practices of ensuring information security.
- Digitalize the policy review process using third party project management or ticketing systems. The company can keep the internal documents in a database or system. A ticket will be raised automatically when it's time for review. When the review process is done the reviewer can update the status in the ticketing system and a notification will be sent to the approver for approval of the review. It will reduce the time of document review period and ensure all the documents are reviewed/approved on time.

References

About Therap. (2023, April 29). (Therap (BD) Ltd) Retrieved April 29, 2023, from https://therapbd.com/#about-us

About Therap Services. (2023, April 29). (Therap Services) Retrieved April 29, 2023, from https://www.therapservices.net/

Gürel, E. (2017). SWOT ANALYSIS: A THEORETICAL REVIEW. *Journal of International Social Research*.

Goyal, A. (2021). A Critical Analysis of Porter's 5 Forces Model of Competitive Advantage.

HIPAA Audit. (2023, May 2). Retrieved May 1, 2023, from The HIPAA Journal: https://www.hipaajournal.com/hipaa-audit-checklist/

Internal Control Types and Activities. (2023, May 1). (Syracuse University) Retrieved May 3, 2023, from https://bfas.syr.edu/audit/general-internal-controls/internal-control-types-and-activities/

What is SOC 2 | Guide to SOC 2 Compliance & Certification. (2023, May 2). Retrieved May 1, 2023, from Imperva.

Appendix A.

C-Suite Executives: C stands for chief, hence C-Suite executives refers to high ranked authorities and officers within their area of expertise.

Controls: Set of activities/processes/guides to ensure security and compliance.

Niche Market: A segment of a larger market that can be identified/defined by its unique needs.

IDD Industry: IDD industry refers to all the agencies and providers who serve people with Intellectual and Developmental Disabilities.

Ticketing System: IT ticket management system is the process that organizations use to collect requests, track the ticket/request lifecycle from creation to resolution. Tickets/requests can be assigned to anyone for resolution and when the resolution is complete tickets can be closed.

Least Privilege: Providing minimum required access necessary to perform assigned job responsibility.

Colocation Provider: A data center facility in which a business can rent space for servers and other computing hardware.