Report On

Managing Compliance in a Healthcare SaaS Organization: Internal and External Audit Practices at Therap

By

Md. Touhiduzzaman Touhid
22264067

An internship report submitted to the BRAC Business School in partial fulfilment of the requirements for the degree of
Master of Business Administration (MBA)

BRAC Business School
BRAC University
May 2026

Declaration

It is hereby declared that

1. The internship report submitted is my own original work while completing 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:

_____

Md. Touhiduzzaman Touhid
22264067

Supervisor's Full Name & Signature:

_____

Dr. Afsana Akhtar
Assistant Professor, BRAC Business School
BRAC University

Letter of Transmittal

Dr. Afsana Akhtar
Assistant Professor
BRAC Business School
BRAC University
Merul Badda, Dhaka 1212

Subject: Submission of Internship Report on “Managing Compliance in a Healthcare SaaS Organization: Internal and External Audit Practices at Therap”

Dear Ma’am,

I am glad to submit this internship report titled "Managing Compliance in a Healthcare SaaS Organization: Internal and External Audit Practices at Therap" as part of my MBA requirements, BRAC Business School, BRAC University.

This report is completely based on my actual working experience in the CQC team of Therap (BD) Ltd. where I was involved in compliance and audit related tasks. It covers my direct experience with audit preparation tasks, evidence verification, internal documentation reviews, tracking training records, monitoring vendor risks, and audit coordination in a healthcare SaaS environment.

I really hope that this report meets the expected standards and demonstrates the learning and growth I experienced during my internship.

Best Regards,
Md. Touhiduzzaman Touhid
Student ID: 22264067
BRAC Business School
BRAC University
Date: April 23, 2026

Non-Disclosure Agreement

This Agreement is signed between Therap (BD) Ltd. and the student and is signed at BRAC University.

_____

Md. Touhiduzzaman Touhid
ID: 22264067

Acknowledgement

To start with, I would like to humbly thank my academic supervisor who guided and directed me during the process of writing this internship report. The valuable feedback and academic insight I received in this process helped me to organize my professional experience as a meaningful analytical study.

I would like to acknowledge my deep gratitude to Therap (BD) Ltd. that allowed me to use my professional capacity as a Compliance and Quality Control Specialist II as the basis of this internship report. Specifically, I would like to mention the help of Malisa Mehjabeen and Iffat Arzuman, Lead Compliance and Quality Control Specialists, who guided, mentored, and supported me throughout the period. Their professional knowledge and management expertise have made a significant contribution to my comprehension of how compliance governance and audit coordination practice should be conducted.

Finally, I also owe my family and well-wishers who have encouraged and supported me all through my MBA.

Executive Summary

This report mainly examines how compliance functions and audit activities are performed at Therap (BD) Ltd., a healthcare SaaS company that deals with sensitive health related information. I did this on my internship between November 2025 and April 2026, where I was working on audit prep, evidence validation, document review, training compliance tracking, aiding with vendor risk, and answering auditors. The report examines how such tasks create actual governance in a regulated technological sector, rather than viewing compliance as a formality.

The investigation follows a qualitative paradigm methodologically because it has relied on first-hand involvement, systematic observation, and the examination of non-confidential records. The subject of discussion is the interaction of audit processes, documentation procedures, risk management, and controls, which relate to training in a multi-framework setting due to regulatory requirements, including HIPAA, SOC 2, and others. It also reflects on the overall organizational environment of Therap, where secure systems, coordination, and discipline of processes are essential to the day-to-day affairs.

The results indicate that Therap maintains a fairly effective compliance environment, with frequent review cycles, centralized documentation procedure, and team interdependence. Simultaneously, the analysis reveals the following real-world issues, such as delays in evidence gathering, the need to manually map similar requirements across frameworks, cross-team dependencies, and time zone coordination. The issues are not indicative of a weak control environment but rather are a mirror of the complications of multi-framework compliance in a real organizational setting.

Lastly, audit work at Therap is not lower than what the outside world requires. They contribute to a better system of governance and risk management within the organization, a high level of accountability, disciplined documentation, and continuous improvement. The report suggests enhancing evidence aggregation, implementing AI automation to eliminate redundant activities, formalizing pre-audit activities, specifying response timelines, and improving monitoring through visualization in the form of dashboards, among other measures.

Table Of Contents

List of Tables

List of Figures

List of Acronyms

AC - Access Control

AICPA - American Institute of Certified Public Accountants

CISO - Chief Information Security Officer

EHR - Electronic Health Record

HIPAA - Health Insurance Portability and Accountability Act

IDD - Intellectual and Developmental Disabilities

ITG - Information Technology Governance

ITM - Information Technology Management

LTSS - Long-Term Services and Supports

PHI - Protected Health Information

POA&M - Plan of Action and Milestones

SaaS - Software as a Service

SOC 2 - System and Organization Controls 2

NIST - National Institute of Standards and Technology

Chapter 1

Overview of Internship

1.1 Student Information

Name: Md. Touhiduzzaman Touhid
Student ID: 22264067
Program: Master of Business Administration (MBA)
Major: Information Technology Management (ITM)

1.2 Internship Information

1.2.1 Organization Information

Therap (BD) Ltd. operates as part of Therap's global healthcare Software-as-a-Service (SaaS) ecosystem and provides Electronic Health Record (EHR) solutions for organizations that support people with intellectual and developmental disabilities (IDD). The organization operates in a highly regulated environment where the security and privacy of sensitive health data and compliance with security and privacy requirements are paramount to its operations.

Office Address:
Block C, House 47, Road No. 4
Banani, Dhaka, Bangladesh

1.2.2 Supervisor Information

During this time, I reported directly to:

- Malisa Mehjabeen - Lead Compliance and Quality Control Specialist
- Iffat Arzuman - Lead Compliance and Quality Control Specialist

Both supervisors provided direction on compliance operations, preparation of audits, and coordination activities between teams.

1.2.3 Job Scope and Responsibilities

During the audit assessment period from November to April, my responsibilities were mainly focused on compliance support and audit readiness activities. My basic responsibilities were as follows:

- Coordinating internal audit preparation and validation of evidence prior to audit submission
- Gathering and submitting audit evidence in accordance with HIPAA, SOC2, and other framework requirements
- Maintenance of vendor risk documentation and support in the collection of SOC2 reports for key vendors
- Optimization of vendor matrix documentation in terms of traceability and clarity
- Monitoring organizational-wide security awareness training completion on a monthly basis
- Assisting with access review coordination according to audit requirements
- Tracking change management documentation of software releases
- Evidence mapping with audit requirements and working on documentation gaps
- Responding to the auditor's additional queries and making sure the expected artifacts were submitted

These responsibilities involved working with several teams, paying attention to documentation, and maintaining communication with stakeholders, local and overseas.

1.2.4 Work Schedule and Coordination Structure

During the period of internship-equivalent, I was operating from the Bangladesh office while keeping regular communication with the stakeholders in the US. My job had typical office hours; however, audit preparation often required inter-time zone coordination. As a result, meetings with US counterparts were often scheduled in the evening to coincide with their working hours.

Twice a week, governance meetings took place to ensure audit progress, discuss pending evidence requirements, and clarify documentation requirements. In addition to planned meetings, urgent matters relating to the audit were dealt with by email communication and ad hoc online communication.

This form of coordination required serious attention to time management to avoid any kind of miscommunication or delays.

1.3 Internship Outcomes

1.3.1 Contribution to the Organization

I could make several meaningful contributions during this time period:

- Published and monitored organization-wide internal training for compliance
- Helped to collect, validate, and submit audit evidence in several different control areas
- Responded to auditor clarification requests, supported evidence acceptance
- Optimized the vendor inventory documentation for better traceability
- Contributed to the development of the System Security and Privacy Plan (SSPP) for several control families such as AC, AT, SC, IA, and MA
- Supported in the remediation efforts to close audit findings

These contributions helped in maintaining the consistency of documentation, and also supported making the audit engagement successful.

1.3.2 Benefits to the Student

This experience assisted me in greatly enhancing my knowledge of compliance and governance practices in a regulated technology environment. In particular, I gained hands-on knowledge of:

- IT governance mechanisms in healthcare SaaS companies
- Compliance management across multiple regulatory frameworks
- Coordinating with Stakeholders Across International Time Zones
- Maintaining Control Documentation and Evidence Management Discipline

The internship also helped me to become a better analytical thinker, a better communicator, and a better person to work in a structured compliance environment.

1.3.3 Challenges Faced

Although the experience was greatly valuable, several difficulties were also encountered during the process:

- Delays in evidence collection due to cross team dependencies
- Manual mapping of similar control requirements along audit frameworks
- Coordination problems due to time zone changes with counterparts in the US

These types of difficulties actually indicate the complexity of dealing with compliance and quality control activities in a multinational organization structure.

1.3.4 Suggestions to the Organization

Based on my observations, there are a number of improvements that could be made for future audits to make them more robust:

- Further optimization of the evidence collection and tracking process
- Internal reviews of the critical controls prior to the opening of the external assessment windows
- Creation of a structured and comprehensive audit readiness checklist for repeating requirements

Such initiatives could contribute to the reduction of reactive work during the audit periods and make the whole process more efficient.

Chapter 2

Organizational Analysis and Strategic Context

2.1 Introduction

This chapter presents an overview of Therap (BD) Ltd. and describes the organizational setting in which this report is based. Since the focus in the report is on compliance management and audit governance in the context of a healthcare SaaS environment, it is important to understand how the company functions as a business, how work is coordinated, and how the business is influenced by the compliance-related activities.

Therap operates in a specialized area of healthcare technology and supplies Software as a Service (SaaS) solution to organizations that serve individuals with intellectual and developmental disabilities and other care-based populations. Because the company deals with sensitive service and health-related information, its operations are not only dependent on technical capability, but also on disciplined processes, secure systems, and structured coordination across teams. For that reason, it is necessary to understand the organization itself before discussing the practices of compliance and audit that are examined in the next chapter.

2.1.1 Objective of Chapter 2

The objective of this chapter is to discuss Therap (BD) Ltd. from an organizational point of view and analyse the key business practices that define the operations. More specifically, this chapter presents an overview of the company, evaluates its management and marketing practices, reviews its operational and information system environment, and examines the position of the company in the industry through competitive analysis. This discussion also forms the basis for the following chapter, in which the issue of compliance and audit governance is analysed in more detail.

2.1.2 Scope of the Study

The scope of this chapter is confined to the organizational and business practices which could be comprehended through hands on exposure, company level information, and the overall working environment which was seen during the internship period. The chapter is primarily concerned with Therap as an organization rather than with a single department. However, in a

few areas there has been limited context from governance- and compliance-related activities included where it helps explain broader organizational practices more clearly.

2.1.3 Methodology

This chapter has been prepared mainly on the basis of qualitative analysis. The discussion is based on practical observation, exposure to organizational processes and review of company-related information available through the workplace environment and public organizational context. The analysis also relies on the coordination observed among teams, use of internal systems, as well as the structural approach employed by the company in documentation, communications and operational control.

2.1.4 Significance of the Study

This study is significant as it brings on board useful insights on how compliance management and audit-related functions work in a healthcare SaaS company. Governance, documentation practices, and regulatory compliance are closely related to the everyday operations in companies concerning sensitive health-related information.

The report is also significant in the sense that it connects the academic concepts of Information Technology Management, such as internal control and risk management, with the actual practice at work. The study contributes to explaining the application of these concepts in a real organizational context through direct participation in compliance-related activities.

2.1.5 Limitations

There are a few limitations to this study. To start with, the analysis relies on experience in one organization, Therap (BD) Ltd., and therefore, its results may not be a true reflection of the practice in other similar organizations or industries. Moreover, there were some internal information that could not be discussed in details because of a restriction of confidentiality. Consequently, some of the analysis areas are not at the specific level. Lastly, the report is primarily concerned with compliance and audit-related practices related to the work experience, meaning that other organizational functions are not studied in the depth of this report.

2.2 Overview of the Company

Figure 1 - Therap Services LLC

2.2.1 Background of the Company

Therap Services LLC is a US-based software company registered in Bangladesh in 2004 under the name Therap (BD) Ltd. The company started its operations in the United States in the year 2003 and its head office is situated in Connecticut. Therap offers Software as a Service (SaaS) solution to government agencies, non-governmental organizations, and service providers that serve people in need of long-term care and support, specifically in the field of intellectual and developmental disabilities.

The company was founded with the mission of enhancing the of service for the people relying on support systems and specialized care. Throughout the years, Therap has come up with an elaborate digital platform that assists service provider organizations in maintaining documentation, communication, reporting, and operational processes in a more efficient and organized manner. The company aims to enhance the process of service coordination and accountability as well as prioritize the needs of individuals, families, and care professionals as the core of its activities through its services.

2.2.2 Nature of Business

Therap operates in the healthcare technology sector and serves a niche market through electronic documentation and service management solutions. Its software is used by organizations involved in intellectual and developmental disability services, home and community-based services, long-term support services, aging and home health, special education, and related support systems.

Therap comes with a vast array of modules to aid different operational and documentation requirements. These modules are used to manage records, communication, reporting, billing, workflow tracking, and other administrative and care-related functions, within service providers. Since it is used in sectors where accuracy, continuity and accountability are extremely important aspects, the business model of the company is strongly linked to the reliability of a process, handling information securely and complying with what is expected by regulation.

2.2.3 Mission and Business Focus

Therap's mission is to improve the lives of people with intellectual and developmental disabilities (IDD) who are served by service organizations. Hence, the focus of the business is cantered on supporting organizations working with vulnerable and care-dependent populations. Therap is supporting service providers to work more efficiently using digital tools that enhance documentation, coordination and access to information. As a result, they are able to focus on meaningful outcomes for the people they serve. In practical terms, this translates into the fact that the software is not only built to make operations more efficient, but to support better service delivery, enhancing communication, and improving accountability in record keeping.

2.2.4 Regulatory and Compliance Environment

One of the most important features of Therap's operating environment is that it has a very strong compliance focus. Since the company is dealing with the protected and confidential information, privacy, security, and internal controls are not an optional issue, they are present in the day-to-day operations. This has implications on how documentation is managed, how systems are managed, how access is controlled and how teams coordinate their work. In other words, the compliance environment influences both the technical and managerial sides of the organization.

2.3 Management Practices

2.3.1 Leadership Style

The leadership style at Therap appears to be more collaborative and participative than top-down approach. Day to day works rely heavily on communication across teams, and employees are generally encouraged to raise and report issues, provide updates, and take responsibility for the work assigned to them. This kind of environment is particularly important in a company where different functions often need to work together to complete one process.

From an operational point of view, decision-making often appears to be discussion-based, especially in areas in which more than one team is involved. This does not suggest the absence of authority but rather that coordination plays a major role in the way the work progresses. In an organization that is compliance sensitive, such as Therap, that approach is useful because so many things are dependent on timely input, review, and follow-up by multiple stakeholders.

2.3.2 Leadership Style and Organizational Goals

The collaborative leadership style supports Therap's goals in a number of important ways. First of all, it helps in better communication across departments and allows teams to work together. Second, it is helpful in keeping the employees connected in the organizational process by making them feel responsible and accountable. Third, it is suitable to the nature of the work of the company where many of the operations and governance activities depend on timely coordination of multiple stakeholders.

At the same time, participative leadership requires a discipline and responsiveness, too. And where work is dependent on contributions from different teams, delays or communication gaps may impact upon the efficiency of the overall process. Therefore, although this type of leadership style is beneficial for the empowerment and coordination of employees, the effectiveness of this type of leadership is dependent on regular follow-up and accountability.

2.3.3 Recruitment and Selection Process

Therap has a formal recruitment and selection procedure. Advertisements of job openings are typically done via company portal and social media and applicants are invited to apply to the job depending on the requirements. The selection process involves various stages such as first screening, interviewing sessions, and role-based assessment where necessary.

As Therap is a software company, its hiring process is set to test both the technical and the interpersonal skills of the candidates. Other than academic background and professional knowledge, the following are also considerate in the selection process: communication skills, analytical ability, adaptability and suitability of the role. This particularly applies to a firm where employees might be requested to work in a process-based and team-oriented setting.

2.3.4 Compensation System

Detailed information about the compensation structure of the company was not available for this report. However, it can be considered that compensation practices in a professional software company is usually associated with role requirements, expertise and performance. Since Therap is operating in a specialized sector and is dependent on skilled human resources, compensation and retention are likely to play an important role in sustaining organizational capability.

2.3.5 Training and Development

Therap has a working culture that includes training and development. As the company is operating in a regulated digital space, the employees must be conversant not only with their work responsibilities but also with data protection, information management and company-specific working procedures. For this reason, training is job-oriented and compliance-oriented.

New employees are introduced to the norms and expectations of the organizations through initial guidance and role-based learning. In addition, continued learning and development are encouraged so that employees can continue to enhance their technical knowledge, professional skills, and knowledge of organizational processes. The regular training is especially relevant in a company like Therap, where the nature of work presupposes not only the precision of the operations but also the sense of the duties in terms of information security.

2.3.6 Performance Appraisal System

Therap has performance-oriented work culture whereby feedback, accountability and quality of work are put at the forefront. Even though the elaborate internal appraisal system was not fully accessible to this report. Nevertheless, performance evaluation is definitely associated with quality and consistency of work, responsiveness and capacity to perform given duties efficiently.

The performance in an organisation such as Therap is not simply determined by the output of a task, but also by how the employees operate under the established processes, how they coordinate with other employees, as well as how they uphold professionalism. Such an appraisal method is usually observed in work environments that require working discipline and prompt delivery.

2.4 Marketing Practices

2.4.1 Marketing Strategy

Therap has a very focused niche marketing strategy. The company does not cater to the mass market of healthcare technology but focuses on service providers, agencies and organizations that cater to people with intellectual and developmental disabilities. Such a focused strategy assists such a company in building its expertise and in maintaining its specialized market status.

Due to the work on a clear market segment, Therap can better customize its services, communication and product development. The company strategy is to lay more emphasis on the long-term value, trust and practical relevance as opposed to the mass market visibility.

2.4.2 Target Customers, Targeting, and Positioning Strategy

The target customers of Therap are those government agencies, non-profit organizations and private service providers that require secure, configurable and efficient digital solutions for service documentation and management. The software of the company is especially applicable to the organizations providing intellectual and developmental disability services, home-based support, special education and other forms of specialized care services.

Therap is branding itself as an expert and trusted player in this niche market. It is positioned on the experience, flexibility of the system and secure data handling in addition to supporting the complex operational requirements. This positioning enables the company to have a competitive advantage in a field where credibility and trust are key.

2.4.3 Marketing Channels

Therap uses direct marketing channels and relationship-based marketing channels. The company operates in a small niche within B2B market, so customer relations, professional communication and interaction, webinars, events, conferences, and online marketing are

believed to be more effective in comparison to mass consumer-oriented advertising. Trust, product familiarity and institutional reputation usually play a more important role than mass promotional activity in such markets.

2.4.4 Product Development and Competitive Practices

The flexibility and constant improvement of the software is one of the biggest marketing strengths of Therap. Since various service providers might have different documentation, reporting and regulatory requirements, configurability is a desirable product attribute. This capability to satisfy user needs also helps in customer retention and also in competition positioning.

The ongoing evolution of the platform of the company is also a means to reinforce its position on the market. Competitiveness in a technology-based industry does not solely rely on the current service quality, but also on the ability to upgrade the system in accordance with the shifting operational and market needs.

2.4.5 Branding Activities

Therap's branding seems to be based more on trust, relevance of service and industry reputation. In a specialized market, brand value is often developed by consistent performance, customer experience and longevity rather than by aggressive promotional campaigns. The company's position within its niche implies that its branding is strongly linked to reliability, expertise and continuity of service.

2.4.6 Advertising and Promotion Strategies

The promotional strategies of the company appear to need targeted communication rather than mass communication by advertising. Professional outreach, webinars, events, digital communication and informational updates are the activities that are likely to facilitate product visibility and engagement with customers. In a niche healthcare technology market, these promotional strategies are more feasible because they can assist the company to communicate directly to the concerned groups of users.

2.4.7 Critical Marketing Issues and Gaps

One possible limitation in Therap's marketing strategy is the fact that its visibility may still be concentrated in a relatively narrow section of the industry. While this specialization is a major strength, it may also be a limiting factor to the broader brand recognition outside of its established market. However, based on the company's business model, concentrated penetration of the markets and deep customer trust may be more important than wide but shallow visibility.

2.5 Financial Performance and Accounting Practices

2.5.1 Financial Performance

A detailed financial performance analysis was not possible for this report, because Therap is a private company for which the required financial statements for the last three to five years were not available. As a result, ratio analysis, trend analysis, comparative analysis, etc. formal methods of financial evaluation could not be applied in a rigorous way.

However, from an organizational perspective, the long-term presence of the company in the market, different operational activities, and its position within its niche imply a stable business base. Although such observations can't replace formal financial analysis, they are an indication that the company has maintained its relevance in the markets over the years.

2.5.2 Accounting Practices

It was also not possible to assess the company's accounting practices in detail as internal accounting records, accounting policies and financial disclosures were not accessible. Therefore, areas like accounting method, policy regarding depreciation, financial disclosure practices and the accounting cycle could not be analyzed completely in this chapter.

2.6 Operations Management and Information System Practices

2.6.1 Use of Information Systems in the Company

Information systems play a central role in Therap's operations. As a SaaS company, Therap uses a lot of digital systems for service delivery, documentation, communication, and

operational management. To start with, Therap's customer facing software allows users to communicate with their support group, raise issues and request live help.

In addition to its customer-facing platform, Therap also uses internal digital tools to support communication, workflow management, file sharing and coordination between employees. The way the company runs business, and the need for accuracy, effectiveness, and data control in its operations, demonstrate that it really depends on information systems.

2.6.2 Data Collection, Storage, and Sharing

Since the company deals with sensitive and regulated health information, data collection, storage and sharing has to be done in a controlled and systematic way. Therap's information management is based on structured documentation processes that are supported by centralized systems and controlled access practices. This kind of approach is necessary not only in terms of operational efficiency, but also security, accountability, and compliance.

2.6.3 Database and Office Management Systems

As Therap is a tech-based organization, it is dependent upon digital infrastructure for our day-to-day office and business activities. Inside, the work is supported by organisational tools that take care of the communication, documentation, file management, monitoring and process tracking. These systems can be used to help ensure that tasks are completed in an organized and traceable manner.

2.6.4 Quality Management, Scheduling, and Resource Allocation

Therap illustrates a clear process-oriented approach to operations management. Here the quality is closely linked to documentation standards, internal coordination and consistency in the execution of workflows. Scheduling and resource allocation are also important since different teams often rely on each other for information, review and completion of related tasks.

In a company that operates within a compliance-sensitive environment, the quality of operations will be influenced not only by technical efficiency but also by the ability to keep accurate records, time management, and coordinate effectively between functions. These elements are important for the delivery of service and internal governance.

2.7 Industry and Competitive Analysis

2.7.1 Porter's Five Forces Analysis

Figure 2 - Porter's Five Forces Analysis - Therap

Threat of New Entrants

The threat of new entrants in this market is relatively low. A high level of technical expertise, a major investment, industry knowledge, and adherence to stringent regulatory and security requirements are required to enter this sector. In addition, organizations in this field have to establish trust over time, which puts an additional barrier to new competitors.

Threat of Substitutes

The threat of substitutes is moderately high. Alternative electronic documentation and service management systems may be present but switching from one platform to another may be difficult and expensive for customers. Since organizations using Therap may have operation processes heavily connected with the platform, substitutes will not provide an easy replacement.

Bargaining Power of Buyers

The bargaining power of buyers can be termed as moderate. Customers might have alternatives in the larger market, but Therap's specialization, configurable nature and established reputation

limit their power to some extent. Buyers in this sector are also likely to place a high value on reliability and trust, which counteracts pure price-based switching behaviour.

Bargaining Power of Suppliers

The bargaining power of suppliers is also moderate. Since Therap relies on technological infrastructure, service reliability and secure systems, it is likely to rely on credible outside vendors and service providers. That offers some influence to suppliers, but developing long-term business relationships with suppliers can help relieve that pressure.

Industry Rivalry

Industry rivalry exists, but Therap appears to have a good position in its niche. Its long experience, specialisation and good industry reputation help to compete well. At the same time, in a marketplace of trust, compliance readiness and quality of service, an established reputation is an important advantage.

2.7.2 SWOT Analysis

Strengths

Therap's major strengths are specialisation in the market, good reputation, strong software and long-term experience in the sector. The company also likes to be in the niche where expertise, trust and structured delivery of service are highly valued. Its compliance sensitive environment is also an added bonus to its credibility.

Weaknesses

The company operates in a specialized market and it might not have more extensive expansion opportunities, which is one of the weaknesses. Moreover, certain parts of the operations involve a high level of team coordination, which can lead to the development of high dependency on timely communications and follow-ups, as Therap has teams across various geographical locations.

Opportunities

Therap can further grow, as the digital documentation, healthcare information systems and process automation are growing in significance. The increasing need of stable and effective

online services platforms may offer additional opportunities to expand and improve service delivery.

Threats

Cybersecurity threats, changes in regulations, technological disruption, and competition in the healthcare technology industry are some of the major threats to Therap. As the company is dealing with sensitive information, any security threat, either outside or within the company, can pose a huge risk to the operations and image of the company.

2.8 Summary and Conclusions

According to the above analysis, Therap is a specialized healthcare SaaS firm and it is operating in a highly controlled environment. The leadership strategy, mode of operation, as well as the market focus of the company are all supportive of compliance-conscious way of working.

At the same time, the analysis of this report also shows that this type of environment comes with its own set of challenges. As the compliance requirements increase and the complexity of audits increases, it should be noted that the organization proceeds to balance operational efficiency and effective controls. This renders Therap a valid and realistic setting on which the dynamics of governance and compliance are explored under real-life organizational circumstances.

2.9 Recommendations/Implications

Looking at the organizational analysis, it is possible to identify some implications for the practical purposes. One, enhanced cross-functional coordination would minimize delays in places where one team depends on another. Second, increased automation in documentation and tracking should be applied more rigorously, which might lead to an increase in efficiency. Third, with the compliance requirements growing, the organization can gain an advantage by creating a greater visibility of process ownership and response timelines.

These recommendations are not significant modifications in the Therap organization, but enhancements that would be realistic in ensuring Therap sustains its discipline in its operations. Academically, it can also be analyzed that in order to gain a clear picture of the working of compliance and audit functions in the real sense, one should first comprehend the organization.

Chapter 3

Compliance and Audit Governance

3.1 Introduction

In regulated, technology-based organisations, compliance transcends the technical satisfaction of formal requirements written on paper. It goes hand in hand with governance, risk management, and performing tasks in a wide variety of teams. In this chapter, the role of the internal controls and audit practices as a governance mechanism in a healthcare SaaS setup is examined, especially in relation to Therap.

Since Therap is an organization that processes protected health-related information, it is under a collection of regulatory and assurance requirements, including the HIPAA framework and SOC 2 standards. Compliance to these comprehensive requirements is far beyond merely the presence of policies and procedures. It requires paperwork, coordination, follow-up, and constant review. For that reason, audit activities at Therap are closely linked to the organization's broader governance structure as opposed to being isolated, compliance events.

This chapter also focuses on how audit processes, risk tracking, documentation practices, and training-related controls contribute to compliance maturity. It also discusses some of the operational difficulties that arise when evidence has to be collected across teams and aligned with multiple frameworks at the same time.

3.1.1 Problem Statement

Healthcare SaaS organizations must adhere to multiple regulatory and assurance frameworks simultaneously. Managing overlapping requirements, coordinating evidence across departments, and ensuring that control is effective on a continuous basis add to the complexity of operations. The central problem addressed in this study is how internal controls and audit mechanisms can be structured to support effective IT governance while minimizing inefficiencies.

3.1.2 Objectives of the Study

This study aims to:

- Review the role of internal and external audits as a means of governance
- Analyse operational challenges in multi-framework compliance environments
- Evaluate the role of risk tracking and documentation discipline
- Identify opportunities for improving audit efficiency and compliance scalability

3.2 Literature Review

Information Technology Governance (ITG) is the structural foundation in which the organization ensures that the information systems meet strategic objectives, and manage risk and set structures of accountability (Weill & Ross, 2004). According to Weill and Ross (2004), IT governance refers to the decision rights and accountability framework that promotes desirable behaviour in the use of IT (Weill & Ross, 2004). In a regulated environment, governance is not about efficiency or performance, but it is, at a fundamental level, about risk control, transparency and regulatory compliance.

In healthcare SaaS organizations, there is a lot more to the complexity of governance because systems involve processing and storage of Protected Health Information (PHI). The HIPAA Security Rule provides the administrative, physical and technical safeguards that organizations must implement to protect electronic health information, according to the United States Department of Health & Human Services [HHS] (n.d.). These safeguards include risk analysis, workforce training, access controls, audit logging and contingency planning. Hence, compliance is not just policy documentation, it requires frequent monitoring, evidence of control implementation, and formal accountability structures.

Figure 3 - Internal and External Audits - Strengthening Governance

Internal audit functions act as assurance mechanisms in this governance ecosystem by assessing risk management, control effectiveness and governance processes (Institute of Internal Auditors [IIA], n.d.). The Institute of Internal Auditors also provides a definition of internal auditing as an independent and objective assurance activity intended to add value and enhance organization operations (Institute of Internal Auditors [IIA], n.d.). In technology-intensive organizations, internal audit goes beyond the financial controls and encompasses evaluation of the IT general controls, access management, change management, and vendor risk oversight. Research in the field of IT governance has indicated that organizations that have structured internal audit practices exhibit a higher level of control maturity and risk awareness.

External information security audit programs, such as SOC 2, strengthen the governance discipline even more. The Trust Services Criteria, as defined by the American Institute of Certified Public Accountants, highlight five principles of trust services: security, availability, processing integrity, confidentiality, and privacy. Unlike the checklist style of compliance, SOC 2 requires that organisations will be able to demonstrate the controls work effectively over time. Thus. the concept of compliance at a 'specific point in time' is replaced by the idea of 'continuous compliance'.

NIST guidance, in particular SP 800-53, offers a powerful resource of security and privacy control families that organizations can adopt to organize governance practices (National Institute of Standards and Technology [NIST], 2020). These control families provide for structured implementation of access control, configuration management and system maintenance practices (NIST, 2020). The significance of risk assessment processes and remediation plan tracking is also emphasised by NIST.

The concept of Plan of Action and Milestones or POA&M (used extensively in federal risk management frameworks) is a structured method of recording the weaknesses, specifying the steps to be taken to correct those weaknesses, and monitoring the progress. From the perspective of compliance and quality control, POA&M actually translates audit findings into measurable and structured improvement activities. Instead of seeing the findings as isolated issues, findings become part of a larger approach to risk management.

A major challenge that has been discussed in compliance literature is the overlap of multiple frameworks. Organizations subject to multiple regulatory standards may experience similar control objectives written in different terms. For instance, access control requirements under

HIPAA may be conceptually similar to other access control requirements under the SOC 2 or NIST frameworks. However, documentation expectations and presenting the evidence may be different. This leads to operational complexity with the calculation of mapping, documentation, and version control.

Studies in the field of IT governance maturity show that organizations move from being reactive in compliance to taking a proactive approach to governance, as they institutionalize documentation practices, automate tracking of evidence, and integrate risk monitoring into the routine of operations (De Haes & Van Grembergen, 2009). Continuous monitoring, structured change management, and recurring training programs add to this progression of maturity.

While there is existing literature on this topic that focuses on governance frameworks and compliance structures, they don't offer much context into the complexity of multi-framework environments in actual SaaS organizations. This study adds to this discussion by investigating the effects of documentation coordination, stakeholder interaction, and iterative remediation processes on the maturity of governance in practice.

In summary, the literature sets out a number of key principles of relevance to this study:

- IT governance involves defined accountability and decision-making.
- Audit functions are the governance assurance tools.
- Healthcare compliance requires constant monitoring and documentation discipline
- Multi-framework environments make the operation more complex.
- Risk Registers and Remediation Tracking help in improving the maturity of governance.

These theoretical foundations offer a framework for the analysis of how compliance and audit practices are implemented in practice at Therap.

3.3 Methodology

This study uses a qualitative methodology based on direct participation and observation of professionals. The analysis is based on my participation in compliance and audit functions during the November - April assessment period. Data sources were observations of governance meetings, reviews of non-confidential documentation and participation in evidence collection and validation processes.

The methodology involved process mapping of the audit lifecycle, documentation workflows analysis and thematic analysis of recurring operational challenges. Meetings with auditors and US-based counterparts also helped to gain insights into decision-making practices and stakeholder coordination. Due to confidentiality requirements, the study concentrates on process-level observations, not technical information about the systems or information about any specific client.

A qualitative approach was suitable for this study because compliance practices involve contextual processes, human coordination, and organizational decision-making that cannot be adequately summarized with quantitative metrics. While direct participant observation allowed insights into actual governance processes, document review allowed process verification. However, the study has some limitations because it relies on non-confidential data and lacks direct system-level analysis.

3.4 Findings and Analysis

Table 1 - Evidence Category and Examples

Evidence Category	**Examples**
Policy Documents	Security policy, access control policy
Training Records	Completion logs, reminder documentation
Access Reviews	User list validation outputs
Vendor Documents	SOC reports, vendor risk tier records
Change Management	Ticket approvals, release logs
Risk Register	POA&M tracking documentation

3.4.1 Audit Lifecycle

The audit lifecycle at Therap is based on a structured sequence, which incorporates governance, documentation and risk management practices. Preparation is initiated with a review of policies, inventories and access records internally based on anticipated audit requirements. This stage - called pre-audit - represents organizational learning from prior assessments and helps reduce the amount of reaction work when formal evidence requests are issued.

Requirement breakdown is an essential stage during which the audit requests are analysed and linked to internal documentation. Evidence collection then involves coordination across operations, development and management teams. Validation is done at the same time to ensure that it is accurate, relevant and traceable before submission.

Audit interviews assist in providing an extra check and auditors may examine both documents and operations understanding. Feedback given by the auditors at this stage typically results in the discovery of gaps or clarification requests. The findings are then tracked into the POA&M and become a process of continuous improvement.

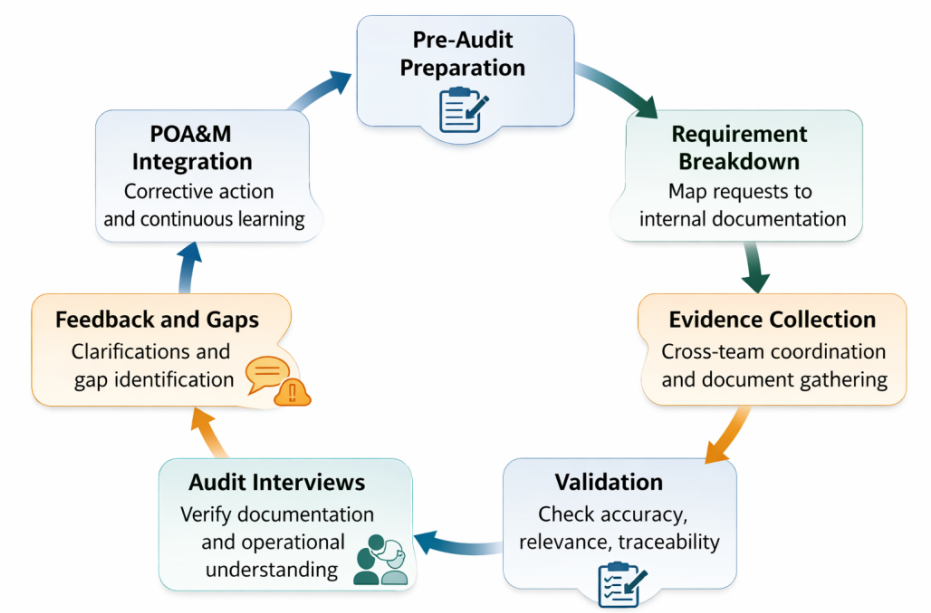

Figure 4 - External Audit Lifecycle at Therap

Within the aspect of governance, this lifecycle demonstrates the effectiveness with which the process of regulatory compliance is transformed into a learning process by the well-designed documentation and continuous feedback systems. Audit activities create accountability, knowledge and risk awareness among organizational units instead of periodic checks of control.

3.4.2 Risk Register (POA&M)

Risk management at Therap is supported by an organized POA&M process managed by the CISO. The register is reviewed periodically and shows results of both internal monitoring and external audits. The POA&M serves as a channel between Therap's operation and governance improvement by matching the gaps as indicated with remedial actions. The POA&M not only enhances the presence of the audit findings, but also ensures that compliance initiatives are not limited to documentation and actively address the risk.

3.4.3 Vendor Risk Management

Vendor risk management at Therap has a tier-based system where vendors are classified according to risk and critical levels. In the case of critical vendors, SOC 2 reports are collected and reviewed on a periodic basis to make sure that third-party relationships meet security expectations. This systematic method acknowledges that the responsibility of compliance is not limited to the boundaries of the organisation and they must ensure that they are on a perpetual basis monitoring external dependency.

3.4.4 Change Management

The change management process in Therap is highly integrated with the governance and formal approval and documented testing processes. The software releases are followed through the systematized ticketing systems that document the validation and the approval of the managers. Such documentation provides the auditors with the assurance that there is proper control and review of changes in the systems.

3.4.5 Training Governance

One of the most crucial elements that must be considered to guarantee compliance is training governance. Training campaigns on security awareness per month and training of new employees are also known to reinforce the knowledge of the employees on their security obligations. The evidence of the preparedness of the workforce during audits is these training records.

3.4.6 Key Obstacles and Root Causes

The main identified operational obstacles include:

Cross-Team dependency for evidence generation and validation: During the audit engagement period, auditors request numerous evidence based on the requirements of the audit framework. The evidence files are collected from almost all the teams of the company. Based on the domain of the control, the requests are forwarded to the appropriate team and communicated with them for collecting the correct evidence that satisfies the auditor's request. Often, the collected evidence is crosschecked and verified by senior management before submission. This causes a high cross-team dependency, affecting the audit process.

Delayed requirement clarification due to time zone differences: The Request for Information (RFI) list that includes all the audit requirements is discussed with the appropriate senior officials for guidance and clarification on how to proceed with the critical items from the list. As Therap is a multinational company, the officials and teams are often from different geographical locations. Due to this difference, the work hours and weekdays also differ, creating a delay in the overall evidence generation and submission process.

Manual mapping of evidence to requirements: As mentioned earlier, Therap gets audited against multiple frameworks and as a result, a few hundred of evidence requirements need to be processed, understood and mapped against the evidence we have in hand. This manual mapping of these regulatory requirements and the auditor's requests against the available data becomes a time intensive process.

These root causes add to the workload during audit cycles and present areas for improvement in structure. Such issues are the manifestation of the reality that compliance and quality control in fact, demand good coordination efficiency and effective communication.

3.4.7 Impact of Implemented Improvements

During the assessment period, a number of improvements led to better compliance execution:

Centralized organization-wide training record improved clarity of audit evidence: During my internship equivalent time, I worked on and maintained a centralized record of all types of organization-wide training for 2025. This gave us a better visibility into the available evidence for the Awareness and Training control family. As a result, the awareness and training related evidence requests were possible to address at the very beginning of the audits.

Vendor matrix optimization improved vendor risk management: The third-party vendors list maintained at the organization is a single source of truth for all the vendor related information. It is a broad spreadsheet filled with information that is required to be submitted to the auditors as evidence. Although the vendor matrix was in good shape, but it lacked the appropriate settings and formatting that allow easier and quick extraction of vendor-related audit evidence. I worked on it and made improvements which led to quicker submission of vendor risk management-related evidence requests.

Closure of administrative findings regarding passwords policy compliance: During the audit engagements, one of the potential administrative findings reported by the auditor was regarding the password policy compliance. Therap's policy included statements regarding the password length and complexity that were in contradiction to with what we had already implemented in various systems. I worked on updating the policy and submitting it within the audit window so that this finding does not appear in the audit reports.

These are actions that show incremental maturity in the compliance function of governance.

3.5 Recommendations

Table 2 - Recommendations by Priority

Priority	**Recommendation**	**Expected Impact**
High	Structured evidence framework	Reduces audit delays
High	Pre-audit exercises	Improves readiness
Medium	AI requirement analysis	Increases efficiency
Medium	Compliance dashboard	Improves visibility into governance
Long-term	Regulatory expansion planning	Supports scalability

According to the outcomes of this research, several feasible measures could be implemented to make the audit ready and reduce unwarranted delays within the process. These suggestions rely on difficulties found during the evidence gathering process, review and mapping of documentation. The purpose of these suggestions is not to redesign the entire compliance

function, but to reinforce those components of the process that cause the repeated friction of audit cycles.

Structured Evidence Management Framework

Among the most regular operational issues that were noticed was the issue of manual evidence coordination and sometimes version discrepancies. To overcome this, a structured evidence management framework needs to be developed. This would include:

- A well-defined evidence ownership designation.
- Version control protocols
- Control family/framework centralized indexing.

This would eliminate duplication, enhance traceability and less time will be wasted in clarification on submissions during the audit cycle.

AI-Assisted Requirement Interpretation Support

Multi-framework requirement mapping can be a time-consuming activity due to the differences in how similar control expectations are written in audit frameworks. An intelligent support tool, which is not that complex and relies on AI, may be beneficial to find probable evidence matches and minimize the volume of manual search required during the preliminary stage. This would not be a substitute for the human review, but it might streamline the initial stage of the requirement interpretation process.

Pre-Audit Exercises

Even though preparedness comes from historical audit experience, well-organized pre-audit simulations may formalize preparations too. An internal pre-audit light review cycle would:

- Find out the gaps in documentation.
- Check the traceability of evidence
- Assess response timelines from various teams.
- Improve the coordination of the parties involved in audit

Such simulations would bolster preparedness without adding a lot of extra work.

Defined Evidence Response Timeline

Establishment of informal response time expectations to audit-related requests would help improve coordination. Distinct deadlines between high-priority and regular evidence requests would boost time efficiency and ease the evidence submission process.

Integrated Compliance Dashboard

Therap may consider developing a compliance dashboard in the long run that is linked to:

- POA&M tracking
- Tracking of training completion.
- Vendor review status
- Access review cycles
- Approvals of change management.

The leadership would be able to get real-time information on governance posture using a centralized dashboard.

Long-Term Regulatory Expansion Strategy

Given that Therap is already familiar with HIPAA, SOC 2, and other regulatory models, the organization will be ready to participate in more advanced federal audits when it is strategically suitable. Nevertheless, this would require the increase in the process, improved documentation, and further automation. Strategic planning of development would ensure that the resources are not overexploited.

Conclusion

To sum up, the current study indicates that compliance and audit practices at Therap are combined governance functions beyond regulatory compliance. This company maintains a form of mature compliance stance in a complicated regulatory environment through systematic documentation, regular review processes, and shared decision-making. The findings bring some light to the capabilities and implementation challenges of multi-framework governance and give few recommendations on how they might be adjusted to make them more efficient and scalable. Altogether, the experience was useful as it helped to understand how IT governance principles are applied to the practical healthcare-software-as-a-service operations.

References

1. American Institute of Certified Public Accountants. (n.d.). *SOC 2® - SOC for service organizations: Trust services criteria*. https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
2. Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control - Integrated framework*. COSO. https://www.coso.org
3. Institute of Internal Auditors. (n.d.). *Definition of internal auditing*. https://www.theiia.org/en/about-us/about-internal-auditing/
4. National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (SP 800-30 Rev. 1)*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
5. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
6. U.S. Department of Health & Human Services. (n.d.). *HIPAA security rule*. https://www.hhs.gov/hipaa/for-professionals/security/index.html
7. Tao, T., Chen, Y., & Zhang, L. (2023). IT governance and IT controls: Analysis from an internal auditing perspective. *International Journal of Accounting Information Systems, 52*, Article 100663. https://doi.org/10.1016/j.accinf.2023.100663
8. Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.
9. ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA. https://www.isaca.org/resources/cobit
10. ISO. (n.d.). *ISO/IEC 27001 information security management*. https://www.iso.org/isoiec-27001-information-security.html
11. De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management.*
12. Whitman, M., & Mattord, H. (2021). *Principles of information security.* Cengage Learning.

Appendix A

Internship Proposal

1. Background and Problem Statement

Software-as-a-Service (SaaS) organizations that operate within the healthcare sector have huge responsibility in terms of ensuring sensitive information is protected and that they are compliant with regulatory requirements. Due to the nature of protected health information (PHI) that is handled, such organizations must comply with multiple regulatory and assurance frameworks such as HIPAA, SOC 2, etc. Such frameworks demand robust information security controls, ongoing monitoring and frequent internal and external audits.

Therap is a US based SaaS company that offers electronic health records (EHR) solutions to government and private organizations all across the globe serving people with intellectual and developmental disabilities. To support regulatory and security requirements, Therap has a dedicated Compliance and Quality Control (CQC) function that is responsible for internal audits, external audit engagements, quality assurance activities, and information security monitoring.

While compliance and audit activities are of extreme importance to the sustainability of the organizations, there is also a consequent complexity in operations. Managing multiple audit frameworks, coordinating the collection of evidence, the management of security awareness training, the monitoring of third-party software risks and maintaining continuous compliance require structured processes and effective information technology governance. From an Information Technology Management (ITM) perspective, knowing how these controls are designed, managed and improved is essential.

The central problem to be addressed in this report is how internal controls and audit mechanisms are used as part of the information technology (IT) governance to support information security, regulatory compliance, and risk management in a healthcare software-as-a-service (SaaS).

2. Objectives of the Study

The main objectives of this project are:

1. To discuss the role of internal and external audits in information security and regulatory compliance in a healthcare SaaS environment
2. To analyse compliance and quality control practices as mechanisms of information technology governance.
3. To examine the challenges associated with dealing with multiple compliance frameworks for a SaaS organization.
4. To suggest some practical recommendations to enhance efficiency of audits and compliance management from an ITM point of view.

3. Background Information and Preliminary Literature Review

Existing studies on this area of healthcare information systems emphasize that IT governance plays an important role of aligning information systems with organizational objectives and of managing risk and regulatory requirements. Studies on IT governance further mentions that internal controls, audit processes and compliance frameworks are important tools for ensuring accountability, security and operational transparency in technology driven organizations.

Research in the area also indicates that regulatory compliance frameworks like HIPAA demand on-going monitoring, access control management, audit logging and vendor risk management. These requirements can be addressed in a SaaS organization with a combination of internal audits, third-party risk assessments and external audit reports such as SOC 2 Type II.

Recent studies have also indicated that companies that have structured audit and compliance functions are better positioned to handle the information security risks and respond to change in regulations. Audits and compliance activities should not only be a mechanism of controls, but also a tool for continuous improvement and control of the processes and the maturity of governance.

4. Preliminary Methodology

The report will be of qualitative approach. Data and insights will be collected through:

- Direct participation and observation in Compliance and Quality Control function

- Review of non-confidential internal audit processes and documentation
- Process mapping of internal and external audits
- Analytical evaluation using established IT governance and information security concepts

The study will not include access to source code, client specific data or sensitive configurations of systems.

5. Significance of the Study

This research is important because it presents the practical use of Information Technology Management concepts in a regulated SaaS environment. It offers an understanding of the role of compliance and audit mechanisms in supporting IT governance, risk management and information security. The study will also provide useful suggestions that can be used to improve compliance efficiency and governance practices in similar organizations.