IE UNIVERSIDAD

TESIS DOCTORAL

Gestión del Cumplimiento y Gestión del Riesgo en la Industria del Cuidado de la Salud

Darwin Michael Rivera

SEGOVIA, 2025

IE UNIVERSIDAD

TESIS DOCTORAL

Gestión del Cumplimiento y Gestión del Riesgo en la Industria del Cuidado de la Salud

Darwin Michael Rivera

Supervisor de Tesis Doctoral: Dr. Alvaro Arenas Sarmiento

IE UNIVERSITY

DOCTORAL DISSERTATION

Managing Compliance and Risk Management in Health Care Settings

Darwin Michael Rivera

SEGOVIA, 2025

IE UNIVERSITY

DOCTORAL DISSERTATION

Managing Compliance and Risk Management in Health Care Settings

Darwin Michael Rivera

Doctoral Thesis Advisor: Alvaro Arenas Sarmiento

Abstract

This dissertation investigates how organizations operating in highly regulated environments manage the concurrent demands of regulatory compliance and information security risk management. Drawing on Oliver's (1991) theory of strategic responses to institutional pressures, the study examines how organizations respond to overlapping external and internal pressures—particularly under resource constraints.

Guided by two central research questions—(1) How do organizations manage compliance and risk management concurrently? and (2) How do they allocate resources to maximize compliance while minimizing security risks?—the study adopts an integrative approach that bridges the traditionally siloed domains of compliance, risk management, and information security.

The research employs a two-part empirical design: a content analysis of compliance policies from 30 healthcare organizations and a case study of a children's hospital implementing a DEA-mandated Electronic Prescription for Controlled Substances (EPCS) system. The findings contribute to theory by identifying a previously undocumented tactic—prioritization—that organizations use to reconcile competing institutional demands. Another theoretical contribution is the development of a process model and a set of propositions that illustrate how organizations operating in highly regulated environments navigate the dual imperatives of compliance and risk management.

By linking policy artifacts with real-world organizational behavior, this dissertation offers both scholarly and practical insights into how organizations

navigate institutional complexity, enhance compliance maturity, and align security and regulatory needs.

Abstracto (Spanish)

Esta tesis investiga cómo las organizaciones que operan en entornos altamente regulados gestionan las demandas concurrentes de cumplimiento normativo y gestión de riesgos de seguridad de la información. Basándose en la teoría de Oliver (1991) sobre las respuestas estratégicas a las presiones institucionales, el estudio examina cómo las organizaciones responden a las presiones externas e internas superpuestas, particularmente bajo limitaciones de recursos.

Guiado por dos preguntas centrales de investigación: (1) ¿Cómo gestionan las organizaciones el cumplimiento y la gestión de riesgos al mismo tiempo? y (2) ¿Cómo asignan recursos para maximizar el cumplimiento y minimizar los riesgos de seguridad?: el estudio adopta un enfoque integrador que tiende un puente entre los dominios tradicionalmente aislados de cumplimiento, gestión de riesgos y seguridad de la información.

La investigación emplea un diseño empírico de dos partes: un análisis de contenido de las políticas de cumplimiento de 30 organizaciones de atención médica y un estudio de caso de un hospital infantil que implementa un sistema de Receta Electrónica para Sustancias Controladas (EPCS) exigido por la DEA. Los hallazgos contribuyen a la teoría al identificar una táctica previamente no documentada, la priorización, que las organizaciones utilizan para reconciliar las demandas institucionales que compiten entre sí. Otra contribución teórica es el desarrollo de un modelo de proceso y un conjunto de proposiciones que ilustran cómo las organizaciones que operan en entornos altamente regulados navegan por los imperativos duales del cumplimiento y la gestión de riesgos.

Al vincular los artefactos de políticas con el comportamiento organizacional del mundo real, esta tesis ofrece perspectivas académicas y prácticas sobre cómo las organizaciones navegan por la complejidad institucional, mejoran la madurez del cumplimiento y alinean las necesidades regulatorias y de seguridad.

Executive outline

This dissertation examines how organizations manage the dual demands of regulatory compliance and information security risk management—two intertwined yet distinct functions that often draw on the same personnel and systems. While compliance focuses on meeting externally defined regulations, risk management addresses internal threats and uncertainties. The research explores how organizations strategically and tactically respond to these overlapping pressures, especially when resource constraints force prioritization between the two.

Drawing on Oliver's (1991) theory of organizational responses to institutional pressures, this study investigates how organizations act under simultaneous internal and external demands. The study is guided by two central research questions:

1. How do organizations manage compliance and risk management concurrently?
2. How do they allocate resources to maximize compliance while minimizing security risks?

The existing literature treats compliance, risk management, and information security in isolation, resulting in a fragmented understanding. This study adopts an integrative approach, combining insights from all three domains to explore how organizations harmonize their activities to achieve regulatory compliance and reduce their risk footprint, all while optimizing resource utilization.

The dissertation follows a multi-method approach. First, it applies content analysis to analyze the features and components of compliance policy documents from 30 healthcare organizations to assess how organizations formally communicate their compliance posture. Second, it presents a case study of a children's hospital implementing a DEA-mandated Electronic Prescription for Controlled Substances (EPCS) system, offering rich insight into real-world decision-making around compliance and risk. Data was collected through 11 interviews with stakeholders ranging from front-line analysts to C-suite executives. Thematic coding was applied using two frameworks: one based on the research questions and another grounded in Oliver's strategic and tactical response model.

The study makes several key contributions. First, it identifies a previously undocumented tactic – prioritization - used by organizations to reconcile competing compliance and risk management needs, extending Oliver's original typology. Additionally, the study develops a process model and a set of propositions that illustrate how organizations operating in highly regulated environments navigate the dual imperatives of compliance and risk management.

Ultimately, this dissertation fills a critical gap in the literature by offering empirical insights into how organizations structure compliance documentation, make operational decisions, and strategically respond to the intersecting challenges of compliance and risk management in real-world settings.

The dissertation is structured in three chapters. The first chapter reviews literature from three key domains: compliance, information security, and strategic organizational responses to institutional pressures. It uses

Oliver's (1991) framework as a theoretical foundation to explore how organizations behave and respond procedurally to compliance and risk challenges in interconnected environments.

The second chapter presents an empirical analysis of compliance documents within healthcare organizations. It examines how compliance policies serve as communication tools that articulate the organization's intent and strategic/tactical responses to regulatory and industry requirements. This chapter provides a deeper understanding of how formal policy structures reflect and support an organization's compliance posture.

The third chapter features a case study of a children's hospital implementing a DEA-mandated Electronic Prescriptions for Controlled Substances (EPCS) solution. It explores how the organization navigated the complexities of achieving compliance while balancing internal risk management priorities. The dissertation concludes with a discussion of theoretical and practical implications, limitations, and recommendations for future research.

Keywords: Compliance, Information Systems, Security, Risk Management, regulated environments, governance, strategic responses to institutional processes, healthcare

Acknowledgments

The journey that brought me to IE Business School and IE University has been a long and challenging one. Thankfully, along the way, I have been blessed by the presence of extraordinary people doing extraordinary things in my life. I am grateful for their support and their contributions to making this dissertation project a reality. First, I would like to thank God, Allah, Yahweh, the universe, and all the beautiful energy that has accompanied me on this journey, allowing me to achieve this goal.

I am grateful to my family for their unwavering support and their belief in me. I dedicate this dissertation to the memory of my mother, Margarita Ortiz Rivera, and my grandmother, Maria Rivera Ofray, who, from heaven, watched over me as I completed this task. I also dedicate it to my daughter Arianna Isabelle Rivera-Ramos to exemplify that pursuing your dreams does not expire and that giving up is not an option. I would like to thank Dr. Alvaro Arenas Sarmiento for his mentorship and guidance, and for never giving up on me when I was ready to throw in the towel. I would also like to thank Dr. Laura Maguire for supporting me and being my guardian angel in so many ways, making sure that I made it to the finish line, and helping make the program feel like a family. Thanks to the DBA program staff throughout the years for their invaluable help and assistance. Thanks, Dr. Mikko Ketokivi, for helping me clarify my theoretical lens. I want to thank the Doctoral Committee for their support and understanding of the challenges I faced over the years, and for providing me with the opportunity to complete my journey at IE. I want to thank my proposal committee, comprising Dr. Ramiro Montealegre, Dr. Patricia Gabaldon, Dr. Jose Esteves, and Dr. Sarah Lee, for their invaluable feedback.

I want to thank my IE DBA cohort for their continued friendship, inspiration, and support. When I grow up, I want to be just like you. Especially in alphabetical order (I got no favorites ☺): Dr. Horacio Arredondo, Dr. Henry Bradford, Dr. Ahmad Hijazi, Mr. Allan Lopez, Dr. Oscar Moreno, and finally, Dr. Periklis Thivaios. I would also like to thank the reviewers of my work throughout this experience, who have helped improve it over the years, as well as those who have contributed their time to making this research project possible. I have grown tremendously at IE, personally, academically, and professionally. The road was long and hard; there were personal challenges and heavy loss, but I am glad that I was able to overcome and achieve this important milestone. I could not think of a better place to have this experience. When I started my journey, I referred to myself as a 'Warrior MBA' in my application essay; today, I can say that I have become the Warrior DBA through IE Business School and IE University. Thank you, and my infinite blessings fall upon you and all those you love.

Table of Contents

Figures

Introduction

Organizations must manage the requirements of compliance with regulations with those requirements related to risk. This threading the needle between compliance and risk management presents a dichotomy akin to two sides of the same coin. On the one hand, understanding how an organization manages its resources to address compliance and risk requirements can provide practitioners with valuable insights on how to address those challenges in their own organizations. For compliance or risk management requirements, the same staff and system(s) are often impacted by these requirements. Some may think that performing information systems compliance tasks is equivalent to performing risk management. Although compliance carries a risk component, compliance, and risk management differ in the organizational context. Compliance and information security risk management draws on complementary but different sets of skills. When addressing risk, you identify and quantify potential threats to the organization, devising and implementing controls to mitigate the impact of those risks. Additionally, the organization must prepare for those “unknown unknowns” to build a resilient organization. Similarly, as a composer creates a melody and a cadence on a blank sheet of music and selects the instruments to write music for, a compliance or risk manager gathers compliance and risk information and builds a set of controls to help mitigate the identified risks and compliance requirements applicable to the organization and its context. An organization's risk management process helps in understanding its risk environment and determining whether to implement the recommended controls, considering whether the risk falls within the organization's risk appetite and can be accepted. On the other hand, compliance comes with its own “sheet of music,” where a regulation’s requirements provide the melody, cadence, and instrument parts,

leaving only the approach to interpreting the piece. Requirements are established by regulators and interpreted by those implementing the regulations, as well as internal and external audit staff who examine compliance with these established requirements. Organizations analyzing regulations and identifying and defining the controls that will address the rule within the organizational context hinges on interpreting the required controls by the organization. To continue the musical analogy, the compliance practitioner interprets this sheet of music the same way a musician plays a sheet of music in front of them with their instrument.

The other side of the coin examines how, according to theory, an organization responds to the institutional pressures resulting from internal resource pressures and external institutional pressures. Thus, the research question is: How does an organization manage compliance and risk? Taking it a step further, what strategic and tactical responses does the organization employ to manage compliance and risk?

The aims of this research open some exciting lines of further inquiry. What strategies or tactics do organizations choose in response to their operational context? How does the organization handle conflict situations where compliance and risk requirements compete for the same resources? The strategies or tactics that organizations choose to employ may provide insight into how they respond to compliance and risk management requirements, enabling them to achieve and maintain compliance while managing risk. This research project aims to pull back the curtain on the black box and explore the mechanics of the process by which organizations leverage strategic and tactical responses, considering the potential for competing organizational pressures. Compliance and risk management are day-to-day realities that affect organizations (Pascarella et al., 2021; Wu & van Rooij, 2021).

My purpose is to address a gap in the literature by providing a theoretical contribution regarding the foundational documents of compliance and the actual decision-making process and strategical responses within organizations. The organizational environment where compliance and risk management requirements compete with each other results in resource and operational challenges when both impact the same systems or resources.

- How does the organization manage compliance and risk management?
- How do organizations manage resource assignments, maximizing compliance while reducing security risk?

Extant literature approaches compliance, risk management, and information security independently. The resulting siloed approach to these topics leaves an opening to explore how organizations can combine information security, risk management, and compliance activities. When combined, information security, risk management, and compliance activities enable the organization to achieve a reduced risk footprint and compliance with applicable regulations (e.g., GDPR, HIPAA) or business and industry requirements (e.g., PCI-DSS, FINRA), while maximizing resource utilization.

To study the research questions, I have taken an integrative approach, utilizing research from three streams of literature: compliance, risk management, and information security. Theoretically, I will explore how the organization responds to institutional pressures through strategic and tactical responses. (Oliver, 1991).

Institutional complexity and pluralism present organizations with numerous pressures and trade-offs daily. Institutional complexity examines how an organization responds to conflicting requirements from multiple fronts. An organization must

choose a response to external pressure(s) using an array of strategies and tactics that guide how it acts upon the requirements of said pressures.

Oliver (1991) highlights the strategic and tactical responses of the organization to these institutional pressures, defining the “how” in the way the organization responds to them. What is missing is insight into how an organization responds to these organizational pressures and what strategies and tactics are most favored in regulated environments, particularly in the context of information systems compliance and risk management activities.

Extant research has provided some examples of the influence of external pressures on individual actors (Arnold et al., 2007; Barton et al., 2016). This opens up opportunities to explore the organizational processes that address the operational requirements of information systems security and compliance. Given the constraints on organizational resources, organizations must be creative in addressing their specific requirements.

Organizations that manage compliance requirements while effectively managing their own information systems security risks can maximize resource utilization, reduce their risk footprint, and achieve compliance with regulatory requirements. My dissertation first examines how a sample of organizations establish and communicate their approach to addressing compliance requirements through their compliance documents. The examination of compliance documents is conducted under the context of the features and components of compliance policies. The United States Sentencing Commission provides primary guidance for effective compliance programs in the United States (*2018 Chapter 8 | United States Sentencing Commission*, n.d.). The Association of Corporate Counsel and Kusserow

provides further refinement of the requirements established by the Commission (Carboni, 2022; Kusserow, 2013, 2014).

This is followed by an examination of how an organization can effectively manage compliance and risk management. The United States Drug Enforcement Administration's Electronic Prescription for Controlled Substances compliance information system solution implementation at a children's hospital system is used to examine compliance requirements and explore how the organization addresses them. Eleven interviews were conducted. The informants included front-line analysts and administrators as well as middle management, senior technical resources, and executives like the Chief Information Officer and the Chief Information Security officer. The interviews were transcribed and coded using thematic coding based on two coding guides. The first coding guide used several research questions aimed at uncovering insights on the process(es) the organization leveraged to balance information security risk management and compliance. The other coding guide is based on Oliver's strategic and tactical responses (Oliver, 1991). The results of the study yielded a theoretical contribution by identifying a new tactic called prioritization, which is not proposed by Oliver (1991) and has not been employed directly in the context of our study. The insights of the direct answers to research questions resulted in the creation of a model that captures how the organization managed the process to balance information security risk management and compliance. This model can be used by scholars and practitioners to build understanding of how an organization can optimize resource allocation to balance the requirements of information security risk management and compliance.

Dissertation Structure

The first chapter reviews the existing literature, divided into three streams of literature: current research on compliance, information security, and strategic responses to institutional processes. Each topic will be examined, and the existing literature will be presented to assess the current state of the art. Oliver's (Oliver, 1991) Strategic Responses to Institutional Processes provides a theoretical lens that offers a foundation for examining the research topic. In this first section, compliance is examined from its behavioral aspects as well as the procedural aspect of it in the context of the organization. Information security is introduced as an interrelated topic since the interconnectedness of compliance and information security is engrained in the modern organization's context and operation.

The second chapter of the dissertation is an empirical examination of compliance-related documents in healthcare organizations. In this context, compliance documents serve as foundational controls for a compliance program. This empirical analysis aims to uncover features and components of compliance policies and their use as a communication tool for internal and external stakeholders regarding the organization's aims in pursuit of compliance with regulatory/industry requirements. The compliance policy becomes an important communication tool of the organization's intent when addressing the requirements imposed on them by the regulatory environment, both government and industry-driven regulations. An examination of compliance policy features and components will be conducted to further our understanding of the response that the organization is communicating and what it will take to approach its response. Central to this exercise is connecting what the organization communicates as the aims of its compliance program and the strategic and tactical responses defined in the policy document features and

components. This chapter provides the policy component of this dissertation. In this context, the policy becomes a written statement of what the organization is committed to implementing in response to the compliance requirements imposed on them. The organization's compliance policy becomes what the organization is saying that it will do and how it plans to do it.

The third chapter of the dissertation presents a case study of a Children's hospital and how it approaches compliance and information security risk with a government mandate. The case study follows the implementation of a multi-factor authentication and credential solution to achieve compliance with the Drug Enforcement Administration Electronic Prescriptions for Controlled Substances (DEA-EPCS) and address identified risk management requirements. In this chapter, the theoretical and practical implications of compliance are explored as an interplay of the different areas of the organization come together to implement a requirement for a compliance activity while at the same time dealing with the tradeoffs required to balance other operational needs like risk management activities. This is followed by an overall discussion of the results and their theoretical and practical implications. An overall conclusion examines the insights derived, research limitations, and next steps.

Page intentionally left blank.

Introducción (Spanish)

Las organizaciones deben gestionar los requisitos de cumplimiento de la normativa con aquellos requisitos relacionados con el riesgo. Este enhebrado de la aguja entre el cumplimiento y la gestión de riesgos presenta una dicotomía similar a dos caras de la misma moneda. Por un lado, comprender cómo una organización administra sus recursos para abordar los requisitos de cumplimiento y riesgo puede proporcionar a los profesionales información valiosa sobre cómo abordar esos desafíos en sus propias organizaciones. En el caso de los requisitos de cumplimiento o gestión de riesgos, estos requisitos suelen afectar al mismo personal y sistemas. Algunos pueden pensar que realizar tareas de cumplimiento de sistemas de información es equivalente a realizar una gestión de riesgos. Aunque el cumplimiento conlleva un componente de riesgo, el cumplimiento y la gestión de riesgos difieren en el contexto de la organización. El cumplimiento y la gestión de riesgos de seguridad de la información se basan en conjuntos de habilidades complementarias pero diferentes. Al abordar el riesgo, se identifican y cuantifican las amenazas potenciales para la organización, ideando e implementando controles para mitigar el impacto de esos riesgos. Además, la organización debe prepararse para esas "incógnitas desconocidas" para construir una organización resiliente. Del mismo modo, al igual que un compositor crea una melodía y una cadencia en una partitura en blanco y selecciona los instrumentos para los que escribir la música, un administrador de cumplimiento o de riesgos recopila información de cumplimiento y riesgos y crea un conjunto de controles para ayudar a mitigar los riesgos identificados y los requisitos de cumplimiento aplicables a la organización y su contexto. El proceso de gestion de riesgos de una organizacion ayuda a comprender su entorno de riesgo y determinar si se deben implementar los controles

recomendados, considerando si el riesgo cae dentro del apetito de riesgo de la organizacion y puede ser aceptado. Por otro lado, el cumplimiento viene con su propia "partitura", donde los requisitos de una regulación proporcionan la melodía, la cadencia y las partes del instrumento, dejando solo el enfoque para interpretar la pieza. Los requisitos son establecidos por los reguladores e interpretados por quienes implementan las regulaciones, así como por el personal de auditoría interna y externa que examina el cumplimiento de estos requisitos establecidos. Las organizaciones que analizan las regulaciones e identifican y definen los controles que abordarán la regla dentro del contexto organizacional dependen de la interpretación de los controles requeridos por la organización. Para continuar con la analogía musical, el profesional de cumplimiento interpreta esta partitura de la misma manera que un músico toca una partitura frente a él con su instrumento.

La otra cara de la moneda examina cómo, según la teoría, una organización responde a las presiones institucionales resultantes de las presiones internas de recursos y las presiones institucionales externas. Por lo tanto, la pregunta de investigación es: ¿Cómo gestiona una organización el cumplimiento y el riesgo? Yendo un paso más allá, ¿qué respuestas estratégicas y tácticas emplea la organización para gestionar el cumplimiento y el riesgo?

Los objetivos de esta investigación abren algunas líneas de investigación interesantes. ¿Qué estrategias o tácticas eligen las organizaciones en respuesta a su contexto operativo? ¿Cómo maneja la organización las situaciones de conflicto en las que los requisitos de cumplimiento y riesgo compiten por los mismos recursos? Las estrategias o tácticas que las organizaciones eligen emplear pueden proporcionar información sobre cómo responden a los requisitos de cumplimiento y gestión de riesgos, lo que les permite lograr y mantener el cumplimiento mientras

administran el riesgo. Este proyecto de investigación tiene como objetivo abrir el telón de la caja negra y explorar la mecánica del proceso mediante el cual las organizaciones aprovechan las respuestas estratégicas y tácticas, considerando el potencial de presiones organizacionales competitivas. El cumplimiento y la gestión de riesgos son realidades del día a día que afectan a las organizaciones. Mi propósito es abordar un vacío en la literatura proporcionando una contribución teórica sobre los documentos fundamentales del cumplimiento y el proceso real de toma de decisiones y respuestas estratégicas dentro de las organizaciones. El entorno organizacional en el que los requisitos de cumplimiento y gestión de riesgos compiten entre sí da lugar a desafíos operativos y de recursos cuando ambos afectan a los mismos sistemas o recursos.(Pascarella et al., 2021; Wu y van Rooij, 2021)

- ¿Cómo gestiona la organización el cumplimiento y la gestión de riesgos?
- ¿Cómo gestionan las organizaciones las asignaciones de recursos, maximizando el cumplimiento y reduciendo el riesgo de seguridad?

La literatura existente aborda el cumplimiento, la gestión de riesgos y la seguridad de la información de forma independiente. El enfoque aislado resultante de estos temas deja una apertura para explorar cómo las organizaciones pueden combinar la seguridad de la información, la gestión de riesgos y las actividades de cumplimiento. Cuando se combinan, las actividades de seguridad de la información, gestión de riesgos y cumplimiento permiten a la organización lograr una huella de riesgo reducida y el cumplimiento de las regulaciones aplicables (por ejemplo, GDPR, HIPAA) o los requisitos comerciales y de la industria (por ejemplo, PCI-DSS, FINRA), al tiempo que maximiza la utilización de recursos.

Para estudiar las preguntas de investigación, he adoptado un enfoque integrador, utilizando la investigación de tres corrientes de literatura: cumplimiento, gestión de riesgos y seguridad de la información. Teóricamente, exploraré cómo la organización responde a las presiones institucionales a través de respuestas estratégicas y tácticas. .(Oliver, 1991)

La complejidad institucional y el pluralismo plantean a las organizaciones numerosas presiones y compensaciones a diario. La complejidad institucional examina cómo una organización responde a requisitos contradictorios desde múltiples frentes. Una organización debe elegir una respuesta a la(s) presión(es) externa(s) utilizando una serie de estrategias y tácticas que guíen la forma en que actúa sobre los requisitos de dichas presiones.

Oliver (1991) destaca las respuestas estratégicas y tácticas de la organización a estas presiones institucionales, definiendo el "cómo" en la forma en que la organización responde a ellas. Lo que falta es una visión de cómo una organización responde a estas presiones organizacionales y qué estrategias y tácticas son las más favorecidas en entornos regulados, particularmente en el contexto de las actividades de cumplimiento de los sistemas de información y gestión de riesgos.

Las investigaciones existentes han proporcionado algunos ejemplos de la influencia de las presiones externas en los actores individuales. Esto abre oportunidades para explorar los procesos organizacionales que abordan los requisitos operativos de seguridad y cumplimiento de los sistemas de información. Dadas las limitaciones de los recursos de la organización, las organizaciones deben ser creativas a la hora de abordar sus requisitos específicos. (Arnold et al., 2007; Barton et al., 2016)

Las organizaciones que gestionan los requisitos de cumplimiento al tiempo que gestionan eficazmente sus propios riesgos de seguridad de los sistemas de información pueden maximizar la utilización de los recursos, reducir su huella de riesgo y lograr el cumplimiento de los requisitos normativos. Mi tesis examina primero cómo una muestra de organizaciones establece y comunica su enfoque para abordar los requisitos de cumplimiento a través de sus documentos de cumplimiento. El examen de los documentos de cumplimiento se lleva a cabo en el contexto de las características y componentes de las políticas de cumplimiento. La Comisión de Sentencias de los Estados Unidos proporciona orientación primaria para programas de cumplimiento efectivos en los Estados Unidos. (2018 Capítulo 8 | Comisión de Sentencias de los Estados Unidos , s.f.)La Asociación de Abogados Corporativos y Kusserow proporciona un mayor refinamiento de los requisitos establecidos por la Comisión (Carboni, 2022; Kusserow, 2013, 2014).

A esto le sigue un examen de cómo una organización puede gestionar eficazmente el cumplimiento y la gestión de riesgos. La implementación de la solución del sistema de información de cumplimiento de recetas electrónicas para sustancias controladas de la Administración para el Control de Drogas de los Estados Unidos (DEA, por sus siglas en inglés) en un sistema hospitalario infantil se utiliza para examinar los requisitos de cumplimiento y explorar cómo la organización los aborda. Se realizaron once entrevistas. Los informantes incluían analistas y administradores de primera línea, así como mandos intermedios, recursos técnicos superiores y ejecutivos como el director de información y el director de seguridad de la información. Las entrevistas fueron transcritas y codificadas mediante codificación temática basada en dos guías de codificación. La primera guía de codificación utilizó varias preguntas de investigación destinadas a descubrir información sobre los

procesos que la organización aprovechó para equilibrar la seguridad de la información, la gestión de riesgos y el cumplimiento. La otra guía de codificación se basa en las respuestas estratégicas y tácticas de Oliver (Oliver, 1991). Los resultados del estudio arrojaron un aporte teórico al identificar una nueva táctica llamada priorización, la cual no es propuesta por Oliver (1991) y no ha sido empleada directamente en el contexto de nuestro estudio. Los conocimientos de las respuestas directas a las preguntas de investigación dieron como resultado la creación de un modelo que captura cómo la organización gestionó el proceso para equilibrar la gestión de riesgos de seguridad de la información y el cumplimiento. Este modelo puede ser utilizado por académicos y profesionales para comprender cómo una organización puede optimizar la asignación de recursos para equilibrar los requisitos de la gestión de riesgos de seguridad de la información y el cumplimiento.

Estructura de la disertación

En el primer capítulo se revisa la literatura existente, dividida en tres corrientes de literatura: la investigación actual sobre cumplimiento, seguridad de la información y respuestas estratégicas a los procesos institucionales. Se examinará cada tema y se presentará la literatura existente para evaluar el estado actual del arte. El libro de Oliver (Oliver, 1991) Strategic Responses to Institutional Processes proporciona una lente teórica que ofrece una base para examinar el tema de investigación. En este primer apartado se examina el compliance desde sus aspectos comportamentales así como el aspecto procedimental del mismo en el contexto de la organización. La seguridad de la información se presenta como un tema interrelacionado, ya que la interconexión del cumplimiento y la seguridad de la

información está arraigada en el contexto y el funcionamiento de la organización moderna.

El segundo capítulo de la tesis es un examen empírico de los documentos relacionados con el cumplimiento en las organizaciones sanitarias. En este contexto, los documentos de cumplimiento sirven como controles fundamentales para un programa de cumplimiento. Este análisis empírico tiene como objetivo descubrir las características y componentes de las políticas de cumplimiento y su uso como herramienta de comunicación para las partes interesadas internas y externas con respecto a los objetivos de la organización en la búsqueda del cumplimiento de los requisitos regulatorios/de la industria. La política de cumplimiento se convierte en una importante herramienta de comunicación de la intención de la organización a la hora de abordar los requisitos que les impone el entorno normativo, tanto el gobierno como las normativas impulsadas por la industria. Se llevará a cabo un examen de las características y componentes de la política de cumplimiento para mejorar nuestra comprensión de la respuesta que la organización está comunicando y lo que tomará para abordar su respuesta. Un elemento central de este ejercicio es conectar lo que la organización comunica como los objetivos de su programa de cumplimiento y las respuestas estratégicas y tácticas definidas en las características y componentes del documento de política. En este capítulo se presenta el componente político de esta tesis. En este contexto, la política se convierte en una declaración escrita de lo que la organización se compromete a implementar en respuesta a los requisitos de cumplimiento que se les imponen. La política de cumplimiento de la organización se convierte en lo que la organización dice que hará y cómo planea hacerlo.

El tercer capítulo de la tesis presenta un estudio de caso de un hospital infantil y cómo aborda el cumplimiento y el riesgo de seguridad de la información con un mandato gubernamental. El estudio de caso sigue a la implementación de una solución de autenticación y credenciales multifactor para lograr el cumplimiento de las Recetas Electrónicas para Sustancias Controladas de la Administración para el Control de Drogas (DEA-EPCS) y abordar los requisitos de gestión de riesgos identificados. En este capítulo, se exploran las implicaciones teóricas y prácticas del cumplimiento como una interacción de las diferentes áreas de la organización que se unen para implementar un requisito para una actividad de cumplimiento y, al mismo tiempo, se enfrentan a las compensaciones necesarias para equilibrar otras necesidades operativas, como las actividades de gestión de riesgos. A continuación, se presenta una discusión general de los resultados y sus implicaciones teóricas y prácticas. Una conclusión general examina los conocimientos derivados, las limitaciones de la investigación y los próximos pasos.

Chapter 1: Compliance, Risk Management, and Information Security - An Integrative Literature Review

1.1 Introduction

Compliance and risk management requirements are a reality of modern businesses. Depending on the operational context, each business's unique situation will drive how compliance and risk management are addressed.

Compliance with government and industry regulations is a reality of doing business for many organizations. Failure to comply with the required regulations can bring significant organizational risks and is an ongoing concern. Organizations can face fines and, in extreme cases, be barred from continuing to do business. (Armour et al., 2020, p. 13). Estimates vary on the amount that organizations spend annually on compliance tasks. A study from the University of Southern California Marshall Institute for Outlier Research in Business estimated that in the United States, compliance costs range between $79 billion to as high as $289 billion per year. (Trebbi et al., 2023, p. 12). Corporate fines and penalties have averaged $ 15 million, with assessed penalties reaching hundreds of millions to billions of dollars per year (Armour et al., 2020, p. 13). As such, considerable time and resources are devoted to ensuring compliance with regulations and other industry requirements (Armour et al., 2020, p. 13). Given the significant impact of potential fines and penalties, including the loss of licensing to conduct business, it makes a solid case to study how compliance is defined and implemented through policy and organizational actions.

Whereas compliance requirements and establishing a compliance program may be driven by the need to comply with regulations and thus avoid potential

liabilities resulting from failure to comply, risk management addresses the organization's operating environment's requirements to identify and mitigate risks. Pascarella defines risk as “the chance of something happening that will have an impact on the achievement of the stated organizational objectives and describes risk management as “all the activities connected with hazard identification, assessment, selection of appropriate responses and risk monitoring” (Kusserow, 2020, p. 49; Pascarella et al., 2021, p. 2897). Well-executed compliance and risk management programs provide the organization with a control set that, when viewed holistically, can reduce the overall risk to the organization and its operations. When dealing with risk, organizations must consider their risk exposure, both internal and outward-facing. Compliance can be viewed as a risk and should be managed effectively by establishing, implementing, and maintaining appropriate controls.

Organizations aim to comply with regulations through policies, standards, and procedures. The practice of compliance with rules is reflected in organizational actions, such as enacting defined policies and procedures in their daily activities. Documented policies and procedures also represent how the organization responds to or plans to respond to external and internal requirements.

In this context, policy documents such as Compliance, Information Security, and Privacy policies, among others, serve as conduits for the organization to establish and communicate the expected behaviors and actions of organizational stakeholders, including employees, contractors, and others tasked with implementing these policies. These policies establish the control framework that the organization must follow to attain and remain compliant with its obligations, whether legal, regulatory, or part of its regular day-to-day business. Beyond communicating the expected behaviors and actions, they can also help guide how controls are defined

and applied to demonstrate adherence to the policy's goals. In plain language, an organization's policies outline what it will do and how its actions will be measured through internal and external audit activities.

1.2 Previous Work on Compliance and Information Systems Risk

A substantial body of knowledge regarding compliance and compliance activities centers on information security and its associated policies. This indicates the vital interplay between the organization's compliance, information systems, and risk management.

Compliance has significantly impacted the development, deployment, support, and protection of information systems. Regulatory requirements must be incorporated into the implemented system to prevent noncompliance and associated negative repercussions. Current literature on compliance focuses on topics such as adoption and adherence rates, influencing adherence to policy, and the effectiveness of education and training (Daljord et al., 2023; Zhou et al., 2022). Other research areas aim to determine the extent to which a particular policy is followed and how the reasons for following or not following a policy might be understood(Kuiper et al., 2023; Wu & van Rooij, 2021). Recent work on eliciting or encouraging compliance includes Daljord et al. (2023, p. 887), who, in a field experiment setting, proposed an approach to targeted promotions to promote compliance in the context of a hotel rewards program. An experimental approach demonstrated that targeted promotions could help achieve desired outcomes. Kuiper (2023) employs a network approach to understand how individual compliance may be influenced by a network of variables, providing a means to connect a complex system of variables that combines

theoretical frameworks rooted in the behavioral and social sciences (Kuiper et al., 2023, p. 493). Using social exchange theory, Lee (2021) leverages a theoretical lens of social exchange. It finds that firms will temper their compliance efforts with tax law based on the perceived value or fairness assigned to the exchange between the business and the government based on the assigned value that the organization assigns to the services provided by the government in return for their tax dollars (Lee et al., 2021, p. 203).

This leaves an opening to seek an understanding of the underlying processes, antecedents, and artifacts that either provide the foundations of a compliance program or create the environment where the goal is to have a compliant and ethical organization.

In the healthcare industry, risk reduction and risk management have increased in importance in recent years.(Pascarella et al., 2021). Following years of increased regulatory complexity, a “compliance-first” mentality is no longer sufficient to keep the organization moving forward. Organizations across industries require new approaches to address regulatory requirements and emerging risk management paradigms driven by new threats such as ransomware, data breaches, and third-party risk, which increase reputational and financial risks that could severely threaten organizational viability. This research primarily focuses on the policy and operational aspects of compliance and risk management. We will use strategic responses to institutional processes as a theoretical lens. (Oliver, 1991) We will explore existing research efforts in risk management and compliance, with a focus on information systems.

In the area of management, the Information Systems Security literature is extensive and diverse. The common thread among them is the emphasis on the

security of information systems as an important topic, given the importance and impact of information systems in our daily lives (Alec Cram et al., 2019; Arenas et al., 2024). Beyond the literature itself, you don't have to go far to find examples in the press and social media of the latest data breach or computer system vulnerability affecting everything from the lives of those victims of identity theft to even the trust in our election system. The old paradigm that just another piece of technology or advances in current technology will solve security problems needs to cede way to the realization that organizational processes have been left behind and will require a concerted effort to update our process and the way we operate to maximize the benefits of the available technologies.

Information Systems Security Literature can be divided into two basic streams, those with a technical emphasis and those with a non-technical focus, represented by the literature in Computer Science/Engineering on the former and management issues on the latter. Non-technically focused research follows a behavioral approach (Albrechtsen, 2007; Ifinedo, 2009, 2014) or an economic approach (Kumar et al., 2008)to explain how organizations implement information security. Ifinedo (Ifinedo, 2014) and Bulgcuru, Cavusoglu, and Benbasat (Bulgurcu et al., 2010) help make the connection between an individual's behavior and its impact on the overall compliance posture of the organization and how it can be improved. This lower-level examination of individual behavior can be used to compare it to the overall posture of the organization and compare the effects of changes at the micro and macro levels of the organization. Kumar, Park, and Subramaniam (Kumar et al., 2008) present an economics-based model that can help an organization rationalize the priority of information security risk management in terms of quantifiable impact on the organization. Their proposed framework could be extended to be applied in

this case and can be explored as a future research topic where it can be extended to address governance, risk management, and compliance in the context of regulated environments.

Hu, Hart, and Cooke (Hu et al., 2007a) suggest a compelling case for the need for a “socio-organizational perspective” in information security, pointing out the insights on change and inertia seen in numerous studies. Hu, Hart, and Cooke (2007) paraphrase Dhillon and Backhouse (Mishra & Dhillon, 2006) and agree with the argument that information security research has been dominated primarily by the technical and functional issues more closely related to information systems design and development more in line with computer and information systems research. The human element, being at the center of information systems activity hence, should be part of the equation when studying the environment, and institutional theory is well suited to provide the theoretical framework that makes the connection between the human and technical elements of information systems security (Bjorck, 2004; Dhillon & Backhouse, 2003; Hu et al., 2007a). Hu, Hart, and Cooke (Hu et al., 2007a) inform an assessment of the impact that a complex regulatory environment and its compliance requirements can have on the institutional environment. Appari (Appari et al., 2009) identify the relevance of studying compliance in an organizational context like health care where “...the growing dependence on It to manage health information is the increased information security and privacy risks.” Modern organizations work in a risk environment littered with operational and reputation risks, where information technology advances can make any organization global (Hsu et al., 2012b). With the added reach afforded by technology comes added risk in the form of cyber threats, such as the attacks on Sony Pictures and the United States-based insurer Anthem. Mignerat (Mignerat & Rivard, 2009), as well as Hsu,

Lee, and Straub (Hsu et al., 2012b), provide a pathway for a Neo-institutional theory framework that can serve to study how institutional changes are propagated and assimilated. They provide further evidence that regulation compliance affects the implementation of information security management (Hsu et al., 2012b). This has implications for policy as well as practitioners that look at finding ways to execute information security requirements as well as those of regulations.

Williams, Hardy, and Holgate (Williams et al., 2013) introduce the dimension of governance to information security management, adopting an institutional perspective that recognizes the need to protect an organization's digital assets to maintain operational continuity. This aligns with a growing call for a holistic approach to Governance, Risk, and Compliance, which has gained traction in recent years (See Tarantino, 2008, for a comprehensive view on Governance, Risk, and Compliance). This can be interpreted to highlight the connection between the operational importance of good information security management and compliance, as both support organizational legitimacy through continued operations and the maintenance of legitimacy through regulatory compliance by examining the development of "competing and even contradictory arrangements" (Williams et al., 2013). Spears, Barki, and Barton (Spears et al., 2013) further drive the relationship between regulations and information security by making the connection between regulations and information security. They propose that identified issues and threats cause the enactment of regulations that, in turn, become institutionalized and influence the implementation of information systems security within individual organizations (Spears et al., 2013). They point to the cross-border effects of regulations in our increasingly interconnected globalized world. Kam, Katerattanakul, and Emerick (H.-J. Kam, Katerattanakul, & Emerick, 2013), Kam, Katerattanakul,

and Gogolin (H.-J. Kam, Katerattanakul, & Gogolin, 2013), and Kam and Katerattanakul (H.-J. Kam & Katerattanakul, 2014) have successfully applied a Neo-institutional theory-based framework to the study of compliance and information security across industries (Banking and Higher Education) and within an industry (Higher Education/Banking). In Kam, Katerattanakul, and Emerick (H.-J. Kam, Katerattanakul, & Emerick, 2013) and Kam and Katerattanakul (H.-J. Kam & Katerattanakul, 2014), the authors provide an institutional perspective on external pressures and their effects on compliance for the banking industry, an example of a regulated environment. Kam, Katerattanakul, and Gogolin (H.-J. Kam, Katerattanakul, & Gogolin, 2013) compare banking and higher education information security compliance.

The literature on compliance explores the effects of regulations like the Sarbanes-Oxley, the Gramm–Leach–Bliley Act, and the Federal Information Security Management Acts. (Hulitt & Vaughn, 2010) and their impact on organizational activities (Gordon et al., 2006). A parallel research stream focuses on internal compliance aspects in how internal actors follow organizational information systems security policies and procedures compliance. (Bulgurcu et al., 2010; Ifinedo, 2014).

Westby's survey report on the state of information security (Westby, 2015) shows a trend regarding the relative importance of risk management versus compliance activities at the organizational level. The trend shows that risk is on its way to overcoming compliance as an ongoing concern soon (Michelberger Jr. & Labodi, 2012). This requires organizations to consider ways to rationalize and integrate their risk and compliance efforts. This is especially true of information systems security. Williams, Hardy, and Holgate (Williams et al., 2013, p. 341) mention that "achieving a sustainable information protection capability within the

complex business, legal and technical environments is an integral part of supporting an organization's strategic and compliance objectives." An organization's regulatory requirements and its own security risk footprint can often be at odds and competing for the same attention and resources.

Other non-technically focused research follows a behavioral approach. (Albrechtsen, 2007; Ifinedo, 2014) or an economic approach (Kumar et al., 2008) To explain how organizations approach and implement information security. Ifinedo (Ifinedo, 2014) and Bulgcuru, Cavusoglu, and Benbasat (Bulgurcu et al., 2010) Help make the connection between an individual's behavior and its impact on the overall compliance posture of the organization and how it can be improved. This lower-level examination of individual behavior can be used to compare it to the overall posture of the organization and compare the effects of changes at the micro and macro levels of the organization. Kumar, Park, and Subramaniam (Kumar et al., 2008) Present an economics-based model that can help an organization rationalize the priority of information security risk management in terms of quantifiable impact on the organization.

Recent work on risk includes the study of risk resource allocation (Insua et al., 2021). The authors point to the inadequacy of risk matrixes and propose an alternative framework through the lens of a case study. (Insua et al., 2021) proposes a portfolio of controls to mitigate risks. The proposed framework aims to optimize said controls portfolio and provide cyber insurance risk mitigation/assignment, maximizing expected utility. The Risk Management Working Group also points out the need to layer and prioritize risk management controls and the need to look at the risks that technology-related controls are expected to address (The RMA Journal, 2020). The current pandemic has exacerbated the risks and challenges faced by

organizations across the spectrum, where the risk to data and organizational assets has increased as they must be protected inside and outside the corporate boundary (Devlin, 2020). Another study of risk in the context of risk management for data centers (Bieser et al., 2020) discusses the extensive availability of risk models and research. They propose that the risk management process should take a holistic approach where qualitative and quantitative analysis are combined to integrate risk management, but it is challenged by the diversity of the theoretical foundations and their interpretations.

The complex environment in which organizations operate requires that management acquire the skills and processes to confront the challenges to the security of their systems. Management also needs to leverage situational awareness to respond to incidents. (Ahmad et al., 2020). Information security is recognized as a strategic business issue due to the rapid adoption of new and emergent technologies and solutions and the direct impact on operations and company profitability in case of a breach.

1.3 Strategic Responses to Institutional Processes

Organizations are a product of their institutional context. Organizational processes and tasks often respond to external or internal requirements that require the organization to respond to external pressures. These pressures can take the form of compliance with regulations or internal requirements, such as measures taken to reduce enterprise risk.

In (Oliver, 1991), Oliver provides a window to examine how organizations respond to their institutional environment. The requirements of the environment move organizations across a spectrum of responses, from passive compliance to

active defiance. Hu, Hart, and Cooke suggest a compelling case for using a Neo-institutional perspective to study the need for the forces that drive organizational change or inertia seen in numerous studies (Hu et al., 2007a). The human element, being at the center of information systems activity, hence, should be part of the equation when studying the environment. Strategic responses to institutional processes (Oliver, 1991) are well suited to provide the theoretical framework that makes the connection between the human and technical elements of information systems security (Bjorck, 2004; Dhillon & Backhouse, 2003; Hu et al., 2007b). Hu, Hart, and Cooke (Hu et al., 2007a) inform our assessment of the impact of a complex regulatory environment and its compliance requirements on the institutional environment.

Modern organizations work in a risk environment littered with operational and reputational risks, where information technology advances can make any organization global. (Hsu et al., 2012b). With the added reach afforded by technology comes added risk in the form of cyber threats, as the well-documented attacks on Sony Pictures and the United States-based insurer Anthem show. Hsu, Lee, and Straub (Hsu et al., 2012b) Provide a pathway for a Neo-institutional theory-based framework that can study how institutional changes are propagated and assimilated. They provide further evidence that regulation compliance affects the implementation of information security management. (Hsu et al., 2012b). This has implications for policy and practitioners who are looking to find ways to execute information security requirements as well as those of regulations.

Williams, Hardy, and Holgate (Williams et al., 2013) add the dimension of governance to information security management with an institutional perspective recognizing the need to protect an organization's digital assets to preserve the

continuity of operations. This aligns with a call for a holistic approach to Governance, Risk, and Compliance that has gained traction in recent years (See Tarantino, (Tarantino, 2008) for a comprehensive view on Governance, risk, and compliance).

Spears, Barki, and Barton (Spears et al., 2013) Further, it drives the relationship between compliance and information security by making the connection between regulations and information security. They propose that identified issues and threats cause the enactment of regulations that, in turn, become institutionalized and affect the implementation of information systems security within individual organizations. (Spears et al., 2013). They point to the cross-border effects of regulations in an increasingly interconnected globalized world. This research helps to inform the inter-institutional effects of regulations not only within national borders but across international borders. This is relevant in studying how banking regulations are established based on our assessment of the similarity in regulatory requirements between countries during professional engagement in the study areas.

Kam, Katerattanakul, and Emerick (2013), Kam, Katerattanakul, and Gogolin (2013,) and Kam and Katerattanakul (2014) have successfully applied a Neo-institutional theory-based framework to the study of compliance and information security across industries (Banking and Higher Education) and within an industry (Higher Education/Banking) (H. J. Kam et al., 2019; H.-J. Kam, Katerattanakul, & Emerick, 2013; H.-J. Kam, Katerattanakul, & Gogolin, 2013; H.-J. Kam & Katerattanakul, 2014). In Kam, Katerattanakul, and Emerick (H.-J. Kam, Katerattanakul, & Emerick, 2013) and Kam and Katerattanakul (H.-J. Kam & Katerattanakul, 2014), the authors provide an institutional perspective on external pressures and their effects on compliance for the banking industry, a key aim of this study. Kam, Katerattanakul, and Gogolin (H.-J. Kam, Katerattanakul, & Gogolin,

2013) compare information security compliance between banking and higher education, which helped inform the approach taken in this paper. This study follows the same line of inquiry, applying a similar theoretical approach to the problem of the effects of external pressures on risk management and compliance in a regulated industry.

Oliver (Oliver, 1991) Offers a menu of strategic and tactical responses that can serve as a starting point to uncover the underlying processes that an organization follows to respond to external and internal pressures and the competition between them for finite organizational resources. Oliver calls for five strategic responses that organizations follow to address environmental pressures. Each strategy is comprised of several tactical responses that exemplify the strategy. Each strategy and its accompanying tactics progressively increase the organizational efforts to resist the impact of those external influences. These strategies and their tactics are defined by Oliver as follows:

(i) Acquiesce – compliance through habit (response is second nature and unconscious, engrained in the institutional environment), imitation (following how others achieve/maintain compliance through mimetic isomorphism), or compliance (a deliberate and concerted effort to comply with the institutional environment)

(ii) Compromise – balance (accommodation of competing demands, seeks parity between stakeholders), pacify (aims to achieve at least partial conformity with one or more constituents' demands, minor resistance to compliance striving for the minimum requirement attainment), or bargain (extract some concessions from external demands or expectations)

(iii) Avoidance – use of concealment (hide non-compliance behind a façade of compliance), buffering (avoid being audited or externally inspected), escape (exit a domain to avoid compliance) tactics to hide non-compliance

(iv) Defy – dismissal (willfully ignoring compliance requirements), challenge (take a defiant stand against compliance), or attack (actively devalue requirements and those that comply with them) of compliance requirements; and

(v) Manipulate – using co-opting (incorporating the source of the pressure inside the organizational structure), influence (lobbying or attempts to manipulate belief systems or acceptable levels of compliance), or controlling (establish power and control as to dominate external stakeholders and their pressure on the organization) tactics to directly influence the compliance dynamic. The distilled insights of the case study result in the identification of the most common strategies and tactics employed by the studied organization when looking to balance information systems risk management and compliance.

The study of information security and compliance within a Neo-institutional theory-based framework like Oliver's strategic responses to institutional processes should help advance our understanding of how organizations can be better prepared to grapple with the challenges faced by modern enterprises in compliance and risk management. In this study, we look forward to extending this field and contributing an additional perspective to inform academics and practitioners.

Chapter 2: Compliance Documents in Health Care – A Content Analysis

2.1 Introduction

Compliance activities are essential in regulated environments, such as healthcare or financial services organizations. The potential impact of failing to achieve and maintain compliance with applicable regulations can be significant to an organization. An organization that fails to achieve and maintain compliance could be subject to fines up to the termination of its authority to operate, as would be the case when losing a license or access to market tools and infrastructure. For instance, non-compliance with the Payment Card Industry – Data Security Standard (PCI-DSS) can result in an organization losing its ability to process credit card payments. Compliance-related tasks have a significant economic impact, with some estimates ranging from $79-$289 billion. (Trebbi et al., 2023, p. 13) and up to $3.079 trillion (Crain & Crain, 2023, p. 4).

Compliance programs help organizations address the requirements of their regulatory environment by helping manage the identification, definition, and implementation of appropriate controls and establishing an ethical environment. These controls form a system of policies, procedures, and processes that help the organization comply with applicable regulations. (Carboni, 2022, p. 1). Compliance documents form the backbone of any organization's compliance program by setting the tone and the direction that the organization has chosen. Organizations use compliance documents to structure and manage their programs and guide both expected behaviors and operations to achieve and maintain compliance with applicable laws and regulations. (Kusserow, 2014, p. 27)

Extant research on compliance is extensive; some lines of inquiry focus on studying compliance in the context of human behavior and its actions rather than as an organizational activity. There is an absence of empirical studies on the specific features and components of compliance policies that provide an understanding of their content and how they reflect organizational decisions on how they approach their compliance efforts. Lopes (Lopes & De Sa-Soares, 2012, p. 3) Provides a comprehensive view of the features of a policy in the context of an analysis of the content of information security policies. The policy documents can be evaluated in terms of their features and components.

This study aims to examine compliance policies in healthcare organizations to identify their features and components. The research seeks to answer the primary questions:

- What are the features of a compliance policy?
- What are the components of a compliance policy?

Documented policies and procedures are prerequisites for formally implementing a compliance program's documentation and processes. There are limited empirical studies on the features and components of compliance documents, as well as the elements they have in common beyond the guidelines provided by regulatory, professional, and law enforcement bodies in government and industry. An examination of compliance policies can inform both theory and practice. Researchers can investigate strategies and models to improve adherence to regulatory compliance by empirically studying compliance policies as a control and the role played by their features and components. Research on the features and components of compliance policies can have a profound impact on practitioners by

providing them with a clear understanding of the regulatory landscape and the necessary steps to ensure compliance. The features of a compliance document

This study will review the compliance policies of 30 (thirty) healthcare organizations. It aims to empirically explore compliance policies in a sample of healthcare organizations.

While analyzing the available compliance documents to respond to our research questions, we can gain a deeper understanding of these documents and address additional questions regarding their characteristics, such as:

- How long are compliance documents?
- For how long are compliance documents valid?
- What sections comprise a compliance document?
- How are compliance documents delivered?
- How can compliance documents be described?

Regarding the components of compliance documents, the following questions can aid in further exploring the prevalence of literature-predicted components on the compliance documents:

- Which components from the literature and best practices are used in compliance documents?
- What are the most common components of compliance documents?
- What, if any, expected components are not included in compliance documents?
- What purpose do compliance documents serve?
- What variability is in the scope of compliance documents?
- How are duties and responsibilities defined in compliance documents?

The scope of the study is limited to publicly available compliance policies adopted by healthcare organizations in North America. These documents will be evaluated against industry and government guidance to empirically study how the compliance policies of different organizations adhere to the expectations set forth by available guidance.

The following section after this introduction will consist of a short literature review, a description of our methodology, study results, a discussion, and a conclusion with suggestions for future work. A more extensive literature review is presented in Chapter 1.

2.2 Literature Review

Compliance as a concept depends on the context in which it is used. Much academic work can be found in law, business, public policy, health care/medicine, and accounting. For this study, compliance will be defined as the tasks an organization engages in to fulfill the requirements of regulators or industry and the processes and activities the organization employs to attain and maintain said compliance. There are other research branches in compliance, as would be the case with the literature on compliance and health outcomes. This study will focus on compliance and its role in the context of organizations. A review of the recent literature on compliance can be organized into three distinct research branches. These branches are behavioral, compliance and risk, and compliance and technology. The behavioral focus area of the literature examines the variables that influence compliance and non-compliance behaviors with established policies or other requirements. Compliance and technology literature focuses on the relationships between technology and compliance. Compliance and risk literature

explores the relationship between risk and compliance. As a recommended control, a compliance policy can be an essential antecedent to a successful compliance and ethics program. There is an opportunity for the analysis of compliance policies to add to the existing extensive examination of information security and privacy policies to expand our understanding of compliance policy as a control in implementing a compliance program.

The first branch of the literature, defined for this study as the behavioral approach to compliance, aims to uncover the actions of individuals and organizations subject to a compliance requirement. Recent examples of these behaviorally focused studies include Kuiper (Kuiper et al., 2023, p. 493), which, when studying compliance requirements with Covid-19 rules, combined variables from key compliance theoretical frameworks in the social and behavioral space and applied a network analysis approach to individual compliance based on those variables. It describes individual compliance behavior as the interplay of variables from each compliance theory and compliance itself. It also identifies interactions between variables that do not conform to the current theoretical framework as the results. Boaye (Boaye Belle & Zhao, 2023, p. 23) proposes a new type of assurance case called systematicity that enables checking how accurate reporting is vis-vis established guidelines. Daljord (Daljord et al., 2023, pp. 887–888) used an experimental approach in a hotel rewards program to uncover recommendations on building compliance promotions and properly selecting within the target population. Its results point to the potential of their proposed approach to improve hurdle and profit estimates that would otherwise be off by 50% to 100%. Zhu (Zhu et al., 2023, pp. 796–798) explored how paternalistic leadership styles influence compliance with information security policies. The experiment results found that the three examined paternalistic leadership styles,

authoritative leadership, moral leadership, and benevolent leadership, positively contributed to influencing compliance with information security policy. Authoritative leadership was shown to have the most substantial impact on eliciting the expected behavior. The study also found support for the positive influence of benevolent and moral leadership at a lower level than that of authoritative leadership. Li (Li & van Rooij, 2022, pp. 729–730) finds the difficulty that external norms, like regulations, have reached into the organizational sphere. Regulatory requirements and their enforcement mechanisms do not readily and successfully enter the organization and with downstream effects that include individual compliance by organizational actors. The study also found that compliance can still occur even if the legal requirements do not reach individual actors. This was attributed to an apparent alignment between an individual's value system and the goals of the law or regulation. Xie (Xie et al., 2021, pp. 2191–2192) find that the legal, political, and social environment in which a firm operates can create conditions where a government mandate can be deemed "semi-coercive" in nature due to several factors related to the threat of enforcement and its accompanying potential penalties. Results indicated that perceived enforcement levels impacted actual organization and individual behavior. In jurisdictions with a mature regulatory establishment, the threat of enforcement is considered high by an organization, resulting in a higher likelihood of compliance to avoid the risk of repercussions for non-compliance in contrast with emergent or less mature jurisdictions where the threat of enforcement poses less of a risk thus the organization is more likely to be in non-compliant status with no threat of repercussions. Politically connected organizations and those led by politically connected individuals appeared willing to avoid compliance with regulations based on a perceived enforcement uncertainty that their relationship with the government

might provide. Organizations with limited or low public exposure also appear willing to be non-compliant for the same reason, “enforcement uncertainty,” or the perceived low risk of being subject to repercussions for non-compliance. Other insights include the willingness of government-owned enterprises to avoid compliance with regulations.

Behavior-based compliance literature focuses on the individual or the organization in the form of its outcomes (i.e., compliance or non-compliance), often identifying the variables, artifacts, processes, controls, etc. This reinforces the need to understand the underlying compliance controls, such as an organization’s compliance policy.

The intersection of compliance and technology offers fertile ground for research. Freij (Freij, 2020, p. 186) Concludes that the regulatory environment's complexity and heterogeneity require technology providers to focus on generic processes and solutions with general applicability instead of one-off bespoke or single-purpose solutions. It also concludes that the current focus of providers on current requirements opens the risk of sacrificing the organization's adaptability to an evolving regulatory environment, sacrificing tomorrow's requirements for the requirements of today, leaving the organization without the flexibility to adapt its processes and tools to new organizational realities. Finally, it concludes that strategic importance and integration of external resources are areas of concern as they could hinder future progress and increase complexity and cost.

Notably, outside of the academic literature, compliance program guidance is often offered by agencies with regulatory and law enforcement responsibilities like the United States Department of Health and Human Services (*Compliance Guidance | Office of Inspector General | Government Oversight | U.S. Department of Health*

and Human Services, n.d.), the Health Resources and Services Administration – Bureau of Primary Care (Health Resources and Services Administration - Bureau of Primary Health Care, 2023)the United States Sentencing Commission 2018 Chapter 8 PART B - REMEDYING HARM FROM CRIMINAL CONDUCT, AND EFFECTIVE COMPLIANCE AND ETHICS PROGRAM (*2018 Chapter 8 | United States Sentencing Commission*, n.d.), as well as consultants and trade associations like the Association of Corporate Counsel (Carboni, 2022). The extent of the available guidance is mostly practical, providing a range that includes descriptive and prescriptive guidance all the way to very detailed instructions in the form of checklists, templates and outlines, among others. Government guidance is grounded on the regulations that the government has a vested interest in organizational compliance; however, due to the legal nature of the regulations themselves, the language tends to be centered around legal terms, making it oftentimes difficult for organizations to make the connection between the regulations and what tasks or activities they need to be engaged with to attain and maintain compliance with regulations. For this reason, consultants, trade associations, and professional organizations provide actionable guidance grounded on the regulations to help draft, implement, and evolve compliance programs.

2.2.1 Features of Compliance Policies

The features of a compliance policy are comprised of the set of characteristics contained within a policy document. Available government and industry guidance agrees on characteristics like length and complexity, how they are written, and how often they are reviewed or updated. A proper compliance and ethics program for which policies are an important component can assist organizations in reducing their

risk from fraud, waste, and abuse (Carboni, 2022) and reduce risk in case of litigation or other government legal action. The US Federal Sentencing Guidelines Manual, Section §8B2.1, Effective Compliance and Ethics Program (*2018 Chapter 8 | United States Sentencing Commission*, n.d.), lists seven elements that should be at the center of a compliance program that exercises due diligence and promotes an ethical culture throughout the organization for which a compliance policy can be a foundational part. Those elements are:

1. Standards, policies, and procedures documentation
2. A dutifully appointed officer, committee, and upper-level executive oversight
3. Exercise due diligence and due care to exclude individuals from positions of authority who have engaged in illegal activities in the past inconsistent with program goals
4. Conduct periodic training on the standards, procedures, and expectations of the compliance and ethics program, ensuring that the required information is delivered to each stakeholder throughout the organization.
5. Audit, monitor, and evaluate periodically the program for effectiveness and the organization's stated program goals. Implement anonymous reporting structures for reporting conduct that does not meet expected standards.
6. Communicate incentives and disciplinary measures in the performance of the compliance program.
7. Respond promptly upon discovery or report of prohibited conduct to prevent its recurrence in the future.

The guidance from the U.S. Sentencing Commission lists first standards, policies, and procedures in their guidance of compliance programs, pointing to the foundational nature of these types of documents. The first element is where

documents like compliance policies reside. These documents provide guidance for implementing the compliance program and serve as the organization's tool for communicating the expectations of its stakeholders. According to Carboni (Carboni, 2022), such documents should be:

1. Guidelines defining expected behavior in the context of identified risks
2. Readily available to all stakeholders
3. Reviewed, updated, and approved at regular intervals (e.g., at least every 12 months)
4. Clear and detailed

Each written policy and procedure should include the following:

1. Expected duties and responsibilities of all stakeholders, those with oversight responsibilities, and those tasked with implementing the policy and or procedure.
2. Training program description and requirements
3. Define:
    - the program's overall operation,
    - reporting requirements,
    - how investigations will occur,
    - corrective responses,
    - issue management,
    - continuous evaluation,
    - and auditing.
4. Duty and responsibility assignments for each area within the organization
5. Description of how interdepartmental interactions shall occur between compliance, audit, operations, legal, and human resources.

6. Key performance indicators of program effectiveness

Policies can be delivered in one or multiple formats: printed, online (e.g., policy portal), or electronic document form. Electronic formats make it easier to make updates and share them with stakeholders faster, ensuring timely and wide dissemination.

2.2.2 Components of Compliance Policies

The components of a compliance policy, as well as other related documents, such as a code of conduct, are all controls that can be used as part of a compliance and ethics program. Beyond establishing the foundations for the policies, procedures, and processes, they also serve to mitigate risks of non-compliance with applicable regulations and to document demonstrable due diligence with compliance requirements as part of probation requirements after a legal proceeding (*2018 Chapter 8 | United States Sentencing Commission*, n.d. Ch 8 Part B 2.1). Industry resources and government agencies provide some guidance on how compliance documents like policies and procedures should be structured. In the United States, agencies like the United States Department of Justice and the United States Department of Health and Human Services and individual agencies like the Food and Drug Administration provide compliance guidelines that help organizations establish acceptable compliance programs under the regulatory regime. For the purposes of this study and based on its health care focus, the recommendations from former United States Department of Health and Human Services Richard P. Kusserow, who provides practical guidance on the key elements of a policy document, will be used, and it is as follows (Kusserow, 2013, 2014):

- Header block, to include:

  - Title
  - Department accountable for policy
  - Effective date
  - Policy identification number
  - Approval date
  - Approving authority
  - Statement if modifies or replaces existing policy
  - Number of pages
- Background
  - Describes the operational context of the environment that the policy exists to address. It should help with understanding and following the policy.
- Purpose
  - This section should define and communicate the goals and objectives of the policy
- Definitions
  - Used to describe legal of highly technical key terms.
- Scope
  - Defines the applicability of the policy to individuals, locations, or activities.
- Policy Statements
  - Reflects organizational goals regarding compliance and provides the rules the organization must follow
- Procedures

    - Prescriptive, describes in detail the expected behaviors within the scope of the compliance requirements.
- Related Policies
    - Cross reference with other policy documents, used to avoid potential conflicting guidance amongst policies
- References/Citations

Like it was the case in Lopes & De Sa-Soares (,2012),) Most of the guidance on the features and components of compliance policies is available from trade groups like the Association of Corporate Counsel, government agencies like the U.S. Department of Health and Human Services, and the U.S. Sentencing Commission and consultants. Those bodies define standards that organizations can leverage in their own compliance undertakings. It is that guidance that will be used in this case to develop the methodology to examine the sample compliance policies.

2.3 Methodology

This study aims to empirically examine Compliance documents within healthcare organizations. To obtain the samples, a search of publicly available compliance policies was conducted on the World Wide Web. For this study, the healthcare sector in the United States and Canada was selected due to its similar regulatory requirements and language. Other similarly regulated sectors, such as financial services, were excluded from the sample to minimize potential inter-industry variability in the features and components of compliance policies due to differences in operational environments and regulations.

The healthcare sector in the United States and Canada was selected for several reasons. The first reason was the public availability of compliance policies

and other ancillary policies. The sample comprises documents from 30 hospitals or hospital systems, spanning both public and private organizations. Since the introduction of the Health Insurance Portability and Accountability Act close to 30 years ago, the sector in the United States has undergone significant changes, resulting in organizations today devoting significant resources to compliance activities as part of the estimated $600 billion to up to $1 trillion of health care spending dedicated to administrative activities. (*Administrative Expenses in the US Health Care System Why So High?*, 2021, p. 1679)

One goal of this study is to explore how organizations in a healthcare setting approach compliance through their stated policies and compliance documents. How compliance is addressed in an organization's policy documents provides insight into how it plans to act and expects its employees and representatives to act accordingly. Understanding how the organization addresses these topics helps in understanding its priorities. Those priorities can make a significant difference in an organization by leveraging synergies between compliance and other areas, such as information security and risk management. To further this point, it is essential to establish how each is defined in the context of this study. For the purposes of this study, compliance, information security, and information security risk management are defined as:

Compliance: In the study context, compliance can be understood interchangeably as an operational function, a process, and an action. The website of the Association of Corporate Counsel defines compliance as "a formalized system of policies, procedures, and processes developed and implemented to prevent, detect, and correct conduct that is inconsistent with applicable federal and state laws" (Carboni, 2022). Li describes compliance as a "process of transmission and reception of legal

norms” (Li & van Rooij, 2022). The operational function refers to the people and processes that help identify and implement the required controls for an organization to demonstrate compliance with a regulation, thereby verifying that the organization meets the specified requirements. Compliance is also a process by which the organization implements and follows the requirements of a regulation or other externally imposed requirements like the Payment Card Industry – Data Security Standard (PCI-DSS). Compliance is the active act of complying with a requirement. As an action and from a theoretical perspective, compliance is one of the tactical responses identified by Oliver in her 1991 paper Strategic Responses to Institutional Processes. (Oliver, 1991)

Information Security: An organization’s policies, procedures, infrastructure, and operational resources (people, process, technology) are used to protect the confidentiality, integrity, and availability of information technology and digital assets.

Information Security Risk Management: An organization’s policies and procedures that define and assist with the identification, qualification, quantification, and mitigation of risks to information assets through the identification and implementation of controls to manage risk according to the organization’s risk appetite. Information Security Risk management can appear as part of the information technology organization, the information security team, or under a risk management operation.

2.3.1 Data sources and research context

The data selected for this study follows a “purposeful selection” strategy. (Maxwell, 2013, p. 97) And focuses on healthcare organizations' compliance policies as the relevant sources to examine the research questions. In the context of this study, said policies act as the organization's voice on how it has decided to define

and address its requirements for its compliance program. The chosen policy examples are sourced from various healthcare organizations that vary in location, size, and focus. The study documents were procured by searching the Internet for healthcare organizations that published their compliance policy documents online. Organizations in the healthcare industry focusing on the North American region were selected to standardize the comparison of the compliance policies. This should help reduce the variability introduced by inter-industry differences and organization-specific requirements. This search resulted in selecting 30 (thirty) compliance policies and documents on which this study is based.

The healthcare sector was selected due to its highly regulated nature. Healthcare organizations have requirements that provide a rich environment for regulatory compliance. They are required to comply with local, state, and federal regulations that create a complex environment where a robust compliance program and its associated controls are needed to help the organization respond to the pressures resulting from the environment in which it operates.

2.3.2 Analysis Strategy

Using content analysis, the selected compliance policies are studied to understand their adherence to the baseline features and components derived from the work of Kusserow and Carboni (Carboni, 2022; Kusserow, 2013). Content analysis is the study of documents and communication artifacts to examine patterns in communication in a replicable and systematic manner. Content analysis has been widely used in information systems research (Hassan & Mathiassen, 2018), and we will follow the guidelines proposed by Gläser-Zikuda.(Gläser-Zikuda et al., 2020) And Guo (Guo, 2019). We used NVivo 14 Plus and a worksheet to perform our content

analysis. The literature on document analysis offers multiple methodologies for examining policy documents at the macro and micro levels, proposing several approaches and frameworks of a qualitative nature.

This study leverages qualitative content analysis using thematic coding to empirically explore the features and components of compliance policies in a subset of healthcare organizations. Using a deductive approach; each policy will be evaluated using a pre-determined codebook based on available research and government and industry guidance. (Kibiswa, 2019, p. 2061) Based on policy features defined by Kuserrow (Kusserow, 2013) and policy components defied Carboni (Carboni, 2022), a baseline code book was defined that incorporates guidance from the U.S. Department of Health and Human Services and U.S. Sentencing Commission on the features and components of compliance policies and an overall compliance program to evaluate the content of the sample documents. This codebook was based on a review of existing literature; the codes were then added to N-Vivo to establish the hierarchy of the codes, as some of the codes are subcodes of other codes, as would be the case for compliance document features and components. Each file was loaded in N-Vivo as an individual case; in parallel, the documents were exported into Word format to obtain document word counts. A Microsoft Excel Worksheet was used in parallel to capture document features and components and other document properties like format, title, delivery medium, number of pages, and number of words. Microsoft Excel functions were used to calculate averages, minimum and maximum number of pages, median page count, and geometric mean.

Once the initial codebook based on existing literature was completed, the primary author evaluated the compliance documents to ensure they covered the identified features and components.

2.4 Results

An initial examination of the collected compliance documents presents a complex picture of how different organizations approach the topic of compliance. Document length and content varied widely, from as short as four pages to 206 pages, and content varied from descriptive to prescriptive. The average length of the compliance documents was 30 pages, the median was 18 pages, and the geometric mean calculated using Microsoft Excel was 17.7 pages. On average, each document contained 4,171 words, with a minimum and maximum word count of 763 and 59,131 words, respectively.

Given the varied complexity of the documents, it can be inferred that some individuals may struggle to navigate them. Using and including definitions could help mitigate some of the difficulties an individual might have with the documents. Only a handful of the documents set any expectations for the document's expected expiration or revision date, making it unclear as to the document's durability. Out of the 33 organizations examined, only two compliance documents provided future data when a revision should be completed; it is possible that a larger sample size could yield different results. The titles of the documents also showed some variation in the names used for the titles. On the sample, the most common words in the title, besides 'compliance, ' were 'Plan' (11 instances), followed by 'Program' (9 instances), 'Policy' (8 instances), and then 'Training' and 'Manual' (2 instances each). None of the collected documents fully implement the expected features and

components described by Kusserow and Carboni. The lowest instance was key performance indicators at 15%. In over 90% of the organizations examined, the compliance documents reviewed included duties and responsibilities as a feature at 91%. Policy statements and procedures, which were the most common components at 91% and 94%, respectively, the component with the lowest number of instances was the header block as a unit at 12%, although its components fared much better within the document with the statement if it modifies or replaces an existing policy at 24% and Department accountable for policy on the higher end with 61%. Only about 15% of the organizations included 70% or above of the features and components recommended in the selected literature, with 73% at the low end and 82% at the top end of the organizations. About 36% of the organizations' compliance documents contained between 50% and 70% of the expected features and components, with 42% of the documents included between 30% and 50% of the expected features and components. Seven percent (7%) of the organizations' compliance documents contained less than 30% of the expected features and components. Compliance documents were either part of a group of documents that serve to document policy and procedures or, in some instances, an all-encompassing document that mixes policy with procedures, merging the descriptive with the prescriptive in their compliance program.

The following tables summarize the features and components of the compliance documents examined and the coverage of the features and components.

Features	Number of Documents	%
Defines duties and responsibilities	30	91%
Training program description and requirements	24	73%
Define the program's overall operation, reporting requirements, how investigations will occur, corrective responses, issue management, continuous evaluation, and auditing.	29	88%
Duties and responsibilities for each area of the organization	25	76%
Description of how interdepartmental interactions shall occur between compliance, audit, operations, legal, and human resources.	14	42%
Key performance indicators of program effectiveness	5	15%

Figure 1 Compliance Document Features Coverage

All the compliance documents examined were available electronically in PDF format. Some were available in print; however, the documents pointed to an electronic version that readers were advised took precedence over the printed version. Two of the compliance documents were available as web pages, and four were delivered as a slideshow presentation intended for use during a compliance training session. The compliance documents were unambiguous in establishing duties and responsibilities across the organization, from the top down, with clearly defined guidelines and expectations.

Another area of focus in the documents was policy statements and procedures. Policy statements served to establish and reinforce expectations from the organization to its stakeholders in matters related to compliance. The inclusion of procedures illustrates the prescriptive nature of the documents in guiding the actions of the organization actors.

About 39% of the compliance documents examined included a purpose section. Purpose sections emphasize the organization's goal to achieve and maintain compliance with applicable laws and regulations and its ethical requirements. Some organizations' purpose sections spoke about compliance in general terms, while others explicitly listed the relevant laws and rules that the program was designed to support.

At 46%, the organization's Scope was included as one of the components of their compliance documents. For some organizations, the scope followed guidance from the U.S Sentencing Commission; others established the extent of their audit program; in some cases, the scope was defined as who was covered under the compliance document.

Components	Number of Documents	%
Header block	4	12%
Title	33	100%
Department acountable for policy	20	61%
Effiective date	17	52%
Policy identification number	9	27%
Approval Date	14	42%
Approving authority	16	48%
Statement if it modifies or replaces existing policy	8	24%
Number of Pages	10	30%
Background	6	18%
Purpose	13	39%
Definitions	14	42%
Scope	15	45%
Policy Statements	30	91%
Procedures	31	94%
Related Policies	12	36%
Refernces/Citations	22	67%

Figure 2 Compliance Document Components Coverage Summary

Features and components sample summary	
Average # of Features Coverage	4.85
Average % Features Coverage	69%
Median # of Features	5.00
Median % of Features	71%
Geometric Mean # of Features	4.61
Geometric Mean % of Features	66%
Average # of Components Coverage	8.30
Average % Components Coverage	52%
Median # of Components	8.00
Median % of Components	50%
Geometric Mean # of Components	7.83
Geometric Mean % of Components	49%
Average Number of Words	8313.3
Minimum Number of Words	763.0
Maximum Number of Words	59131
Median Number of Words	4820
Geometric Mean of Number of Words	4821.8
Average Length in Pages	30.5
Minimum Number of Pages	4
Maximum number of pages	206
Median Number of Pages	18
Geometric Mean Number of Pages	17.8

Figure 3 Features, Components, and Document Properties Sample Summary

2.5 Discussion

This study aimed to conduct empirical research on compliance documents in healthcare organizations. Using Carboni (Carboni, 2022) to define the features of compliance documents and Kuserrow (Kusserow, 2014),Carboni informs the evaluation of compliance documents to answer the first research question, "What are the features of compliance documents?" The examined documents varied in length from two to over two hundred pages. This high degree of variability is due to choices made by organizations in drafting these documents. Some organizations preferred what appears to be a single document that combines policy, planning, and procedures versus other organizations that opted for drafting multiple smaller documents. The validity period of about 2-5 years for the documents might point to some risk in the documents themselves, as it could put the organization at risk of

operating with obsolete documentation, thus increasing their chance of failing to maintain compliance. The literature is unclear on an appropriate validity period for such documents; however, it agrees that documents should be reviewed periodically for relevance and to incorporate any updates to applicable and new regulations and related changes. The results of the sample might indicate that a larger document would require more effort to update, hence the longer validity periods to account for the larger undertaking that is required to update the document. Duties and responsibilities as the most common feature is not surprising as one of the main goals is to influence the actions of the organization through the actions of the individuals who comprise said organization. Clearly established duties and responsibilities improve the chances of the organization eliciting the desired behaviors, thus reducing its risk of non-compliance. Following duties and responsibilities, reporting requirements were stressed throughout the examined documentation. The non-compliance risks require robust reporting and documentation to successfully demonstrate that the appropriate controls have been implemented and are working as expected or document deficiencies uncovered and the remedial action taken to bring the organization back into compliance.

It was surprising that none of the organizations examined for the study included any feature in their compliance documents regarding interdepartmental interactions and key performance indicators. In the case of interdepartmental interactions, it might be that the complexity of defining such interactions might have proven challenging to document. The lack of key performance indicators was also surprising; organizations might have chosen to leverage key performance indicators outside of compliance documentation. This makes sense from an operational standpoint since key performance indicators serve as markers to measure the health

of the program and are tactical vs compliance documents that are more focused on policy and procedures.

The second part of the study examined compliance document components. The most widely used components described by Kuserrow (Kusserow, 2014) Policy Statements and Procedures provide insights into the aim of said documents. Through policy statements, the organization clearly communicates expectations and goals regarding its policies and procedures. Other common components of the policies, like definitions, aid in establishing a common language, and declaring the department accountable for a policy ensures that those tasked with maintaining and updating policy are clearly identified and held accountable for the necessary evolution of the documentation to respond to an ever-changing regulatory landscape.

In the organizations that comprised the sample, there was significant variability in the scope of the documents themselves. Some documents were short and meant to be used as a reference. Other documents were comprehensive and combined policy, procedures, and other guidance like a Code of Conduct and supporting prescriptive guidance. Some documents were clearly drafted for use in a training setting to educate employees and other stakeholders. Duties and responsibilities for each documented position provided clear and actionable guidance on the expectations of the organization of each individual when it comes to compliance activities. When considering the aim of a compliance document is to influence the actions of the individuals in the organization, clearly establishing duties and responsibilities is key in eliciting the expected response. Some of the duties and responsibilities in the compliance documents were presented in paragraph form, while others were presented in bullet or list format. The format might help drive

adoption, as organizations aim to provide the necessary guidance in a friendly format to maximize understanding and retention.

2.6 Conclusion

This study provides empirical evidence on the implementation of features and components of compliance documents in the field, examining compliance documents from 33 healthcare organizations. This study contributes to the literature by collecting empirical evidence of the use of compliance document features defined by Carboni and compliance document components defined by Kusserrow. (Kusserow, 2014). By understanding the contents of compliance documents, organizations can identify areas of their documentation that could benefit from a review and implementation of additional best practices, ultimately helping them achieve their goal of attaining and maintaining compliance with applicable laws and regulations. Uncovering how compliance documents on the field are drafted and maintained can provide insights to organizations on what best practices might be missing from their compliance document repertoire. This could help organizations target their efforts to ensure compliance documents are drafted to maximize their effectiveness.

A limitation of this study is the number of organizations and documents examined. Although it is considered sufficient for the insight it produces, a larger dataset can provide a richer one.

The study is also limited by its focus on one sector, namely healthcare, and one country, primarily the United States of America. This excludes other organizations, sectors, and territories, thus excluding how other regulated environments approach compliance documents, their features, and components.

Future avenues of inquiry include comparing the results of this study with a larger sample. Dig deeper into the features and components that appear less frequently in the sample and validate whether they are not considered as important for an organization as they are from a literature standpoint. Considering that other sectors and countries can also provide additional insights into what can be generalized across industries when it comes to compliance documents and best practices. Enhanced compliance documents could help organizations mitigate their compliance-related risks by considering the approaches of their peers in their documentation. A potential case study or multiple case study of how an organization responds to a compliance requirement could also provide insights into how the application of compliance documentation is operationalized in the actions of the organization's individual actors. This could contribute to reducing the gap between theory and practice, benefit both practitioners and enrich the literature on compliance documents.

Chapter 3: Managing Compliance, Information Security, and Risk in Health Care Organizations

3.1 Introduction

Organizations face a complex and constantly evolving regulatory environment. In the United States alone, it is estimated that in 2022, approximately $3.079 Trillion dollars (in 2023 dollars), or about twelve (12%) of the Gross Domestic Product, is spent on compliance activities. (Trebbi et al., 2023) The significant number of resources invested in those activities are expected to materially impact how the organization operates and evolves to comply with said regulations. In the same operational environment, the importance of information systems when they become unavailable, as would be the case when they are under attack. The cybersecurity firm NordLayer, since the year 2004, has approximately 16.5 billion accounts that have been breached. (*12 Most Significant 2023 Data Breaches | NordLayer Blog*, n.d.)

The banking, retail, government, and healthcare industries are under constant assault from those who seek to steal their data for financial gain. Examples of systems risks include ransomware, Distributed Denial of Service (DDoS), and malware. According to some estimates, cybercrime costs the world economy billions or even trillions of dollars annually. According to the latest IBM Security/Ponemon Institute report, the average cost of a data breach is $4.45 million dollars per incident. Ransomware attacks continue growing at an alarming rate, reaching up to one every 12 seconds in the United States alone, affecting individuals and organizations large and small. (Wertheim, 2020)

These significant changes in the cyberthreat landscape are happening against substantial increases in the number of external regulations organizations are expected to comply with (citation). External regulatory compliance activities have substantially increased the resources devoted to external regulatory compliance activities. New European regulations (e.g., General Data Protection Regulation-GDPR) and the United States (e.g., New York Shield Act, California Consumer Privacy Act) have placed additional stress on the organization by diverting resources and personnel to regulatory and compliance activities.

Through an increased focus on information systems risk management, organizations aim to contain the effects of data breaches and cyberattacks and the corresponding impacts on their operations and reputations. Organizations must seek to meet the requirements of compliance with those of information security risk management. This interplay between compliance and information security risk management presents a dichotomy akin to two sides of the same coin. On one side, understanding how an organization employs its resources to address its information security risk management and compliance requirements can help practitioners with insights on how to address those challenges in their organizations. For information security risk management or compliance requirements, often the same staff and system(s) are impacted by those requirements. Some might be inclined to think that performing information systems compliance tasks is equivalent to performing risk management. Click or tap here to enter text. Although compliance carries a risk component, compliance, and risk management differ in the organizational context. Kusserow (Kusserow, 2020) defines the difference between the two as follows: “Risk management identifies, assesses and seeks ways to mitigate them whereas compliance focuses on meeting established rules, regulations, and standards to

prevent their organization from regulatory and legal violations that could give rise to serious liabilities. Information security risk management and compliance draw on complementary but different sets of skills. When addressing risk, you are identifying and quantifying potential threats to the organization to devise and implement controls to mitigate the impact of those risks.

Additionally, the organization might prepare for those “unknown unknowns” to build a resilient organization. Similarly, as a composer with a blank sheet of musing creates a melody and a cadence and selects what instruments to write music to, a risk manager gathers risk information and builds a set of controls to help mitigate the identified risks to the organization. An organization's risk management process helps with understanding its risk environment and deciding whether to pursue the recommended controls or if the risk is within the organization's risk appetite and can be accepted. Conversely, compliance comes with its own “sheet of music” where a regulation’s requirements provide the melody, cadence, and instrument parts, leaving only how to approach the interpretation of the piece. Laws and conditions are established by regulators and interpreted by those implementing the regulations and internal and external audit staff examining compliance with the code. Organizations analyzing regulations and identifying and defining the controls that will address the rule within the organizational context hinges on interpreting the required controls by the organization. To continue the musical analogy, the compliance practitioner interprets this sheet of music the same way a musician plays a sheet of music in front of them with their instrument.

The other side of the coin explores how we could describe, according to theory, how an organization responds to the institutional complexity brought upon by internal resource pressures and external institutional pressures. Thus, the research

question is: How does an organization manage information security, risk management, and compliance? What strategic and tactical responses does the organization leverage to manage information security, risk management, and compliance?

The aims of this research open some exciting lines of additional questioning. How does the organization handle conflict situations where information security and compliance requirements compete for the same resources? The strategies or tactics organizations choose to employ might provide insights into how organizations respond to attain/maintain their legitimacy and ensure their long-term viability. (Oliver, 1991). This research project explores the mechanics of the process organizations use to choose and carry out a strategic or tactical response, considering that there might be competing external requirements. This study aims to address a gap in the literature by providing empirical insights into the decision-making process followed by organizations and their responses when dealing with regulatory compliance and security risk requirements. This dynamic creates an environment where regulatory compliance and information systems risk management requirements can cause resource and operational competition when both impact the same organizational systems or resources.

This study takes an integrative approach to studying the research questions, utilizing research from two streams of literature: strategy and information security. Theoretically, the case study explores how the organization responds to organizational pressures through strategic and tactical responses, as presented by Oliver (1991) (Oliver, 1991). An organization must choose a response to external pressure(s) using an array of strategies and tactics that guide how it acts upon the requirements of said pressures.

Oliver (1991) highlights the organization's strategic and tactical responses to institutional pressures, defining the “How” in the way that the organization responds to external and internal pressures. Empirically examining how an organization responds in the form of its processes in action provides insights into how an organization responds to said institutional pressure(s) and what strategies and tactics are most favored in regulated environments in the context of information systems risk management and compliance activities.

The direct answers to the research questions provide valuable insights into how the organization managed the process of implementing compliance and information security risk management. The strategies and tactics leveraged by the organization in the study can be used by scholars and practitioners to build on our understanding of how an organization can optimize resource allocation to balance the requirements of information security risk management and compliance.

The following section provides a high-level literature review, followed by a case study methodology. Results, discussion, and a conclusion with suggested future research work complete the section. A more comprehensive literature review is presented in Chapter 2 of this dissertation.

3.2 Literature review

Organizations do not operate in a vacuum; they are subject to the push and pull of internal as well as external expectations from a wide array of stakeholders. These external influences can take the form of compliance requirements imposed by government regulations or the expectations of external stakeholders like sponsors of a non-governmental organization engaging in onerous audit and reporting schemes

(Cazenave & Morales, 2021) or shareholders (Min et al., 2022) seeking proactive governance processes. (Dimaggio & Powell, 1983) (Min et al., 2022; Oliver, 1991)

Previous research has provided some examples of the influence of external pressures on individual actors. (Arnold et al., 2007; Barton et al., 2016) Opening the door to exploring the organizational processes that handle operationally addressing the requirements of compliance and information systems security risk. Given the constraints on organizational resources, organizations must creatively address their specific compliance and information security risk requirements. Oliver (Oliver, 1991) Provides a robust framework for understanding how organizations respond to these institutional pressures through the strategies and tactics deployed in their responses. Oliver's theory categorizes organizational responses along a continuum from passive compliance to active defiance. This theoretical framework is particularly useful for analyzing the driving forces behind organizational change or the tendency to remain static, as articulated by Hu, Hart, and Cooke. (Hu et al., 2007a).

Central to this perspective is the recognition of the human element in organizational behavior, especially in the realm of information systems security. Oliver's framework adeptly connects the technical and human elements, which is crucial for developing comprehensive strategies for information systems security, as supported by the works of Bjorck (Bjorck, 2004), Dhillon & Backhouse (Dhillon & Backhouse, 2003), and Hu (Hu et al., 2007a). The contemporary organizational landscape is fraught with numerous risks, both operational and reputational. Technological advancements have amplified these risks, as organizations now operate on a global scale, increasing their exposure to cyber threats. This phenomenon is extensively discussed by Hsu, Lee, and Straub (Hsu et al., 2012b),

who highlight the complexities introduced by technology in managing organizational risks.

The relationship between regulatory compliance and information security risk is a critical area of study. Hsu, Lee, and Straub (Hsu et al., 2012a) present a compelling case for a Neo-institutional theory-based framework to understand how institutional changes influence information security practices. Their research underscores the significant impact of regulatory compliance on the implementation of information security management policies, which has profound implications for both policymakers and practitioners. Spears, Barki, and Barton (Spears et al., 2013) delve deeper into the connection between regulatory compliance and information security. They argue that regulations often arise from identified security issues and threats, which then become institutionalized, affecting the implementation of information security measures within organizations. This cycle is particularly relevant in the context of an increasingly interconnected and globalized world, where regulations have cross-border effects, influencing practices beyond national boundaries. The work of Kam, Katerattanakul, and their colleagues ((H.-J. Kam & Katerattanakul, 2013, 2014) provides insights into how compliance and information security are managed across different industries, particularly banking and higher education.

Oliver's Strategic Responses to Institutional Pressures

Oliver's framework, as outlined in Oliver (1991), categorizes the ways in which organizations address both external and internal pressures into five broad strategic responses, each supported by specific tactics. The first strategy, **Acquiesce**, is characterized by a passive compliance approach. Here, organizations might rely on ingrained habits, where compliance becomes an unconscious part of the

organizational culture. They may also imitate the practices of other organizations or engage in deliberate compliance efforts to meet regulatory demands.

The second strategy, **Compromise**, involves a balancing act between conflicting pressures. Organizations adopting this approach aim to accommodate the needs and demands of various stakeholders by finding a middle ground. This can involve balancing competing interests, pacifying stakeholders through minimal conformity, or bargaining to secure concessions from regulatory bodies.

In contrast, the **Avoidance** strategy is about evading compliance altogether. Organizations might hide their non-compliance through concealment, create buffers to avoid external audits or inspections, or even escape from regulatory environments where the cost of compliance outweighs the benefits.

The fourth strategic response, **Defy**, is a more confrontational approach where organizations actively resist compliance. This resistance can take the form of dismissal—simply ignoring regulatory requirements—challenging these requirements, or outright attacking the value and legitimacy of the compliance demands.

Finally, the **Manipulate** strategy involves a proactive effort to shape the regulatory landscape to the organization's advantage. Tactics here include co-opting regulatory bodies by incorporating their representatives within the organization, lobbying to influence policy-making, and even establishing control over regulatory interactions to dictate terms.

Understanding these strategic responses provides valuable insight into how organizations manage compliance and risk. It highlights the diversity of approaches available—from passive acceptance to active resistance or even the reshaping of the

regulatory environment—depending on the organization's goals and the pressures it faces. (Oliver, 1991)

Understanding what strategic responses an organization provides valuable insights for organizations striving to manage compliance and risk effectively. A substantial body of knowledge about compliance and compliance activities revolves around information security and information security policies. This highlights the essential interplay between organizational compliance, information systems, and risk management. Compliance has significantly influenced how information systems are built, deployed, supported, and protected. Regulatory requirements must be integrated into implemented systems to avoid noncompliance and its negative repercussions. Contemporary literature on compliance often focuses on topics such as adoption and adherence rates, strategies to influence adherence to policy, and the importance of education and training. Other research areas investigate the extent to which specific policies are followed and explore the reasons behind compliance or non-compliance.

Daljord et al. (2023) proposed an approach to targeted promotions within a hotel rewards program to encourage compliance. Through a field experiment, they demonstrated that strategic promotions could achieve desired compliance outcomes. (Daljord et al., 2023, p. 887). This is in line with the interest in how compliance can be influenced to the desired outcomes. Kuiper (Kuiper et al., 2023) Leveraged a network approach to understand how individual compliance might be influenced by a network of variables. This approach combines theoretical frameworks rooted in behavioral and social sciences to provide insights into the complex system of factors affecting compliance. (Kuiper et al., 2023, p. 493).

Lee (2021) utilized social exchange theory to explore how businesses balance their compliance efforts with tax laws based on the perceived value of government services. Firms temper their compliance efforts based on the fairness and value assigned to this exchange. (Lee et al., 2021, p. 203).

Wu and van Rooij (Wu & van Rooij, 2021) Examined the relationship between individual values and compliance with information security policy requirements. They found that personal values significantly influence compliance behavior, highlighting the difference between compliant and non-compliant actions. (Donalds & Barclay, 2022, p. 71).

There remains an opportunity to understand the underlying processes, antecedents, and artifacts that either provide the foundations for a compliance program or foster an environment conducive to a compliant, ethical organization. Industries such as financial services and healthcare have seen a shift from a compliance-first mentality to a balanced approach that includes risk management. New threats like ransomware, data breaches, and third-party risks have made way for new strategies to address regulatory requirements and manage emerging risks. For a more comprehensive overview of the literature please refer to Chapter 2.

3.3 Research Design

The selected methodology is that of a case study of implementing a regulatory requirement at a Children's Hospital System in North America. The case study is particularly effective for exploring "how" questions due to its descriptive nature (Yin, 2013). A single case study was conducted on a medium-sized Children's Hospital System with locations in multiple states in the United States. I have a professional relationship with the hospital, which facilitates access to the informants. The hospital

provides a fertile environment for my research on implementing information security risk management and compliance. During the study, the Hospital addressed the requirements of several initiatives that had a dependency on practically the same set of resources in the organization. This created a situation that could potentially create duplicate efforts amongst several projects with the same underlying technology, multi-factor authentication. The organization had started the evaluation of a solution to enable the issuance of Electronic Prescriptions for Controlled Substances according to Drug Enforcement Administration (DEA) regulations. During the testing of the DEA-EPCS, additional requirements were identified as the result of a Payment Card Industry-Data Security Standard (PCI-DSS) audit and as part of an internal evaluation of the organizational security posture conducted by the Chief Information Security Officer. Part of those requirements also involved the deployment of a multi-factor authentication solution to strengthen the security posture of the organization and to address several findings from a PCI-DSS audit.

3.3.1 Research context

The United States Drug Enforcement Administration (DEA) issued the regulatory requirements to allow healthcare organizations to issue Electronic Prescriptions for Controlled Substances (EPCS). This regulation provided the rules required for healthcare organizations to be able to deliver electronic prescriptions for controlled substances. The ability to leverage electronic means to deliver prescriptions for controlled substances opened new avenues to reduce the time and documentation efforts required to deliver controlled substance prescriptions to patients using electronic means like pharmacy exchanges and electronic health records systems. To comply with this new regulation and to provide additional value

to telehealth patients, an identity validation and authentication solution was implemented at the Children's Hospital system at the center of the case study. This implementation provides an excellent opportunity to examine an example of a regulatory compliance requirement and explore how the organization responds to said requirement and the context of such a response.

During the case study, a new Chief Information Security Officer (CISO) was appointed at the hospital. The Board of Directors tasked the CISO with evaluating the organization's risk footprint. The CISO reviewed the hospital's current environment, established a baseline, and developed a plan to address uncovered vulnerabilities. One initiative involved picking up a previous security technology implementation project that had been dormant for some time. Still, it should be able to provide a solution to ameliorate some of the identified risks within your infrastructure and provide a good starting point. The CIO then points out that one of the groups within the IT Department is about to start a project that will implement a solution with similar functionality to address a regulatory requirement for the electronic prescription of controlled substances. In parallel, the operations department informs of the findings of a recent Payment Card Industry Data Security Standards (PCI-DSS) audit, which has requirements that must be implemented to comply with a tight deadline so as not to impact the hospital's ability to accept and process credit card payments. Addressing those recommendations is central to retaining the ability to process credit and debit card payments from patients. This creates a situation in which the proposed solution to the audit findings would require another system with similar functionality to the one already being tested to address the Drug Enforcement Administration – Electronic Prescriptions for Controlled Substances (DEA-EPCS). Adding to the concerns, a slew of high-profile data

breaches at other hospitals, insurers, and other healthcare industry players makes board members nervous about the organization's security and request constant updates on what steps are being taken to manage and minimize the organizational cybersecurity risk footprint.

The situation experienced by the hospital during the case study is not that different from the experience of Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) in regulated environments. Regulated environments like those of financial services, higher education, and health care have the requirement to comply with often complex government-imposed regulations. The complexity of understanding and implementing those regulations has given rise to internal organizations solely dedicated to compliance (DiMaggio and Powell, 1983; Freeman, 2007; DeMott, 2013). At the same time, the complexity and breadth of Information security risks caused by increased operational use of information technology have elevated the profile of Information Security (Kam, Katerattanakul, 2014).

An organization’s regulatory requirements and its own security risk footprint can often be at odds and competing for the same attention and resources. In organizations, operational separations or silos between business functions, like information security and compliance, could also create an environment where the same tasks could be duplicated. This could lead to inefficient use of resources and decreased effectiveness in appropriately managing the organization's overall risk and compliance footprint.

3.3.2 Data Sources

The primary source of qualitative data used in the study was semi-structured field interviews. (Albrechtsen, 2007; Hsu et al., 2012b; Trochim & Donnelly, 2008) of hospital personnel and consultants working with the organization (Argyris, 1958; Hu et al., 2007a; Williams et al., 2013). The participants are selected to provide a cross-section of the participants in the implementation of the information risk management and compliance activities as part of the information systems management function of the hospital. Participants included front-line business analysts, technical security resources, middle managers, consultants, and senior executives. Primary informants include resources directly involved with the DEA-EPCS project as well as resources that could provide insights into the organizational context of information systems risk management and compliance activities. Primary informants include resources directly involved with the DEA-EPCS project as well as resources that could provide insights into the organizational context of information systems risk management and compliance activities.

Eleven interviews were conducted with hospital and provider informants, with an average interview duration of 40 minutes. The informants included front-line analysts, administrators, middle management, senior technical resources, and executives like the Chief Information Officer and the Chief Information Security officer. The interviews were transcribed and coded using thematic coding based on two coding guides. The first coding guide used several research questions to uncover insights on the process(es) the organization leveraged to balance information security risk management and compliance. The other coding guide was developed based on Oliver's strategic and tactical responses. (Oliver, 1991) Both

coding exercises followed a deductive approach to analyze the information based on the defined code books.

Primary informants for the case study are presented in Table 1.

Table 1. Interviewees and duration of each interview

Role	Description	Interview Duration (minutes)
IT Operations Manager	Responsible for the initial implementation and testing of the strong authentication project.	59
Information Security Architect	Responsible for the day-to-day operation of the solution and providing guidance on security policies related to the implemented solution	57
Technical Security Architect	One of the initial advocates for the solution and provided support for the solution definition	46
Information Security Manager, risk and compliance	Resource in charge of policy regarding risk management and regulatory compliance within Information Security	45
Medical Informatics Senior Analyst	Performed user acceptance testing of the solution and provided feedback during the requirements phase	55
Compliance Analyst	Provided context on the compliance environment	22
Internal Audit Manager	Internal audit and data analysis group	
Implementation Consultant – Project Manager	External consultant providing Project Management services from the solution vendor	30
Implementation Consultant – Technical Consultant	External consultant providing technical services from the solution vendor. Involved in gathering requirements, documenting, and managing the implementation of the final solution	19
Chief Information Officer	Senior Executive leading the information technology team system-wide	60
Chief Information Security Officer	Senior Executive leading the Information Systems Security operations system-wide	55
Total Interviews: 11	Average interview duration: 40 minutes	

3.3.3 Case Study Design

The initial exploration of the research questions was a Case study. The Case was a medium-sized children's hospital based in the United States with locations across multiple states. The reason the case was chosen is two-fold. First, the principal researcher has worked for several years with the organization providing consulting services, and second, regulated industries like health care are at the center of the research questions to be studied. A hospital is a good example of a

highly regulated environment subject to the pressures of externally mandated regulations and other requirements.

The use of the case study as a research strategy is consistent with Eisenhardt's view that such an approach "focuses on understanding the dynamics present within single settings." (Eisenhardt, 1989, p. 534) The primary source of qualitative data takes the form of semi-structured field interviews (Albrechtsen, 2006; Trochim and Donnelly, 2008; Hsu, Lee, and Straub, 2012) of hospital personnel and consultants working with the organization (Hu, Hart, and Cooke, 2007, Williams, Hardy and Holgate, 2013; Argyris, 1958). The interviewees are selected to provide a cross-section of the participants in implementing the information risk management and compliance activities as part of the information systems management function of the hospital. Informants included front-line business analysts, technical security resources, middle managers, consultants, and senior executives. The interviews focused on understanding the organizational environment and processes around organizational responses to recent regulatory changes with an impact on an Information security component in exploring the research questions. The semi-structured interviews were facilitated using an interview guide consisting of 13 questions. The questions were related to the research questions and aimed to capture organizational insights around:

- Organizational influences
- Governance of Information Systems Requirements
- Compliance and Information Systems Risk Management Requirements
- Identifying challenges between information risk management and compliance requirements

- Resolving the challenges between compliance and information risk management

Each interview aimed to capture a deeper understanding of the user experience and knowledge of the compliance and information systems risk management processes within the organization. Each informant interview was recorded through electronic means and submitted to a transcription service for transcription. All interviews were conducted between native English speakers, reducing the introduction of deviations due to translation issues of discussions of information technology-related topics. The number of informants was chosen for practical reasons and to achieve theoretical saturation. The object of this study was to capture insights into how an organization works through addressing regulatory requirements with the goal of determining the strategies and tactics in the theoretical context of Oliver's Strategic Responses to Institutional Processes. (Oliver, 1991) Another way to describe how to select the number of informants can be found in Kvale (1996) – “interview the number of persons that are needed to find out what you need to know.” The number of informants required should be enough to achieve “theoretical saturation.” (Albrechtsen, 2007, p. 278; Strauss & Corbin, 1998, p. 292). In practical terms, the researcher should aim to maximize the collection of data within the operational and practical constraints in which the research takes place until no additional data of significance can be obtained or any additional data would be of limited impact. Due to circumstances outside of the investigator’s control, additional access to additional informants is not available currently. However, based on the analysis performed, theoretical saturation is present in the data collected. The informants interviewed for the study provided general insights that resulted in some general patterns with little difference between the informants.

3.3.4 Analysis strategy

The analysis of the interview data followed a thematic coding approach. (Boyatzis, 1998) using a deductive approach based on strategic responses and tactics (Oliver, 1991). For the analysis of the interview data. The interview questions were designed to identify the organizational environment and seek answers to the research question: How does an organization manage compliance and information security risk management?

Once all the interviews were collected and transcribed, they were analyzed using the NVivo Plus version 12 content analysis software package. Each individual transcript was loaded into the software package, and several coding processes were used to analyze the interviews. The first coding of the interview transcripts was conducted using the thirteen (13) questions contained in the semi-structured interview artifact. This artifact was created to guide the questioning of the informants and gain insights into the organizational environment by tracing back external processes as well as the internal processes that occur in response to said processes. Questions one (1), two (2), and three (3) were designed to identify examples of the external organizational influences affecting the environment. Questions four (4) and five (5) were designed to identify what information systems governance mechanisms are present in the identification and prioritization of requirements. Questions six (6) and seven (7) were aimed at understanding what the organization deemed their top sources for information security risk management and compliance requirements. Questions eight (8) and nine (9) attempted to uncover how the organization assigned priority for information security risk management requirements vis-à-vis compliance and how the assignment of resources is handled. Questions ten (10) to thirteen (13) explore the processes and the governance

structures that help harmonize resource assignment and decision-making. The semi-structured interview analysis artifact is included in Appendix A. A researcher conducted independent coding of the interview data of two interviews to be compared with the coding completed by the primary researcher.

A secondary analysis focused on the identification of strategies and tactics performing thematic coding using the constructs for strategic and tactical responses as defined in Oliver. (Oliver, 1991). (See Appendix B) Both analyses made use of a deductive approach to the data, using the prepared codebooks as the basis for the analysis.

The use of a single case is not enough to establish generalization and thus is not one of the aims of this research. The goal is to identify best practices in an organization that others in a similar situation could leverage when addressing compliance and information systems risk management issues within a similar regulatory and organizational environment. I also recognize the limitation of the external validity of this initial single-case approach. However, I believe that it should be enough if theoretical saturation is achieved. Nonetheless, further research will be needed to provide additional empirical data and expand on the applicability across organizations and other highly regulated industries beyond health care like financial services or across national boundaries.

3.4 Results

Like any other organization, the hospital is subject to several forces that exert push and pull effects on its operations. Compliance with local, state, and federal regulations requires the organization to devote considerable resources to collect, maintain, and report on compliance activities. Beyond government-imposed

requirements, the organization needs to contend with industry requirements, such as compliance with the Payment Card Industry – Data Security Standard (PCI-DSS), to retain the ability to accept and process credit card payments. This also enables them to maintain a cybersecurity posture that allows them to obtain and maintain cybersecurity insurance at reasonable rates.

During my exploration of the black box of what happens in the area between the pressures and the responses, several overarching and narrow governance processes emerged. Such processes come into play in decision-making when responding to external pressures. One important governance process in the organization studied is centered around communication and how it can avoid conflict. The CIO provided the following example.

> *"There might be a specific department who's trying to do something, but then they may not realize the impact back to Payroll or to the scheduling department or what occurs. Having a group in (inaudible) IT in the Hospital, which has an enterprise view that can see things across the side boundaries, is very helpful. Because as integrated as we are in our electronic environment, it's also crucial that we implement perspective. If we were to change one thing at a site like [Site A], it could also impact [Site B], who are not aware of those enterprise requirements as we build our electronic environment to be as highly integrated as it is."*

It is a way that certain silos can be breached, and information can flow throughout the organizational units (Mignerat & Rivard, 2009, Scott, 2014). Working together, although in different manners, they impact the organization and impact its decisions. (Mignerat & Rivard, 2009). This could readily translate into a direct threat to organizational survival, for example, in the case of a hospital that loses its license to operate due to failure to comply with regulatory requirements. We can see the organization studied is heavily influenced in this area by several regulatory bodies in government as well as industry, exemplified by HIPAA and PCI-DSS. Such external

influences remain top of mind as informants often referenced them during our interviews, as exemplified by this quote from the compliance manager:

> *"HIPAA is the main platform, the main set of requirements. HIPAA is not a very prescriptive type of requirement because our organization is not publicly traded, so we do not have [Sarbanes Oxley]. We do accept credit card payments, the payment card industry [data security standard], for that part of our information, that has to be taken into consideration."*

The consideration given by the organization to these external pressures makes them the most consequential in the short term, as they are always top of mind and have been socialized as a priority, thoroughly communicated throughout the organization. A strong compliance culture reflects the organization's ingrained commitment to adhering to regulatory requirements within a regulated environment. The priority given reflects the potential impact of regulatory fines, as well as the continuity of the operation. Such importance could be related to their relative short to medium-term impact, both positive and negative. A constantly evolving regulatory environment makes it imperative that the hospital and its staff stay up to date with changing requirements and work collaboratively to remain compliant.

Informants clearly identified that the organization heavily relies on the experiences of their peers through direct information exchange or participation in various professional and industry organizations. The organizational emphasis on "not reinventing the wheel" resonates as they leverage the experience of their peers to avoid pitfalls and engage in shared best practices when evaluating and implementing any new requirements or improving existing processes (Jeyaraj & Zadeh, 2020).

The Chief Information Officer's comments regarding those external pressures provide an overview of the operating environment and the forces that operate within it:

> *"You know, HIPAA is the one that most people jump to in healthcare, and it's the biggest and probably the most known. There are plenty of others; PCI-DSS, regulatory issues, and the payment cards industry are other ones that we must adhere to, as we take credit card information, and that's a pretty strict compliance requirement on the PCI world and how we handle that data. Even down to how quickly we reset passwords or what those requirements are for those users directly. Obviously, we're working with the HID implementation, the DEA, and drug (Drug Enforcement Agency – Electronic Prescriptions for Controlled Substances) related to the way we prescribe medication and, especially, controlled substances. Also, it influences how we build and interact with our partners, what we can and can't do, you know, at a federal level. Then you get in the state issues in being in five states. We have five different issues we have to deal with."*

The Chief Information Officer's comments illustrate how external organizational influences come from multiple directions, with several jurisdictions and compliance levels required. These influence the organization and its operations through the controls, tasks, and process changes required to be implemented to achieve and maintain compliance. He comments further that the dimension of operating within different jurisdictions also adds to the complexity of its operating environment:

> *"Positions are licensed by the state practitioners, which bring a certain amount of rules related to how those positions or practitioners can and what they can do within the state. And it also affects how we operate the business, (inaudible) an example, highly, it's easy to use, and it's highly integrated right now, especially in this time of crisis, but, (inaudible) rules vary state by state, you can see someone, where the doctors have to be, where the patient has to be, how we implement those systems, can be governmental agencies, like state agencies, federal agencies, you know, even industry kind-of agencies and regulatory bodies like around the payment card industry that we have to follow. There are a lot of aspects other than the HIPAA that we have to look at in how we handle and deal with the information and how we practice within each state."*

In the case study, several external and internal influences were delineated during the interviews. The Hospital is subject to regulatory processes. (Mignerat &

Rivard, 2009) In the form of external government mandates that include the Health Insurance Portability and Accountability Act (HIPAA), Federal regulations issued by the Office of the Inspector General, and state and local health regulations, among others. The Hospital is also subject to external processes that amount to quasi-regulatory standards like the Payment Card Industry – Data Security Standard (PCI-DSS), necessary for the hospital to maintain its ability to process credit card payments. The array of certifications held by the personnel (Certified Information Systems Security Professional - CISSP, Certified Information Systems Auditor - CISA, Certified Privacy Officer - CPO, Certified Information Security Officer – c-CISO). Several examples were provided by the informants where the hospital has benchmarked their processes against their peers and by actively participating and engaging in information sharing with other organizations in their industry represented by organizations like Children's Hospitals associations, Privacy Officers Association, and their interaction with consultants and external counsel used it as a form of organizational learning and avoid some of the pain points their peers have experienced by bringing best practices from their network into their own internal processes.

Interview questions also explored how information security requirements are communicated throughout the organization and what processes the hospital had in place to handle any conflict or competition for resources. Regarding communication, informants described several efforts within the organization to ensure that information about activities and requirements is disseminated widely. When discussing communication and conflict resolution, an IT Operations Manager commented:

> *"Creating more visibility into what project teams are working on, there's definitely more visibility across the organization and then creating that visibility with other organizations basically it's to cut out conflicting projects or projects that don't directly tie in with the mission, or we call them "true north" goals or organizational goals trying to limit someone working on a project that ultimately doesn't impact what the company is trying to achieve."*

In the process of evaluating requirements, the Hospital used review boards to sort out the requirements as described by the IT Operations Manager:

> *"There's also a board to review the projects, so as competing priorities are identified, they're brought before the board must they need to be escalated from that, they are escalated so that the project manager or manager of that team would work with our executive team to determine the course of action."*

When identifying the source of requirements for information security risk, the hospital leveraged several sources, including legal, industry associations, professional organizations, vendors, consultants, and industry reports, as well as an internal resource, among others. When discussing leveraging internal resources, the topic of internal surveys was brought up by the CIO, who commented:

> *"When we look at risk management, we do a survey throughout the years of key leaders in the enterprise. The team actually interviews them on their top concerns and what they're hearing. For risk management, we try and pull in not only what we see through our own channels but also what we hear from various parts of the enterprise."*

When the sources of compliance requirements were discussed, the informants mentioned both internal and external resources. Since the Hospital operates in a highly regulated industry, it is subject to several layers of compliance at the local, state, and federal levels. The Health Insurance Portability and Accountability Act

(HIPAA), a United States Federal Government Regulation signed in 1996, was the most often cited regulation by all the informants.

When it comes to managing the requirements of information security risk management and compliance, the informants described several processes and working groups or boards that work in tandem to address said requirements, as provided in this excerpt from the interview with the CIO:

> *"We have a good process in place. We've developed a really good working model that includes information security, information systems, compliance, legal, and privacy. Audits are all on the table, and we have regular meetings with these groups, where we talk about the risk and the prioritization; we even present to our board audit and finance committee every chord on risk audit and security. Those teams we have are really close together. There is a lot of communication about the risk and what we're doing, how we track them, any barriers, risks, risks to the project itself."*

Strategic and Tactical Responses – Empirical evidence

After gaining an initial understanding of the hospital operating environment, the analysis pivoted to understanding how the processes in the hospital aligned with Oliver (Oliver, 1991). Oliver provides a framework of strategies and tactics that describe the actions of the organization in the context of the influence of requirements of the organizational environment. Table 2 presents the strategies and tactics that arise in our analysis of the informant's interviews. In the context of strategic responses in a regulated environment, the two main strategies that emerged from the study were Acquiesce and Compromise, which may be due to the potential impact on the organization from a finding of non-compliance in the form of fines and revocation of authorization to operate. The most mentioned tactical responses included Imitate, Comply, Pacify, Bargain, and Influence. It was also interesting that the organization recognized the need to deploy influence tactics at the government policy level to stay abreast and provide input to regulatory changes.

Table 3 below summarizes Oliver's Strategic Responses (Oliver, 1991) strategies and tactics that were identified in the interviews.

Table 2. Number of tactics identified

Strategic Response	Tactic	Number of occurrences
Acquiesce	Imitate	59
	Comply	19
	Habit	20
Compromise	Pacify	6
	Bargain	12
	Prioritization*	30
Manipulate	Influence	2

* New tactical response

Table 3. Strategic Responses and Tactics (Oliver, 1991) **Occurrences in data collected**

Strategic Response	Tactic	Example of Evidences
Acquiesce	Imitate	*"…we look at our professional associations, but we also look at our industry associations, so, the Children's Hospital Association, in Florida, there's a Florida Hospital Association that has a compliance and a privacy forum where compliance officers, privacy officers, and others like internal audit, can participate and learn from each other and they also have where you can ask questions of the group and get feedback."*
	Comply	*"When you look at our hospital, there are the Conditions of Participation with the Centers for Medicare and Medicaid Services, and sometimes our audits need to look at whether we are in compliance with those Conditions of Participation. … So, if we go in and look at a service like Audiology, there are certain state and national-based regulations that we have to look at to ensure that the payment that we are receiving is appropriate, for*

		instance, what type of provider is providing the service."
Compromise	Pacify	*"Well, from the compliance standpoint, as I said, there is some focus through that, but more of the focus is definitely on the risk side, making sure that the organization weighs different risks. Compliance, at least at the stage at [Hospital], we tend to try to meet regulatory compliance, or we look at standards bodies as well, so looking at information security, for example. If we're looking at information security, we've got different bodies out there, MIST and organizations that have already provided a standard, so these are frameworks to help us keep our processes so that we do meet compliance as well as mitigate our risk."*
	Bargain	*"We're starting to morph into more of an agile type environment, so right now, if it's projects that have competing priorities, so maybe it's a conflict of resources, we tend to move towards where there's no true saying no to a request. Whereas moving more towards an agile environment, we're starting to create visibility on those to move them to like a multi-organizational type board to go back and say, "Hey, we have these ten requests; we can only work on one of these requests right now, which one is your top priority?" or basically working with… to identify what we should be working on rather than taking on multiple tasks and continuing to work with those."*
	Prioritization	*"In the future state, a future project will be weighed, as I said, and more organizational versus department standpoint. Basically, those projects we'll try to align those with the strategic direction of the company in the future state. Creating more visibility into what project teams are working on, there's definitely more visibility across the organization, and then creating that visibility with other organizations basically it's to cut out conflicting projects or projects that don't directly tie in [0:20:47 inaudible] with the mission, or we call them "true north" goals or organizational goals trying to limit someone working on a project that ultimately doesn't impact what the company is trying to achieve."*
Manipulate	Influence	*"…we have [lobbying] resources assigned in the State Capital. In [Washington] D.C., we have [lobbying] resources assigned to Washington D.C. working with government officials to make sure that we understand these requirements but also help with policy that provides better care for children in the state and from a national perspective."*

Although only a subset of strategic and tactical responses was found in Oliver (Oliver, 1991), it is possible that in other organizations, additional strategies and tactical responses could be present. It appears that imitate is leveraged to "not reinvent the wheel," as the CIO stated, which the organization leverages to manage its risks, particularly implementation and compliance risks. By leveraging the experience of other organizations that have achieved compliance with a regulatory requirement or addressed a particular risk before, the hospital expects to have a roadmap to address the requirements successfully. Relying upon imitation tactics could help reduce an initiative learning curve as well as reduce risk and ideally improve the chances of successfully achieving compliance.

During the study, a new tactical response, not already described in the literature, was discovered in the process used to select a course of action when facing competing requirements. The process is an intense governance process that is coded as *prioritization*. Prioritization is different from balancing. In the context of Oliver's Strategic and Tactical Responses, balancing refers to harmonizing the needs of diverse stakeholders during operation, whereas prioritization is focused on the requirements at hand. During coding, 30 instances of this tactic were found. *Prioritization* can be described as the process by which the organization ranks and implements requirements in response to external pressures. In the studied case, prioritization encompassed a combination of qualitative and quantitative measures to prioritize or select a course of action as part of the governance process. The quantitative part of prioritization involves the assignment of a weighted numeric priority by experienced staff members, like the Delphi method. The qualitative evaluation of requirements consists of consensus amongst stakeholders on how closely the chosen

requirement advances their “true north” principle of patient-centered care and the organizational strategy. For the hospital, having the patient at the center of every effort helps focus efforts on those actions that will have the largest positive impact on patients. Such evaluations allow the organization to achieve consensus on the best course of action for the organization, taking into consideration its values and resource constraints. During the interviews, the Chief Information Officer described the process as follows:

> “We’ve developed a really good working model that includes information security, information systems, compliance, legal, and privacy. Audits are all on the table, and we have regular meetings with these groups, where we talk about the risk and the prioritization; we even present to our board audit and finance committee every quarter on risk audit and security. Those teams we have are really close together; there is a lot of communication about the risks and what we’re doing, how we track them, any barriers, and risks, risks to the project itself. So that kind of keeps that process moving; in the end, that group works to define the priority levels and the areas that we need to work on mitigation. The compliance side is also making sure that we’re doing the things we need to be doing, like reporting to the board for awareness, getting the board [of Directors] signed off on certain items, or adhering to plans and things we have in place. There is a really tight working relationship there; there is a working group that meets once a month, and we also meet cordially with that group and a higher-level group, including our CEO, to do what we call our leadership compliance and security meeting, where we present to them the state of risks and compliance areas and what actions we’ve taken. I think there is a good working relationship and process around, keeping that risk curved managed and making sure that each one of those inner factions is doing their piece and is involved at the right time.”

The governance process behind prioritization involves smaller committees at the operational activity level that serve as inputs to higher-level committees. The committees at the intermediate level, mainly composed of mid-level managers, applied the qualitative and quantitative measures to the requirements and chose a course of action, taking a patient-centered approach. These requirements, along with the analysis and the recommended course of action, are presented to Senior

Executives/ In this case, external and internal pressures serve as the inputs for information systems security risk management and regulatory compliance requirements. This governance process enables the dissemination of requirements throughout the organization, resulting in a holistic view of requirements with the side effect of being able to identify initiatives that could leverage one project to address the requirements of other projects in the portfolio. An example of the impact of prioritization on the organization is provided by the Operations Manager.

> *"A project will be weighed, as I said, and more organizational versus department standpoint."…*
>
> *"We're cutting out some of these department-only projects that the company doesn't necessarily see value to and helping. Organizations always struggle with having enough resources, so it kind of tackles that part too where it really focuses your resources on what's important for the company."*

This is underpinned by how the organization leverages multi-disciplinary teams as described by the Operations Manager:

> *"[We start the process by] presenting through our change boards so eventually we present our changes to our project board …, the project board is made up of individuals from all of our corporate services departments. When I present, and I'm describing my […] project, we have a training department. The training team may say, "What type of resources are required from our side? I see you don't have a resource from my team on that". It may be that either we do need training from their resources, or it's a slight change, and we handle the training ourselves. In this case, my team is handling the training ourselves. We said a learning services training team member isn't required for this project. By presenting to that board, we're able to catch areas where if the project manager may missed a team, the projects board helps to assign those resources; Also as we do have a PMO, and our project management office will help make some recommendations in that area as well."*

The empirical evidence collected in the case provides fertile ground for the discussion that follows.

3.5 Discussion

The objective of this case study was to investigate two research questions:

- How does an organization manage information security, risk management, and compliance?
- What strategic and tactical responses does the organization leverage to manage information security, risk management, and compliance?

In the pursuit of the research questions, three important lines of discussion emerge from the case study. The contributions of the case study include empirical observations of the organization's strategic and tactical responses, an emerging process within which the organization incorporates new requirements by considering organizational pressures, and finally, the governance processes that undergird the response process. Oliver (Oliver, 1991) provided the theoretical framework to study the mechanics of their processes, identifying what strategic and tactical responses the organization leverages in their activities. How the organization responds becomes a function of its internal processes and how its chosen strategies and tactics are implemented. This is in contrast with the study in Chapter 2, where the organization "speaks" through its policy and compliance documents as well as its procedures about its stated response to external pressures, and this case study, how it "acts" through the processes and actions that the organization engages in implementing policy in their responses. The empirical evidence collected from the informants points to acquiesce as the most widely used strategy; given the potential negative impacts of regulatory compliance with the organization, it was not surprising that this strategy featured so prominently in the chosen response. Evidence of all three tactics under acquiesce was found, with comply and habit at about the same levels. This can be attributed to the strong compliance culture that permeates the

organization. Informants understood the importance of compliance and its potential impact on the organization and acted accordingly. By far the most important tactic amongst all strategies, was imitate, this aligns well with the informant's desire "not to reinvent the wheel" and reduce risk by leveraging other organization's lessons learned. Observations of the compromise strategy and its tactics were less than the observations of the acquiesce strategy and tactics. This could be attributed to their strong compliance culture and the reality that organizations need to navigate the regulatory landscape while still navigating their own operational landscape. The identification of a new tactical response named prioritization under the compromise strategy provides a way to describe how the organization crafts a response to changes in its environment. Supported by strong governance processes, prioritization is the response that the organization chooses to make sure that its actions have the best chance at success and maximize its resource utilization. The presence of the Manipulate strategy and the influence tactic, although limited, demonstrates the need by organizations to have a seat at the table and have a say in guiding the regulations that would apply to them. By ensuring having a say in the crafting of laws and regulations, the organization has a chance to shape its regulatory landscape and reduce its risks. Given its inherent risks, it is no surprise that avoidance and defiance were not observed as strategies as, in this case, the consequences of following such strategies could be severe for the organization. The continuum of strategic responses available to the organization shows progressively limited resistance from the organization to external pressure. In the case of the Hospital, not all strategies/tactics were identified.

The second contribution of the study on how the organization manages compliance and information systems risk is the identification of a Continuous Organizational Alignment process, illustrated below.

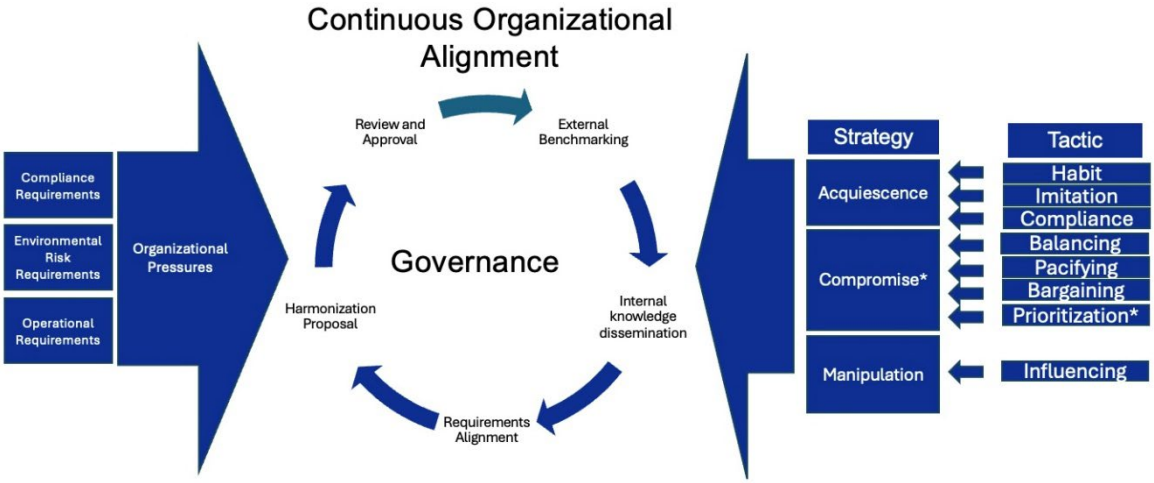

Figure 4 Continuous Organizational Alignment

This process is influenced on one side by the organizational pressures in the operational environment. On the other side, the organization incorporates its chosen responses from a menu of strategies and tactics theorized by Oliver (Oliver, 1991).Compliance requirements like those imposed by government regulations, existing and emerging information security risks, and operational requirements like Payment Card Industry – Data Security standards are just examples of the pressures the organization is being subject to and to which they need to respond. In responding to these pressures, the organization was observed following a five-step process that we have named Continuous Organizational Alignment. The five steps in the process are:

1. **External Benchmarking**: This step involves benchmarking how other organizations have or plan to address similar requirements.
2. **Internal Knowledge Dissemination**: This step focuses on sharing the information gathered on the requirements from external sources and

incorporating this information in the analysis being conducted internally by the different departments.

3. **Requirement Alignment**: This step matches internal requirements analysis from departments and projects with the information learned on requirements from external organizations.
4. **Harmonization Proposal**: This step involves proposing how to harmonize the projects being considered and in flight. Combines bottom-up and top-down approaches to identify potential synergies, reduce risk, and avoid duplicity of efforts.
5. **Review and Approval**: This step includes the revision of proposals by a review board to identify potential duplicity of efforts and their corresponding approval.

The process that the organization follows to select a response is highly influenced by how the organization manages compliance and risk through its governance processes. In the organization studied strong formal and informal governance structures ensure that there are multiple avenues that an organization can leverage to help manage risk and compliance. Cross-departmental cooperation helps break silo barriers that help identify conflict and bring its resolution to the primary organization goals or “true north” goals of patient-centered care.

The organization’s governance processes support decision-making, communication, and coordination controls. Through multiple working groups and governance boards, the Hospital is implementing the processes to manage risk and compliance supported by a said network of governance structures that help choose the strategic direction. From the comments provided by the informants, a picture

emerges that such governance structures are multi-level and are driven by a multi-disciplinary approach that includes internal and external users.

The organization studied responded to competing organizational pressures by having processes that allow the proverbial “right hand” to talk to the “left hand,” providing the opportunity to leverage tasks across the organization by bringing together multiple stakeholders through purposeful collaboration avenues that allowed for the opening of communication channels and the timely sharing of information. By minimizing the impact of operational silos in the decision-making process, the organization developed a holistic view of its compliance and information security risk management requirements portfolio with the aim of attaining alignment between the two. This was accomplished in one of two ways: First, a top-down approach, where a top executive (in this case, the Chief Information Officer - CIO) has an enterprise view of all the technology-focused projects. This provided the CIO with the information to identify those that could impact other areas of the organization by repurposing some or all its deliverables. Second, bottom-up leveraging the work of cross-functional groups or boards enabled a high level of collaboration between the different departments throughout the organization. In the case studied a combination of both processes was witnessed. From the bottom-up approach, two separate projects arose around the same time, with one being more developed than the other. Both projects—one from medical informatics for compliance with Drug Enforcement Administration (DEA) Electronic Prescriptions for Controlled Substances (EPCS) regulations and one from the information security team to address identified risk management and Payment Card Industry – Data Security Standards audit recommendations. The information from both projects was ushered through the governance process of the project and change boards until being raised to the CIO

as a requirement. When the requirements reached the CIO, the top-down approach took over, with the CIO asking the information security team to hold off on their project until the DEA-EPCS project was completed.

When the organization takes a holistic view of such requirements, the proper governance structure can assist in the harmonization of compliance and information security risk management controls and maximize the use of organizational resources. It is through this alignment that the organization can address multiple requirements brought upon by organizational pressures by repurposing or increasing the efficiency of its use of resources. In this case, the hospital has leveraged information security and compliance Governance processes through change, and project boards in their pursuit of balancing information systems security and compliance, include:

- The hospital has governance structures in place that allow for the control and coordination of activities related to compliance and risk management. These boards or groups, like the change or project, start at the department or activity level and consolidate to organization-level review boards and, ultimately, the board of directors.
- The organization has taken active steps to identify its current organizational risk footprint
- The organization takes active steps to rationalize spending on compliance and risk management activities (e.g., repurpose a compliance Project result to address an identified risk or vice versa)

Information Systems Security and Compliance Governance processes provide the organization with a space that enables the sharing of information amongst what often

is described as silos within the organization. By leveraging multi-disciplinary teams in the examination and response selection, the organization increased the sharing of information between the business functions and increased the opportunities for collaboration and awareness of initiatives that could potentially address other requirements.

By having an organizational view of current initiatives, the organization can evaluate or identify potential synergies, thus increasing the efficiency in the deployment of organizational resources to address information systems risk management and compliance requirements. By bridging operational silos, governance processes enable the organization to reinforce lines of communication that could spur collaboration, and spur the collaborations that result in the pool of organizational resources that could help address multiple goals within the resource constraints of the organization. The organization's governance processes then become a bridge that allows the flow of requirements through the organization, enabling the coordination of activities and procurement that enables increased efficiencies in the assignment of resources.

In this case, the governance process involves smaller committees at the operational activity level that serve as inputs to higher-level committees. The committees at the intermediate level, mainly composed of mid-level managers, apply qualitative and quantitative measures to the requirements and choose a course of action, taking a patient-centered approach. These requirements, along with the analysis and the recommended course of action, are presented to Senior Executives. Organizational pressures serve as the inputs for information systems compliance and information security risk management requirements. These governance processes enable the dissemination of requirements throughout the

organization, resulting in a holistic view of requirements with the additional benefit of being able to identify initiatives that could leverage one project to address the requirements of other projects in the portfolio.

Based on the observations from the case study, the following five propositions are put forward to guide future research. Each is based on the components of the Continuous Organizational Alignment process:

Proposition 1: External Benchmarking – *Organizations that benchmark their compliance and risk management practices against peer organizations will report higher levels of efficiency and effectiveness in managing organizational pressures.* Organizations can lower their risk and increase their response success by leveraging the collective experience of their industry peers.

Proposition 2: Internal Knowledge Dissemination - *Organizations that have effective internal communication and dissemination processes for compliance and risk management requirements will report fewer conflicts and higher alignment with organizational goals.*

Effective communication is key in overcoming potential organizational silos and enabling the sharing of information across and up and down the organization.

Proposition 3: Requirements Alignment - *Organizations with strong governance processes for aligning internal requirements with external benchmarks will report higher levels of harmonization and prioritization of competing demands.* By aligning requirements both internally and externally, the organization can reduce its risk and increase its chances of successfully responding to organizational pressures through the efficient assignment of resources and implementing an appropriate response.

Proposition 4: Harmonization Proposal - *Organizations that develop harmonization proposals through collaborative efforts involving multi-disciplinary teams and governance boards will report higher levels of successful implementation and stakeholder satisfaction.*

Organizations whose governance processes encourage the flow of information and focus collective efforts on attaining efficiency by identifying areas where overlapping requirements can be combined are better able to assign resources and reduce risk. Through the involvement of stakeholders from different sides of the organization and incorporating their different perspectives, it encourages the successful interaction of what otherwise would be organizational siloes towards implementing organizational responses.

Proposition 5: Review and Approval - *Organizations with a review board for approving harmonization proposals will report lower levels of duplication of effort and more efficient resource allocation.*

Through various boards, committees, and other control and coordination mechanisms, an organization can achieve both bottom-up and top-down visibility into its efforts and responses to the pressures it experiences in its operational environment.

Together, these propositions offer a structured set of insights into how organizations operating in highly regulated environments navigate the dual imperatives of compliance and risk management. By distilling the empirical findings into theoretically grounded propositions, this study contributes to a more nuanced understanding of the decision-making processes organizations engage in when facing institutional complexity. These propositions not only extend Oliver's (1991) framework by introducing prioritization as a previously undocumented tactic but also

offer a lens through which future research can explore the dynamics of organizational responses under resource constraints.

3.6 Conclusion

The results of the case study yielded several empirical observations that align with the theory. The informants identified organizational pressures, and a direct connection between the pressures and the organization was confirmed. Such pressures occupy a significant share of the organization's mind. The presence of those pressure results can then be tied to the organizational response strategy and tactics. Acquiesce was by far the most widely used strategy, followed by compromise and manipulate. The top three tactics included imitate, comply, and habit. By far, imitate is the most used tactic in the organization, which falls in line with the theoretical prediction of the organization moving towards isomorphism.

The study makes three contributions: two theoretical and one practical. These contributions include a newly identified tactic, prioritization under the compromise strategic response, and a framework that describes the mechanics of a Continuous Organizational Alignment process, which occurs when an organization manages information security risk management and compliance. The proposed framework provides a roadmap for examining how organizations manage the requirements of organizational pressures through information systems governance activities or behaviors. This framework can help both academics and practitioners understand how, under proper governance, internal and external inputs can be leveraged in the organizational response. Organizations that apply similar governance processes when addressing the requirements of competing institutional pressures are better positioned to select an approach that could reduce their risk and achieve their

compliance goals. The proposed theoretical framework provides a map to explore how the organization can manage the requirements of organizational pressures and extends our understanding of how strategies and tactics are implemented within the organization beyond established executive sponsorship and project management paradigms.

3.5.1 Limitations

Single case studies are not sufficient to provide insights that can be generalized, but they can provide the foundation for a research project that yields additional insights that can be generalized. Further study is required to explore the use of the prioritization tactic and confirm its existence as a strategic response tactic under the compromise.

3.5.2 Future work

Future work could include additional case studies in healthcare or other regulated environments, such as financial services, critical infrastructure, or education. Further study could also explore the connection between tactical responses and stated policy in the organization's information security and compliance policies.

Page intentionally left blank.

Dissertation Discussion

In the first part of the dissertation, an exploration of the literature on compliance, risk management, and information security was presented. An opportunity was identified to expand our understanding by examining how organizations in regulated environments balance the requirements of regulations with their own risk management. This served as a foundation for the work of the subsequent sections. The first study empirically analyzed compliance documents in healthcare organizations, focusing on their features and components. Drawing on guidance from the Association of Corporate Counsel (Carboni, 2022) and Kusserow (2014) as references, the study examined the variability in document length, structure, and validity period. Some organizations opted for a single comprehensive document, while others used multiple smaller documents. This considerable variability in size, format, and content suggests an uneven implementation of documentation related to compliance programs. The documents examined exhibited a 2–5-year validity period, which poses potential risks, as outdated documents may lead to non-compliance with regulations and increased risks. Although the literature does not prescribe an ideal validity period, it emphasizes the importance of periodic reviews, which, when formalized in the documentation, can help the organization with the discipline needed to keep the documentation relevant and up to date.

Other findings of the examination of the compliance documents indicate that duties and responsibilities were the most common feature, as they guide individual actions within organizations, reducing non-compliance risks. Reporting requirements were also consistently emphasized to ensure proper control mechanisms and remedial actions. Surprisingly, interdepartmental interactions and key performance

indicators (KPIs) were absent from the examined documents, possibly due to the complexity of defining interactions or the operational nature of KPIs.

When examining the expected components of policy documents, policy statements, and procedures were the most widely used, as they define expectations and accountability. The scope of compliance documents varied, with some serving as reference materials while others incorporated training elements, codes of conduct, and prescriptive guidance. Documents also differed in format, with some using paragraphs and others using bullet points to enhance readability and retention. The study highlights the importance of clearly defined duties, responsibilities, and structured compliance documentation to ensure adherence to regulatory standards. Given the significant variability within the sample, it is not possible to determine the effectiveness of the different compliance documents examined. For a more comprehensive discussion of the results, please review the discussion in Chapter 2.

The following study, a case study of a Children's Hospital, investigates how an organization manages information security, risk management, and compliance, exploring both strategic and tactical responses. It identifies three key contributions: (1) empirical observations of the organization's response strategies, (2) an emerging process for integrating new requirements based on organizational pressures, and (3) the governance structures that support these responses.

Using Oliver's (1991) theoretical framework, the study highlights that the organization predominantly employs the *acquiesce strategy*, mainly through compliance and habitual practices. The *imitate tactic*—adopting best practices from other organizations—was the most commonly observed, aligning with the organization's desire to minimize risk. A *compromise strategy*, including prioritization as a newly identified tactic, allows the organization to balance regulatory and

operational demands particular to their environment. The *manipulate strategy* was minimally observed but underscores the organization's need to influence regulatory frameworks. *Avoidance and defiance strategies* were absent, likely due to their high risks.

A central finding is the identification of the *Continuous Organizational Alignment (COA) process*, a five-step approach used to manage compliance and risk:

1. *External Benchmarking* – Learning from the approaches of other organizations.
2. *Internal Knowledge Dissemination* – Sharing external insights within departments.
3. *Requirements Alignment* – Matching internal requirements with external benchmarks.
4. *Harmonization Proposal* – Combining top-down and bottom-up efforts to streamline initiatives.
5. *Review and Approval* – Final evaluation to prevent redundancy and ensure optimal resource utilization.

The study emphasizes that strong governance structures enable the organization to coordinate compliance and risk management effectively. These structures bridge operational silos, fostering collaboration and resource efficiency. Through governance mechanisms such as working groups and project boards, the hospital aligns compliance and information security strategies with its broader organizational goals.

The study concludes with five research propositions to guide future studies on the COA process, focusing on the importance of benchmarking, internal communication, governance structures, harmonization efforts, and review mechanisms in enhancing organizational efficiency and compliance effectiveness.

Page intentionally left blank.

Dissertation Conclusion

This dissertation set out to explore how healthcare organizations manage the intertwined challenges of regulatory compliance and information security risk management within the constraints of limited resources. By integrating insights from strategic responses to institutional pressures (Oliver, 1991) with empirical investigations of policy artifacts and organizational practices, the study contributes to a deeper understanding of how organizations navigate competing institutional pressures. Through a multi-method approach combining content analysis and case study research, the findings illustrate the formal and informal mechanisms that shape organizational responses to complex compliance environments.

The dissertation examined compliance documents from 33 healthcare organizations, providing empirical evidence on how compliance document features as defined by the Association of Corporate Counsel guidance (Carboni, 2022) and components as outlined by Kusserow (Kusserow, 2020) are implemented in practice. The findings help organizations identify areas for improvement in their documentation and adopt best practices to enhance compliance with regulations. By analyzing how compliance documents are drafted and maintained, organizations can refine their approaches to ensure that documents are effective in achieving compliance goals.

The Compliance Document Analysis study highlights the variability in compliance documents and the potential benefits of improving documentation practices. The limited sample size contributed to a higher level of variability. Further study of additional compliance documents is necessary to refine our understanding of the features and components, as well as their impact on the efficacy of a compliance program. The results may also have been limited by the geographical

and industry focus of the sample; further study is needed to expand into additional geographies and industries, as regulated industries often share similar characteristics and requirements.

In the case study of a children's hospital's response to a regulatory requirement, informants confirmed the presence of organizational pressures that significantly influence the organizational strategy and tactics chosen. The study introduces *prioritization* as a new tactic under the *compromise* strategy proposed by Oliver in her Strategic Responses To Institutional Processes (Oliver, 1991) , adding to the theoretical understanding of compliance responses by identifying a tactic that focus on resource and organizational alignment vs a tactic like balancing that focuses on stakeholder alignment.

The study proposes a Continuous Organizational Alignment (COA) Framework that describes how organizations can manage compliance and risks through internal governance structures. This framework provides insights into how organizations respond to external and internal pressures, as well as optimizes resource allocation by establishing a process that breaks up silos and optimizes the assignment of resources.

The findings on governance and compliance management underscore the importance of governance mechanisms in ensuring that compliance strategies are effectively implemented, extending beyond traditional executive sponsorship and project management paradigms. Organizations that choose to implement robust internal governance structures can benefit from increased efficiency in resource allocation, reduced risk, and enhanced compliance.

The case study chapter is based on a single case, which, although foundational, requires further research to confirm and expand upon the findings.

Additional research is needed to assess whether prioritization is a widely used tactic under the compromise strategy. Another avenue of study could be the examination of the connection between stated policies in compliance documents and actual tactical responses within organizations, aiming to bridge the gap between theory and practice. Overall, this dissertation offers critical insights into the implementation of compliance documents, governance processes, and strategic responses, providing both theoretical advancements and practical guidance for organizations navigating compliance challenges.

.

Page Intentionally Left Blank

Conclusión de la tesis (Spanish)

Esta tesis se propuso explorar cómo las organizaciones de atención médica gestionan los desafíos entrelazados del cumplimiento normativo y la gestión de riesgos de seguridad de la información dentro de las limitaciones de los recursos limitados. Al integrar los conocimientos de las respuestas estratégicas a las presiones institucionales (Oliver, 1991) con investigaciones empíricas de los artefactos de política y las prácticas organizacionales, el estudio contribuye a una comprensión más profunda de cómo las organizaciones navegan por las presiones institucionales competitivas. A través de un enfoque multimétodo que combina el análisis de contenido y la investigación de estudios de caso, los hallazgos ilustran los mecanismos formales e informales que dan forma a las respuestas organizacionales a entornos complejos de cumplimiento.

La tesis examinó los documentos de cumplimiento de 33 organizaciones de atención médica, proporcionando evidencia empírica sobre cómo se implementan en la práctica las características de los documentos de cumplimiento, según la guía y los componentes de la Asociación de Abogados Corporativos, según lo descrito por Kusserow. Los hallazgos ayudan a las organizaciones a identificar áreas de mejora en su documentación y a adoptar las mejores prácticas para mejorar el cumplimiento de las regulaciones. Al analizar cómo se redactan y mantienen los documentos de cumplimiento, las organizaciones pueden refinar sus enfoques para garantizar que los documentos sean eficaces para lograr los objetivos de cumplimiento. (Carboni, 2022)(Kusserow, 2020)

El estudio de Análisis de Documentos de Cumplimiento destaca la variabilidad en los documentos de cumplimiento y los beneficios potenciales de

mejorar las prácticas de documentación. El tamaño limitado de la muestra contribuyó a un mayor nivel de variabilidad. Es necesario realizar más estudios de documentos de cumplimiento adicionales para refinar nuestra comprensión de las características y componentes, así como su impacto en la eficacia de un programa de cumplimiento. Los resultados también pueden haber estado limitados por el enfoque geográfico e industrial de la muestra; Se necesitan más estudios para expandirse a otras geografías e industrias, ya que las industrias reguladas a menudo comparten características y requisitos similares.

En el estudio de caso de la respuesta de un hospital pediátrico a un requerimiento regulatorio, los informantes confirmaron la presencia de presiones organizacionales que influyen significativamente en la estrategia organizacional y las tácticas elegidas. El estudio introduce *la priorización* como una nueva táctica bajo la estrategia de compromiso propuesta por Oliver en sus Respuestas Estratégicas a los Procesos Institucionales, que se suma a la comprensión teórica de las respuestas de cumplimiento mediante la identificación de una táctica que se centra en la alineación de los recursos y la organización frente a una táctica como el equilibrio que se centra en la alineación de las partes interesadas.(Oliver, 1991)

El estudio propone un Marco de Alineación Organizacional Continua (COA, por sus siglas en inglés) que describe cómo las organizaciones pueden gestionar el cumplimiento y los riesgos a través de estructuras de gobierno interno. Este marco proporciona información sobre cómo las organizaciones responden a las presiones externas e internas, así como optimiza la asignación de recursos mediante el establecimiento de un proceso que rompe los silos y optimiza la asignación de recursos.

Los hallazgos sobre la gobernanza y la gestión del cumplimiento subrayan la importancia de los mecanismos de gobernanza para garantizar que las estrategias de cumplimiento se implementen de manera efectiva, más allá de los paradigmas tradicionales de patrocinio ejecutivo y gestión de proyectos. Las organizaciones que optan por implementar estructuras sólidas de gobernanza interna pueden beneficiarse de una mayor eficiencia en la asignación de recursos, un menor riesgo y un mejor cumplimiento.

El capítulo del estudio de caso se basa en un solo caso, que, aunque fundamental, requiere más investigación para confirmar y ampliar los hallazgos. Se necesita investigación adicional para evaluar si la priorización es una táctica ampliamente utilizada en el marco de la estrategia de compromiso. Otra vía de estudio podría ser el examen de la conexión entre las políticas establecidas en los documentos de cumplimiento y las respuestas tácticas reales dentro de las organizaciones, con el objetivo de cerrar la brecha entre la teoría y la práctica. En general, esta tesis ofrece información crítica sobre la implementación de documentos de cumplimiento, procesos de gobernanza y respuestas estratégicas, proporcionando avances teóricos y orientación práctica para las organizaciones que atraviesan los desafíos de cumplimiento.

.

Appendix A - Semi-Structured Interview

Artifact/Initial Coding Protocol

Item	Objective		Question
1	Identify Institutional Pressures	Capture information on Coercive pressures in the organization.	What if any requirements exist that need to be taken into account when planning and or implementing a system that is coming from outside your organization?
2	Identify Institutional Pressures	Capture information on Normative pressures in the organization.	What external resources does the organization use to identify and implement best practices when planning or implementing a system?
3	Identify Institutional Pressures	Capture information on Mimetic pressure on the organization.	Does the organization leverage what other industry peers are doing when planning and implementing a system? Please provide examples.
4	Governance of Information Systems Requirements	Capture information on how information systems requirements are communicated through the organization across operational units.	Are information systems requirements communicated/coordinated across organizational units? If so, how?

5	Governance of Information Systems Requirements	Capture information on the organizational experience identifying and dealing with competing requirements.	Have competing requirements been identified in the past? What process, if any, is in place to choose a course of action?
6	Risk management of information systems	Capture information on the sources of information systems' risk management requirements and the priority assigned to them.	What would you consider are the sources of your top information risk management requirements?
7	Compliance management of information systems	Capture information on the sources of information systems' compliance requirements and the priority assigned to them.	What would you consider are the sources of your top information system compliance requirements?
8	The conflict between information systems risk management and compliance	Capture information on how the organization assigns priorities in the assignment of resources when there is the possibility of conflict between them.	What do you consider is the priority the organization assigns to compliance vs. information systems risk management requirements?

9	The conflict between information systems risk management and compliance	Capture information on what the organization considers its capabilities in addressing competing requirements.	Do you consider your organization successful at balancing the requirements of information risk management and compliance? Why?
10	Achieving a balance between information systems risk and compliance	Capture information on the process the organization follows to assign resources to risk management requirements. This question is used to validate any differences in the responses from interviewees from the responses given when risk and compliance are combined.	What process does the organization follow to assign resources to meet information security risk requirements?
11	Achieving a balance between information	This question is related to question 10; however, the focus of this question is compliance, in contrast with question 10, which	What process does the organization follow to assign resources to meet compliance requirements?

	systems risk and compliance	focuses on risk management. It is meant to capture information on the process the organization follows to assign resources to compliance. This question is used to validate any differences in the responses from interviewees from the responses given when risk and compliance are combined.	
12	Achieving a balance between information systems risk and compliance	The purpose of this question is to understand if, at any point, the organization did not purposely consider requirements across the organization. It is an attempt to understand if the organization attempts	How has the organization responded to information risk management requirements in the past?

		or considers requirements across departments.	
13	Achieving a balance between information systems risk and compliance	This question is similar to question 12; the focus is on compliance vs. the risk management focus of question 12. The purpose of this question is to understand if, at any point, the organization did not purposely consider requirements across the organization. It is an attempt to understand if the organization attempts or considers requirements across departments.	How have compliance requirements been addressed in the past?

Appendix B - Strategic and Tactical Responses – Oliver, 1991

Oliver, C 1991 Strategic Responses to Institutional Pressures Academy of Management Review Vol. 6 No. 1 151-159

Strategy	Description	Tactic	Description
Acquiesce	"Organizational acquiescence depends on the organization's conscious intent to conform, its degree of awareness of institutional processes, and its expectations that conformity will be self-serving to organizational interests."	**Habit**	"Habit refers to unconscious or blind adherence to preconscious or taken-for-granted rules or values. Particularly when institutional norms have attained the persisting status of a social fact, an organization may be unaware of institutional influences and, accordingly, precluded from responding to them strategically. Under these conditions, organizations reproduce actions and practices of the institutional environment that have become historically repeated, customary, conventional, or taken-for-granted. Organizations, for example, reproduce widely institutionalized roles such as students and teachers, line managers and staff, and professional and clerical functions on the basis of conventional definitions of these activities (Scott, 1987b)."
		Imitate	"Imitation, which is consistent with the concept of mimetic isomorphism, refers to either conscious or unconscious mimicry of institutional models, including, for example, the imitation of successful organizations and the acceptance of advice from consulting firms or professional associations (DiMaggio & Powell, 1983). One such example is Galaskiewicz and Wasserman's (1989) study of mimetic processes, whereby organizational decision-makers, under conditions of uncertainty, imitated the behavior of other actors in their environment, particularly those actors whom they knew and trusted."
		Comply	"Compliance, by comparison, is defined here as conscious obedience to or incorporation of values, norms, or institutional requirements. The elaboration of

			structural or administrative complexity in response to environmental complexity is one example of structural compliance, as Meyer, Scott, and Strung (1987) demonstrated in their study of American public school districts. Compliance is considered more active than habit or imitation to the extent that an organization consciously and strategically chooses to comply with institutional pressures in anticipation of specific self-serving benefits that may range from social support to resources or predictability (DiMaggio, 1988; Meyer & Rowan, 1983; Pfeffer & Salancik, 1978). For example, an organization may comply with external pressures because the approbation of external constituents or society enhances its legitimacy, increases its stability, or sustains the logic of confidence necessary to conduct organizational activities in good faith (Meyer & Rowan, 1983). Compliance may also establish the adequacy of "the organization as theory" (Meyer & Scott, 1983) by reducing the organization's vulnerability to negative assessments of its conduct, products, or services. For example, an organization's compliance with the variety of procedures specified by the Environmental Protection Agency elevates its legitimacy and protects it from public criticism and the financial penalties of noncompliance. Organizational acquiescence depends on the organization's conscious intent to conform, its degree of awareness of institutional processes, and its expectations that conformity will be self-serving to organizational interests."
Compromise	"Organizations are often confronted with conflicting institutional demands or with inconsistencies between institutional expectations and internal organizational objectives related to efficiency or autonomy. Under such circumstances, organizations may attempt to balance, pacify, or bargain with external constituents. These compromise tactics represent the thin edge of the wedge in	**Balance**	"balance can be defined as a tactical response to institutional processes. Powell and Friedkin (1986: 262-2651, for example, have described how a public television station was able to balance multiple funding sources by playing one funder off against another. Balancing tactics refer to the accommodation of multiple constituent demands in response to institutional pressures and

	organizational resistance to institutional pressures."		expectations. More specifically, balance is the organizational attempt to achieve parity among or between multiple stakeholders and internal interests. Particularly when external expectations conflict (e.g., shareholder demands for increased efficiency versus public pressures for the allocation of corporate resources to a social cause), organizations' interests may be served most effectively by obtaining an acceptable compromise on competing objectives and expectations."
		Pacify	"Pacifying tactics also constitute partial conformity with the expectations of one or more constituents. In his analysis of healthcare organizations, Scott (1983~: 106) observed that these organizations may rail against the interference of government authorities, but to do so is to "bite the hand that feeds them." Accordingly, these organizations tend to conform to at least the minimum standards of care and fiscal controls established by federal agencies. An organization that employs pacifying tactics typically mounts a minor level of resistance to institutional pressures but devotes most of its energies to appeasing or placating the institutional source or sources it has resisted. One such example would be an organization that is coming under increasing pressure to discontinue the production of a potentially harmful product: It may continue to manufacture the product but will allocate considerable financial resources to redesigning the product to fit institutional expectations and to promoting its subsequent safety."
		Bargain	"Bargaining tactics involve the effort of the organization to exact some concessions from an external constituent in its demands or expectations. For example, an organization may negotiate with a government agency to reduce the frequency or scope of its compliance with a newly instituted government policy. Resource dependence theorists, in particular, have elaborated the "negotiated

			environment" of organizations (Pfeffer & Salancik, 1978: 143-187), assuming that organizational relations with the environment are open to negotiation and the exchange of concessions."
Avoid	"Avoidance is defined here as the organizational attempt to preclude the necessity of conformity; organizations achieve this by concealing their nonconformity, buffering themselves from institutional pressures, or escaping from institutional rules or expectations."	**Conceal**	"Concealment tactics involve disguising nonconformity behind a facade of acquiescence. An organization, for example, may establish elaborate rational plans and procedures in response to institutional requirements in order to disguise the fact that it does not intend to implement them. Organizations may, additionally, engage in "window dressing,"; ritualism, ceremonial pretense, or symbolic acceptance of institutional norms, rules, or requirements (Meyer & Rowan, 1977). One example would be that in anticipation of scheduled site inspections by government representatives, organizations may display a variety of expected activities that are not a part of their normal routines. Concealment can therefore be distinguished from the acquiescent strategy of compliance by the degree to which conformity is apparent or real. From an institutional perspective, the distinction between appearance and reality is a theoretically important dichotomy (Scott, 1983b; Zucker, 19831, because the appearance rather than the fact of conformity is often presumed to be sufficient for the attainment of legitimacy."
		Buffer	"Buffering refers to an organization's attempt to reduce the extent to which it is externally inspected, scrutinized, or evaluated by partially detaching or decoupling its technical activities from external contact (Pfeffer & Salancik, 1978; Scott, 1987b; Thompson, 1967). Institutional theorists have elaborated the virtues of decoupling internal work activities from formal structures and external assessment as a means of maintaining the faith and legitimacy of the organization once it is highly institutionalized (Meyer & Rowan, 1977, 1983; Meyer et al., 1983). Meyer and Rowan (19831, for example, explained how educational

			organizations are buffered from the scrutiny of the details of instructional activities. Similarly, Powell (1988) has shown how an academic book publisher was able to buffer its technical activities from external demands because the production and manufacturing departments remained mainly in distant contact with the authors they served."
		Escape	"...an organization may exit the domain within which pressure is exerted (Hirschman, 1970) or significantly alter its own goals, activities, or domain to avoid the necessity of conformity altogether. As an example: If government inspections and evaluations of an organization's compliance with pollution emission standards are considered too stringent by the organization, it may change its goals and activities so that the offending production process is no longer required, or it may move to an alternative location where rules and requirements are lenient or nonexistent. Certain chemical manufacturers have established production facilities in Third World countries to produce and sell chemicals that are now banned in North America, for example. In contrast to acquiescence and compromise, which constitute strategic responses that organizations employ with the objective of partial or total conformity to institutional processes, avoidance is motivated by the desire to circumvent the conditions that make conforming behavior necessary."
Defy	"A defiant strategy, in contrast to acquiescence, compromise, and buffering, represents an unequivocal rejection of institutional norms and expectations, and it is more likely to occur when the perceived cost of active departure is low when internal interests diverge dramatically from external values, when organizations believe they can demonstrate the rationality or righteousness of their own alternative convictions and conduct, or when organizations believe they have little to lose by displaying their antagonism toward	**Dismiss**	"Dismissing, or ignoring institutional rules and values, is a strategic option that organizations are more likely to exercise when the potential for external enforcement of institutional rules is perceived to be low or when internal objectives diverge or conflict very dramatically with institutional values or requirements. The temptation to ignore authority or the force of cultural expectations is exacerbated by deficient organizational comprehension of the rationale behind the institutional pressures

	the constituents that judge or oppose them."		and the consequences of non-compliance. For example, an organization that chooses to ignore affirmative action requirements in the recruitment and selection of personnel may inadequately understand either the reasons for the policy or the ramifications of disobedience. Alternatively, the organization may argue, albeit unjustifiably, that the likelihood of "getting caught" is very low or that its success is not dependent on government approval and support. Salancik (1979), in his study of responsiveness to affirmative action pressures, for example, found the likelihood of compliance to be positively related to resource dependence on the government."
		Challenge	"Challenge is a more active departure from rules, norms, or expectations than dismissal. Organizations that challenge institutional pressures go on the offensive in defiance of these pressures and may indeed make a virtue of their insurrection. The fact that schools, for example, conform to a highly institutionalized set of structures and procedures that define what a school "should be" suggests that institutional pressures for a common understanding of educational requirements (through the process of accreditation, adherence to shared classifications, etc.) predict and explain the structure and process of educational systems (Meyer & Rowan, 1983; Meyer et al., 1983). However, Neo-institutional theory is unable to explain the continuing reappearance of alternative schools that attempt to make a virtue of their active departure from institutional beliefs and commonly held definitions of what constitutes effective education. Organizations will be more prone to challenge or contest the rationalized norms or collective rules of the institutional environment when the challenge can be reinforced by demonstrations of organizational probity or rationality. Just as rights activists will challenge extant laws and societal norms as a means of expressing their own convictions

			and integrity, organizations, in general, will be more likely to challenge institutional rules and values when they attach considerably less significance to widely shared external beliefs than to their own insular and elevated vision of what is or should be, appropriate, rational, or acceptable. Several Canadian manufacturers, for example, have attempted to challenge Ministry of Environment directives to conform to specific water pollution standards because they feel these directives are not "rational" and that their own behavior on pollution is above reproach."
		Attack	"Attack is distinguishable from the challenge as a tactic of defiance by the intensity and aggressiveness of the organization's active departure from institutional pressures and expectations. Attacking organizations strive to assault, belittle, or vehemently denounce institutionalized values and the external constituents that express them. For example, an organization's strategic response to increasing public criticism of its operations may be an attack on the media's representation of public opinion toward the organization. An attacking strategic posture is most likely to occur when institutional values and expectations are organization-specific rather than general or defocalized, when these values and expectations are particularly negative and discrediting, or when the organization believes that its rights, privileges, or autonomy are in serious jeopardy."
Manipulate	"Manipulation is the most active response to these pressures because it is intended to actively change or exert power over the content of the expectations themselves or the sources that seek to express or enforce them. Manipulation can be defined as the purposeful and opportunistic attempt to co-opt, influence, or control institutional pressures and evaluations." "Manipulation involves the active intent to use institutional processes and relations	**Co-opt**	"In response to institutional pressures, an organization may choose to co-opt the source of the pressure (Burt, 1983; Pennings, 1980; Pfeffer & Salancik, 1978). An organization may, for example, attempt to persuade an institutional constituent to join the organization or its board of directors. Pfeffer's (1974) research on electrical utility boards of directors showed how political support and legitimacy were obtained by co-opting important economic sectors in

	opportunistically, to co-opt and neutralize institutional constituents, to shape and redefine institutionalized norms and external criteria of evaluation, and to control or dominate the source, allocation, or expression of social approval and legitimation."		which the utility was under regulation. Selznick's (1949) study of the Tennessee Valley Authority also described in detail how outside interests were co-opted by the organization and persuaded to support its projects. The intended effect of co-optation tactics is to neutralize institutional opposition and enhance legitimacy. The opportunistic use of institutional links is also revealed in coalition-building processes and the strategic use of institutional ties to demonstrate the organization's worthiness and acceptability to other external constituents from whom it hopes to obtain resources and approval (Benson, 1975; DiMaggio, 1983; Oliver, 1990; Wiewel & Hunter, 1985). A social service agency, for example, may cultivate or advertise its ties to an influential charitable foundation in order to demonstrate to other potential public and corporate donors that it is deserving of resources and support."
		Influence	"Influence tactics may be more generally directed toward institutionalized values and beliefs or definitions and criteria of acceptable practices or performance. The manipulation of belief systems is reflected, for example, in the efforts of a trade association to influence public perceptions of its industry and to lobby government regulators for changes in the institutional rules to which its members are advised or required to conform. In a study of arts organizations, DiMaggio (1983) noted how various nonprofit art organizations forged lobbying coalitions to influence the amount of funding and support obtainable from public sources. Organizations also may strategically influence the standards by which they are evaluated, as Scott (1983~) observed in his examination of nursing home owners' abilities to influence the political processes that determine nursing home standards. Because performance in institutionalized environments is itself institutionally defined and prescribed (Hinings & Greenwood,

			19881, the actual definitions and criteria of acceptable performance are often open to strategic reinterpretation and manipulation."
		Control	"Controlling tactics, by comparison, are specific efforts to establish power and dominance over the external constituents that are applying pressure on the organization. Several empirical studies from an institutional perspective have noted that struggles for power and control often underlie institutional processes (Covaleski & Dirsmith, 1988; Rowan, 1982; Tolbert, 1985, 1988; Tolbert & Zucker, 1983). Control is a more actively aggressive response to institutional pressures than co-optation and influence because the organization's objective is to dominate rather than to influence, shape, or neutralize institutional sources or processes. Organizations are more likely to use controlling tactics when institutional expectations are incipient, localized, or weakly promoted. By way of an example, an organization may be more inclined to attempt domination of a small advocacy group that has recently opposed its products or practices than a large institutionally powerful organization that has vocalized its criticisms of the organization widely and over a protracted period of time. Organizations also may attempt to exert control over the allocation or expression of social approval by external constituents. For example, an organization may attempt to control the budgetary processes used to assess the value of the organization's social and economic contributions (Covaleski & Dirsmith, 1988; Pfeffer & Moore, 1980; Pfeffer & Salancik, 1974) or strive to alter the way in which organizational achievements and transgressions are announced to the public. Co-opting, influencing, and controlling tactics constitute more active strategic responses to institutional pressures than alternative strategies in that pressures and expectations are not taken as a given constraint to be

			obeyed or defied. Instead, organizations actively alter, re-create, or control the pressures themselves or the constituents that impose them."

Appendix C Features and Components

Observation Table per Organization

Organization	1	2	3	4	5	6	7	8	9	10
Features										
Number of pages	206	16	22	12	9	12	4	31	24	13
Revision	x			x	x	x	x	x		x
Medium	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic
Document Type/Title	Complete Policy	Policy Summary	Individual Policy	Policy Summary	Compliance Plan	Individual Policy	Individual Policy	Corporate Compliance Plan	Compliance Plan	Corporate Compliance Manual and Code of Conduct
Defines duties and responsibilities	x	x	x	x	x	x	x		x	
Training program description and requirements	x		x	x	x	x		x	x	
Define the program's overall operation, reporting requirements, how investigations will occur, corrective responses, issue management, continuous evaluation, and auditing.	x	x	x	x	x	x	x	x	x	
Duties and responsibilities for each area of the organization	x	x	x	x	x	x		x	x	x
Description of how interdepartmental interactions shall occur between compliance, audit, operations, legal, and human resources.	x			x				x		x
Key performance indicators of program effectiveness	x				x					
Components										
Header block										
Title	x	x	x	x	x	x	x	x	x	x
Department acountable for policy	x	x	x	x	x		x	x		x
Effiective date	x			x		x	x			
Policy identification number						x	x		x	x
Approval Date	x			x		x	x	x	x	
Approving authority	x			x	x	x	x		x	
Statement if it modifies or replaces existing policy	x			x			x	x		
Number of Pages	x					x	x	x		
Background								x	x	x
Purpose	x			x	x		x	x		
Definitions	x	x	x				x		x	
Scope				x					x	x
Policy Statements	x		x	x	x	x	x	x	x	x
Procedures	x	x	x	x	x	x	x	x	x	x
Related Policies		x				x				
Refernces/Citations	x		x	x		x	x		x	

Figure 5 Features and Components Observation Table per Organization 1-10

Organization	11	12	13	14	15	16	17	18	19	20
Features										
Number of pages	8	6	5	54	191	33	12	28	18	4
Revision			x							
Medium	Electronic	Electronic	aper/Electron	Electronic	Electronic	Electronic	Web page	Electronic	Electronic	Electronic
Document Type/Title	Compliance Plan	Compliance Program Description	Compliance and HIPPA Training	Compliance and Ethics Program	Corporate Compliance and Ethics Program	Compliance Plan	Compliance Policy	Code of Conduct and Compliance Program	Compliance Plan	Compliance Program
Defines duties and responsibilities	x	x	x	x	x	x	x	x	x	x
Training program description and requirements	x	x		x	x	x	x	x	x	x
Define the program's overall operation, reporting requirements, how investigations will occur, corrective responses, issue management, continuous evaluation, and auditing.	x			x	x	x	x	x	x	x
Duties and responsibilities for each area of the organization	x	x		x	x	x	x	x	x	x
Description of how interdepartmental interactions shall occur between compliance, audit, operations, legal, and human resources.				x	x	x	x	x		
Key performance indicators of program effectiveness	x				x			x		
Components										
Header block								x	x	x
Title	x	x	x	x	x	x	x	x	x	x
Department acountable for policy	x			x	x		x		x	x
Effiective date				x	x		x	x		x
Policy identification number					x					
Approval Date				x	x		x			x
Approving authority				x	x				x	x
Statement if it modifies or replaces existing policy										
Number of Pages	x			x		x		x		
Background			x	x				x		
Purpose	x			x	x			x		
Definitions		x			x	x				
Scope		x		x	x	x				x
Policy Statements	x		x	x	x	x	x	x	x	x
Procedures	x		x	x	x	x	x	x		x
Related Policies						x		x		x
Refernces/Citations		x		x	x	x		x	x	x

Figure 6 Features and Components Observation Table per Organization 11-20

Organization	21	22	23	24	25	26	27	28	29	30
Features										
Number of pages	8	10	21	14	19	64	6	32	20	7
Revision										
Medium	Electornic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic	Electronic
Document Type/Title	Corporate Compliance Plan	Corporate Compliance Policy & Procedure	Compliance Standards of Conduct	Hospital Compliance Plan	Compliance Plan	Integrity and Compliance Program New Hire Training	Hospital Compliance Plan	Compliance Manual	Compliance Program Oversight	Corporate Compliance Code of Conduct - Policy '+ Corporate
Defines duties and responsibilities	x		x	x	x	x	x	x	x	x
Training program description and requirements		x		x	x	x	x	x	x	
Define the program's overall operation, reporting requirements, how investigations will occur, corrective responses, issue management, continuous evaluation, and auditing.	x	x		x	x	x	x	x	x	x
Duties and responsibilities for each area of the organization						x	x	x	x	
Description of how interdepartmental interactions shall occur between compliance, audit, operations, legal, and human resources.						x	x			
Key performance indicators of program effectiveness										
Components										
Header block	x									
Title	x	x	x	x	x	x	x	x	x	x
Department acountable for policy			x	x			x		x	
Effiective date	x	x	x				x			x
Policy identification number		x	x				x			
Approval Date					x		x			x
Approving authority			x	x	x		x			x
Statement if it modifies or replaces existing policy		x	x				x			
Number of Pages		x		x						
Background										
Purpose				x						
Definitions		x				x	x			x
Scope		x	x		x	x	x			
Policy Statements	x	x	x		x	x	x	x	x	x
Procedures	x	x	x	x	x	x	x	x	x	x
Related Policies				x	x		x	x		

Figure 7 Features and Components Observation Table per Organization 21-30

Organization	**31**	**32**	**33**	**Number of documents**	**%**
Features					%
Number of pages	34	29	33		
Revision					
Medium	Electronic	Electronic	Electronic		
Document Type/Title	Compliance Plan	Compliance Program	Integrity and Compliance program		
Defines duties and responsibilities	x	x	x	30	91%
Training program description and requirements	x			24	73%
Define the program's overall operation, reporting requirements, how investigations will occur, corrective responses, issue management, continuous evaluation, and auditing.	x	x	x	29	88%
Duties and responsibilities for each area of the organization	x	x	x	25	76%
Description of how interdepartmental interactions shall occur between compliance, audit, operations, legal, and human resources.	x		x	14	42%
Key performance indicators of program effectiveness				5	15%
Components				Number of Documents	%
Header block				4	12%
Title	x	x	x	33	100%
Department acountable for policy		x	x	20	61%
Effiective date	x	x	x	17	52%
Policy identification number			x	9	27%
Approval Date		x		14	42%
Approving authority		x		16	48%
Statement if it modifies or replaces existing policy			x	8	24%
Number of Pages				10	30%
Background				6	18%
Purpose	x	x	x	13	39%
Definitions	x		x	14	42%
Scope	x	x		15	45%
Policy Statements	x	x	x	30	91%
Procedures	x	x	x	31	94%
Related Policies	x	x	x	12	36%
Refernces/Citations	x		x	22	67%

Figure 8 Features and Components Observation Table per Organization 31-33 and Summary

Appendix D – Organizations and Policy

Documents List

Hospital	Document Name/Type
Adventist Health	Complete Policy
Beth Israel Lahey	Policy Summary
Beverly Hospital	Individual Policy
Bradford Regional Medical Center	Policy Summary
Broward Health	Compliance Plan
Craig Hospital	Individual Policy
HealthQuest	Individual Policy
Johns Hopkins	Corporate Compliance Plan
Jones Memorial Hopspital	Compliance Plan
Lackey Memorial Hospital	Corporate Compliance Manual and Code of Conduct
Loretto Hospital	Compliance Plan
Main Line Health	Compliance Program Description
Newton Wellesley Hospital	Compliance and HIPPA Training

Nuvance Health	Compliance and Ethics Program
NYC Health and Hospitals	Corporate Compliance and Ethics Program
Promedica Health System	Compliance Plan
Shawnee Health Service	Compliance Policy
Sparrow Health System	Code of Conduct and Compliance Program
Springstone	Compliance Plan
St Johns Medical Center	Compliance Program
St Josephs Hospital Health Center	Corporate Compliance Plan
St Tammany Parish Hospital	Corporate Compliance Policy & Procedure
The Childrens Hospital of Philadelphia	Compliance Standards of Conduct
The University of Texas MD Anderson Center	Hospital Compliance Plan
Trillium Health	Compliance Plan
Trinity Health Care	Integrity and Compliance Program New Hire Training
UNC Health Care	Hospital Compliance Plan
Universal Health Services	UHS Compliance Manual

University of Kentucky Healthcare	Compliance Program Oversight
University of Missouri Health	Corporate Compliance - Code of Conduct - Policy '+ Corporate Compliance Reporting and Non-Retaliation Policy
University of Toledo	Compliance Plan
University of Washington Medicine	UW Medicine Compliance Program
Veterans Health Administration	VHA Integrity and Compliance program

Bibliography

12 most significant 2023 data breaches | NordLayer Blog. (n.d.). Retrieved July 6, 2024, from https://nordlayer.com/blog/data-breaches-in-2023/

2018 Chapter 8 | United States Sentencing Commission. (n.d.). Retrieved March 16, 2024, from https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8

Administrative Expenses in the US Health Care System Why So High? (2021). https://doi.org/10.1001/jama.2021.17318

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2020). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*, 276–289. https://doi.org/10.1016/j.cose.2006.11.004

Alec Cram, W., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly: Management Information Systems*, *43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Appari, A., Johnson, M. E., Anthony, D. L., Anderson, N., & Zezima, K. (2009). HIPAA Compliance: An institutional theory perspective. *Americas Conference on Information Systems 2009 Proceedings*, 1–9.

Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior.

Technological Forecasting and Social Change, *198*. https://doi.org/10.1016/j.techfore.2023.123028

Argyris, C. (1958). Some Problems in Conceptualizing Organizational Climate: A Case Study of a Bank. *Administrative Science Quarterly*, *2*(4), 501–520. https://doi.org/10.2307/2390797

Armour, J., Gordon, J., & Min, G. (2020). Taking Compliance Seriously. *Yale Journal on Regulation*, *37*. https://heinonline.org/HOL/Page?handle=hein.journals/yjor37&id=5&div=4&collection=journals

Arnold, V., Benford, T., Canada, J., Sutton, S. G., Bamberger, K. A., Johnson, P. R., Esayas, S., Mahler, T., Bonazzi, R., Pigneur, Y., Kwon, J., Johnson, M. E., Čyras, V., Riedl, R., Prous, J., Sheth, A., Breaux, T., Mather, T., Cram, W. A., … Albrechtsen, E. (2007). The role of external and internal influences on information systems security - a neo-institutional perspective. *MIS Quarterly*, *16*(1), 1–12. https://doi.org/10.1016/j.jsis.2007.05.004

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *59*(19), 9–25. https://doi.org/10.1016/j.cose.2016.02.007

Bieser, J., Kurzrock, B.-M., & Batra, R. (2020). Risk management in facility management for data centres : status and deficits. *Property Management*, *38*(2), 219–240. https://doi.org/10.1108/PM-11-2019-0068

Bjorck, F. (2004). Institutional theory: a new perspective for research into IS/IT security in organisations. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004.*, *00*(C), 5 pp. https://doi.org/10.1109/HICSS.2004.1265444

Boaye Belle, A., & Zhao, Y. (2023). Evidence-based decision-making: On the use of systematicity cases to check the compliance of reviews with reporting guidelines such as PRISMA 2020. *Expert Systems with Applications*, 119569. https://doi.org/10.1016/J.ESWA.2023.119569

Boyatzis, R. E. (1998). *Transforming Qualitative Information | SAGE Publications Inc*. https://us.sagepub.com/en-us/nam/transforming-qualitative-information/book7714

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly*, *34*(3), 523–548. http://web.a.ebscohost.com.ezxy.ie.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=abca585d-5313-4a51-9504-d9e7ad2afe06%40sessionmgr4010

Carboni, L. Esq. (2022, April). *A. What is a Compliance Program?* Association of Corporate Counsel Web Article. https://www.acc.com/resource-library/healthcare-compliance-programs-united-states-101#

Cazenave, B., & Morales, J. (2021). NGO responses to financial evaluation: auditability, purification and performance. *Accounting, Auditing and Accountability Journal*, *34*(4), 731–756. https://doi.org/10.1108/AAAJ-01-2020-4397

Compliance Guidance | Office of Inspector General | Government Oversight | U.S. Department of Health and Human Services. (n.d.). Retrieved March 16, 2024, from https://oig.hhs.gov/compliance/compliance-guidance/

Crain, N. V, & Crain, W. M. (2023). *The Cost of Federal Regulation to the U.S. Economy, Manufacturing and Small Business*. https://nam.org/competing-to-win/cost-of-regulations.

Daljord, Ø., Mela, C. F., Roos, J. M. T., Sprigg, J., & Yao, S. (2023). The Design and Targeting of Compliance Promotions. *Marketing Science*, *42*(5), 866–891. https://doi.org/10.1287/mksc.2022.1420

Devlin, F. (2020). RISK CULTURE , REGULATION , AND COMPLIANCE IN A PANDEMIC. *The RMA Journal*, *102*(10 (Jul/Aug 2020)), 42–44. http://ezxy.ie.edu/login?url=https://www.proquest.com/trade-journals/risk-cultureregulation-%0Acompliance-pandemic/docview/2438196724/se-2?accountid=27285

Dhillon, G., & Backhouse, J. (2003). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Donalds, C., & Barclay, C. (2022). Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. *European Journal of Information Systems*, *31*(1), 58–73. https://doi.org/10.1080/0960085X.2021.1978344

Eisenhardt, K. M. (1989). Building Theories from Case Study Research Published by : Academy of Management Stable. *The Academy of Management Review*, *14*(4), 532–550.

Freij, Å. (2020). *Using technology to support fi nancial services regulatory compliance : current applications and future prospects of regtech*. *21*(2), 181–190. https://doi.org/10.1108/JOIC-10-2020-0033

Gläser-Zikuda, M., Hagenauer, G., & Stephan, M. (2020). The potential of qualitative content analysis for empirical educational research. *Forum Qualitative Sozialforschung*, *21*(1). https://doi.org/10.17169/fqs-21.1.3443

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Guo, J. X. (2019). Measuring information system project success through a software-assisted qualitative content analysis. *Information Technology and Libraries*, *38*(1), 53–70. https://doi.org/10.6017/ital.v38i1.10603

Hassan, N. R., & Mathiassen, L. (2018). Distilling a body of knowledge for information systems development. *Information Systems Journal*, *28*(1), 175–226. https://doi.org/10.1111/isj.12126

Health Resources and Services Administration - Bureau of Primary Health Care. (2023). *Health Center Program Compliance Manual*. https://bphc.hrsa.gov/sites/default/files/bphc/compliance/hc-compliance-manual.pdf

Hsu, C., Lee, J., & Straub, D. W. (2012a). *Security Innovations*. *August 2014*.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012b). Institutional Influences on Information Systems Security Innovations. *Information Systems Research*, *23*(3-part-2), 918–939. https://doi.org/10.1287/isre.1110.0393

Hu, Q., Hart, P., & Cooke, D. (2007a). The role of external and internal influences on information systems security - a neo-institutional perspective. *Journal of Strategic Information Systems*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004

Hu, Q., Hart, P., & Cooke, D. (2007b). The role of external and internal influences on information systems security - a neo-institutional perspective. *Journal of Strategic Information Systems*. https://doi.org/10.1016/j.jsis.2007.05.004

Hulitt, E., & Vaughn, R. B. (2010). Information system security compliance to FISMA standard: A quantitative measure. *Telecommunication Systems*, *45*(2–3), 139–152. https://doi.org/10.1007/s11235-009-9248-8

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions. *Information Management & Computer Security*, *17*(5), 372–387. https://doi.org/10.1108/09685220911006678

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Insua, D. R., Couce-vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & Rasines, D. G. (2021). *An Adversarial Risk Analysis Framework for Cybersecurity*. *41*(1), 16–36. https://doi.org/10.1111/risa.13331

Kam, H. J., Mattson, T., & Goel, S. (2019). A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness. *Information Systems Frontiers*, 1–24. https://doi.org/10.1007/s10796-019-09927-9

Kam, H.-J., & Katerattanakul, P. (2013). Impact of External Pressures on Information Security Policy Compliance in the Banking Industry. *CONF-IRM 2013 Proceedings*, *July*, 1–13.

Kam, H.-J., & Katerattanakul, P. (2014). Information Security in Higher Education: A Neo-Institutional Perspective. *Journal of Information Privacy and Security*, *10*, 28–43. https://doi.org/10.1080/15536548.2014.912482

Kam, H.-J., Katerattanakul, P., & Emerick, G. (2013). Impact of External Pressures on Information Security Policy Compliance in the Banking Industry. *CONF-IRM 2013 Proceedings*, *July*, 1–13.

Kam, H.-J., Katerattanakul, P., & Gogolin, G. (2013). A Cross Industry Study: Differences in Information Security Policy Compliance between the Banking Industry and Higher Education. *Icis*, 1–19. http://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/4/

Kibiswa, N. K. (2019). Directed Qualitative Content Analysis (DQlCA): A Tool for Conflict Analysis. In *The Qualitative Report* (Vol. 24, Issue 8).

Kuiper, M. E., Chambon, M., de Bruijn, A. L., Reinders Folmer, C., Olthuis, E. H., Brownlee, M., Kooistra, E. B., Fine, A., van Harreveld, F., Lunansky, G., & van Rooij, B. (2023). A Network Approach to Compliance: A Complexity Science Understanding of How Rules Shape Behavior. *Journal of Business Ethics*, *184*(2), 479–504. https://doi.org/10.1007/s10551-022-05128-8

Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. In *Journal of Management Information Systems* (Vol. 25, Issue 2). https://doi.org/10.2753/MIS0742-1222250210

Kusserow, R. P. (2013). *Structuring Compliance Policy & Procedures with a Compliance Document Template*. https://www.compliance.com/resources/how-to-structure-compliance-policy-documents/

Kusserow, R. P. (2014). Developing and Managing Compliance Policy Documents Always Use Caution When Developing Documents for Your Organization. *Journal of Health Care Compliance*, *16*(3), 27–30.

Kusserow, R. P. (2020). Understanding the difference between Compliance and Risk Management. *Journal of Health Care Compliance*, *May-June*.

Lee, S. H., Gokalp, O. N., & Kim, J. (2021). Firm–government relationships: A social exchange view of corporate tax compliance. *Global Strategy Journal*, *11*(2), 185–209. https://doi.org/10.1002/gsj.1340

Li, N., & van Rooij, B. (2022). Law Lost, Compliance Found: A Frontline Understanding of the Non-linear Nature of Business and Employee Responses to Law. *Journal of Business Ethics*, *178*(3), 715–734. https://doi.org/10.1007/s10551-021-04751-1

Lopes, I. M., & De Sa-Soares, F. (2012). INFORMATION SECURITY POLICIES: A CONTENT ANALYSIS. *PACIS - The Pacific Asia Conference on Information Systems*. http://hdl.handle.net/10198/7421

Maxwell, J. alex. (2013). *Qualitative Research Design: An Interactive Approach 3rd Edition*. SAGE Publications Inc.

Michelberger Jr., P., & Labodi, C. (2012). After Information Security - Before a Paradigm Change (A Complex Enterprise Security Model). *Acta Polytechnica Hungarica*, *9*(4), 101–116.

Mignerat, M., & Rivard, S. (2009). Positioning the institutional perspective in information systems research. *Journal of Information Technology*. https://doi.org/10.1057/jit.2009.13

Min, B. S., Chen, C. N., & Tien, C. (2022). Firms' responses to corporate governance reform in an emerging economy from the perspective of institutional logics. *Journal of Business Research*, *147*, 278–289. https://doi.org/10.1016/j.jbusres.2022.04.025

Mishra, S., & Dhillon, G. (2006). Information Systems Security Governance Research : A Behavioral Perspective. *1st Annual Symposium on Information Assurance Academic Track of 9th Annual NYS Cyber Security Conference*, 27–35. http://www.albany.edu/iasymposium/proceedings/2006/mishra.pdf

Oliver, C. (1991). Strategic Responses To Institutional Processes. *Academy of Management Review*, *16*(1), 145–179. https://doi.org/10.5465/AMR.1991.4279002

Pascarella, G., Rossi, M., Montella, E., Capasso, A., De Feo, G., Snr, G. B., Nardone, A., Montuori, P., Triassi, M., D'auria, S., & Morabito, A. (2021). Risk analysis in healthcare organizations: Methodological framework and critical variables. *Risk Management and Healthcare Policy*, *14*, 2897–2911. https://doi.org/10.2147/RMHP.S309098

Spears, J. L., Barki, H., & Barton, R. R. (2013). Theorizing the concept and role of assurance in information systems security. *Information and Management*, *50*(7), 598–605. https://doi.org/10.1016/j.im.2013.08.004

Strauss, A. L., & Corbin, J. M. (1998). Basics of qualitative research : techniques and procedures for developing grounded theory LK - https://ie.on.worldcat.org/oclc/39257153. In *TA - TT* - (2nd ed.). Sage Publications. http://catdir.loc.gov/catdir/enhancements/fy0655/98025369-t.html

Tarantino, A. (2008). *Governance, risk, and compliance handbook : technology, finance, environmental, and international guidance and best practices*. John Wiley & Sons. https://books.google.com/books?hl=en&lr=&id=3aUyqPxYw10C&oi=fnd&pg=PR9&dq=tarantino+2008+grc&ots=sxi6DAg2BA&sig=MjxLqIke0LT8hRMAtLr5xuOMLoc#v=onepage&q=tarantino%202008%20grc&f=false

The RMA Journal. (2020). TECHNOLOGY RISK FRAMEWORK 2020. *The RMA Journal*, *103*(1 (Sep 2020)), 62–73.

Trebbi, F., Zhang, M. Ben, & Simkovic, M. (2023). The Cost of Regulatory Compliance in the United States. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.4331146

Trochim, W., & Donnelly, J. (2008). *Research methods knowledge base* (Third). Atomic Dog. http://www.anatomyfacts.com/research/researchmethodsknowledgebase.pdf

Wertheim, B. S. (2020). Tips for Fighting Off Cybercrime in 2020. *The CPA Journal*, *March 2020*, 64–67.

Westby, J. R. (2015). *Governance of Cybersecurity : 2015 Report How Boards & Senior Executives Are Managing Cyber Risks*.

Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, *23*(4), 341–354. https://doi.org/10.1007/s12525-013-0137-3

Wu, Y., & van Rooij, B. (2021). Compliance Dynamism: Capturing the Polynormative and Situational Nature of Business Responses to Law. *Journal of Business Ethics*, *168*(3), 579–591. https://doi.org/10.1007/s10551-019-04234-4

Xie, X., Shen, W., & Zajac, E. J. (2021). When Is a Governmental Mandate not a Mandate? Predicting Organizational Compliance Under Semicoercive Conditions. *Journal of Management*, *47*(8), 2169–2197. https://doi.org/10.1177/0149206320948579

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321–332. https://doi.org/10.1177/1356389013497081

Zhou, J., Fang, Y., & Grover, V. (2022). MANAGING COLLECTIVE ENTERPRISE INFORMATION SYSTEMS COMPLIANCE: A SOCIAL AND PERFORMANCE MANAGEMENT CONTEXT PERSPECTIVE. *MIS Quarterly: Management Information Systems*, *46*(1), 71–99. https://doi.org/10.25300/MISQ/2022/14727

Zhu, J., Feng, G., Liang, H., & Tsui, K. L. (2023). How Do Paternalistic Leaders Motivate Employees' Information Security Compliance? Building a Climate and Applying Sanctions. *Journal of the Association for Information Systems*, *24*(3), 782–817. https://doi.org/10.17705/1jais.00794