Internship Report on Third-Party Risk Management at BCBST

Autumn Harrison

Undergraduate, East Tennessee State University

harrisonad@etsu.edu

April 13, 2024

CSCI 4905-800

Spring 2024

Table of Contents

[Introduction 3](#_Toc163927985)

[Objectives Overview 3](#_Toc163927986)

[Coursework Analysis 6](#_Toc163927987)

[Reflection 7](#_Toc163927988)

[Conclusion 7](#_Toc163927989)

# Introduction

 Blue Cross Blue Shield of Tennessee’s IT GRC (Governance, Risk, and Compliance) serves as a comprehensive system for managing and navigating the complex landscape of regulatory requirements, internal policies, and risk management processes within the organization. It encompasses establishing governance structures and ensuring compliance with relevant laws and regulations. GRC promotes transparency, accountability, and integrity within an organization while mitigating risks and fostering sustainable business practices. Within the GRC framework, Third-Party Risk Management (TPRM) emerges as a specialized section/team specifically focused on managing the risks associated with third-party vendors, suppliers, or partners. TPRM involves identifying, assessing, and mitigating risks arising from external entities’ involvement in the organization’s operations. Additionally, TPRM ensures that third-party relationships adhere to BCBST’s risk tolerance and compliance requirements. It provides a targeted approach to safeguarding the organization from potential threats and vulnerabilities posed by its extended network of vendors, thus contributing to the overall effectiveness of GRC.

# Objectives Overview

 During my internship at BCBST, I had the opportunity to immerse myself in various aspects of Information Security and TPRM. Over the course of the past few months (Jan 22, 2024 – Present), I engaged in a diverse range of tasks aimed at expanding my knowledge and skills in the cybersecurity field. The learning objectives outlined for my internship included:

* Beginning the internship with an open, positive, growth mindset and applying what I’ve learned during my time at Blue Sky Tennessee Institute.
* Navigating and interpreting findings from Black Kite, a crucial tool in Information Security assessment.
* Generating executive summaries based on Information Security assessment answers and Black Kite findings.
* Acquiring proficiency in navigating vendor requests in Scout and locating vendor profiles in NAVEX IRM – Keylight.
* Familiarizing myself with Vendor Information Security Assessments and creating RAPIDS for Technical Assurance Council (TAC) meetings.
* Reviewing and evaluating Common Vulnerabilities and Exposures (CVE) from Black Kite vulnerability findings.
* Contract review and negotiation, specifically regarding Information Security Clauses.
* Uploading Compliance documentation into Black Kite and assessing vendor documents such as SOC2T2 to gauge their impact on different frameworks.
* Conducting annual assessments of vendors to ensure regulatory compliance with NIST 800-53 R5 standards.
* Gaining insights into quantitative risk modeling and fair quantitative risk assessment, including primary and secondary loss types.
* Deepening my understanding of data classification principles and practices.

By actively engaging in these tasks, I was able to meet all the learning objectives, as stated above, set out for my internship. For example, my first objective is: “Beginning the internship with an open, positive, growth mindset and applying what I’ve learned during my time at Blue Sky Tennessee Institute.” I achieved this by actively learning, engaging, and practicing the necessary skills taught to me by my team. I was able to overcome my own doubts by asking questions when clarification was needed, continue my own research into the software and processes utilized, and tremendously aid my team in completing work efficiently.

For understanding, Black Kite is a cybersecurity firm specializing in proactive threat detection and prevention, safeguarding businesses from digital threats. With advanced technology and expert analysis Black Kite ensures that BCBST remains resilient and secure in the digital landscape. To navigate and interpret findings in Black Kite’s software (will be referred to as Black Kite), I frequently engaged with the tool, familiarizing myself with its interface and functionalities. I utilized my analytical skills to interpret the data presented and draw meaningful insights to inform my team and write summaries. In generating executive summaries based on Information Security assessments and Black Kite findings, I applied my communication skills to distill complex information into concise and informative summaries suitable for executive review. In acquiring proficiency in navigating vendor requests in Scout and locating vendor profiles in NAVEX IRM (Keylight), I dedicated time to familiarize myself with the platforms meaning that I explored their features and functionalities to streamline the vendor management process. I also became familiar with the Annual Assessments (Information Security Vendor Assessments) by paying attention to detail and organization. My job was also to make sure that all relevant information was accurately captured and ready to present in order to support the decision-making process (Scout request approval or denial). Reviewing CVEs from Black Kite vulnerability findings required a methodical approach as I had to systematically assess each CVE and identify potential vulnerabilities and document it. For the majority of my internship, I uploaded compliance documentation into Black Kite and assessed/analyzed vendor documents such as SOC2T2. I ensured that all compliance documentation was accurately recorded and assessed its impact on the NIST 800-53 R5 framework, as there is a requirement that ALL vendors have to meet. Lastly, I deepened my understanding of data classification principles and practices by studying BCBST standards and policies. I applied the corresponding knowledge to accurately classify data and ensure that I handled sensitive data responsibly.

# Coursework Analysis

The coursework done in CSCI 3500 – Information Security and Assurance, provided me with a strong foundation in key areas directly applicable to my internship. Specifically, modules covering Information Security Management, Risk Management, Incident Response and Contingency Planning, and Legal, Ethical & Professional Issues in Information Security proved highly relevant to my role. I learned about the principles and practices of effectively managing information security within an organization. That, in turn, enabled me to understand the importance of establishing and maintaining robust security protocols and procedures, which I applied when navigating and interpreting findings from Black Kite. Risk Management coursework equipped me with the skills to identify, assess, and mitigate risks effectively. This module helped me to analyze annual assessments of vendors to ensure regulatory compliance with standards such as NIST 800-53 R5. I applied those risk management principles to majority of my tasks. The coursework on Legal, Ethical, and Professional Issues in Information Security heightened my awareness of the legal and ethical considerations surrounding Information Security practices. Ultimately, this was beneficial during contract review regarding Information Security clauses. Overall, the coursework in CSCI 3500 provided me with a strong foundation and practical skills necessary to navigate the complexities of TPRM.

# Reflection

 The internship experience has a significant impact on my short-term, mid-term, and long-term career goals. In the short term, I have an intrigued interest in pursuing a career in cybersecurity and TPRM. The hands-on experience gained at BCBST has provided valuable insights into the field, motivating me to further my education by pursuing a master’s degree in cybersecurity and obtaining relevant certifications. In the mid-term, I plan to leverage the skills and experience gained during the internship to secure a position in TPRM, using my knowledge to contribute effectively to the organization. Staying at BCBST for a few years after graduation will allow me to gain practical experience and deepen my expertise in the field. In the long term, I aim to continue learning and adapting to the evolving digital landscape, staying updated of emerging technologies and best practices in cybersecurity to remain a proficient and effective professional in the field. Furthermore, in the future, I hope to become an entrepreneur and utilize all my knowledge and abilities to drive me to success.

# Conclusion

 In conclusion, my internship experience at Blue Cross Blue Shield of Tennessee has been both rewarding and transformative, allowing me to apply theoretical knowledge from my coursework to real-world situations and gain valuable insights into the marketing industry. I am grateful for the opportunity to learn and grow professionally, and I am confident that the skills and experiences I have gained during my internship will serve me well in my future career endeavors. I am hopeful that I will continue to enjoy and benefit in the future months during my internship.