CENTRAL MINDANAO UNIVERSITY

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

IT SECURITY AUDIT FOR AMA COMPUTER LEARNING CENTER

JHO ANNA MARIE H. CASTRO

KERTZBY KYZA G. COLIPANO

EDGAR JR FLORES

PRINCE ZELJAY KENT INVENTO

KHENT MARK J. DAHAY

MEREAL KATE C. SILVESTRE

JIU AXL R. TABILLA

MAY 2024

TABLE OF CONTENTS

CHAPTER 1

BACKGROUND OF THE PROJECT

Introduction

Almost every institution is increasingly reliant on Information Technology Systems. The security of storing, processing, and managing sensitive information is dependent on the system. Due to this reliance comes the risk of cyber threats that can compromise the confidentiality, integrity, and availability of data. Cyber attacks, data breaches, and other security incidents can have serious consequences for institutions, including financial losses, reputational damage, and legal liabilities. Therefore, institutions need to assess and enhance their IT security posture regularly.

Overview of The Project

The project aims to conduct a comprehensive IT Security Audit for an institution to assess and enhance its cybersecurity posture. The institution's existing IT security policies, procedures, and infrastructure will be evaluated to identify vulnerabilities and risks. The audit will include a thorough examination of the institution's IT systems, networks, applications, and security controls to ensure they are adequately protecting sensitive information and mitigating potential threats. Stakeholder input will be crucial in understanding the institution's security concerns and requirements, guiding the audit process toward addressing specific security challenges.

Key components of the project include planning the audit scope, objectives, and methodologies; collecting data on the institution's IT infrastructure and security practices; conducting risk assessments and compliance evaluations; and performing security testing to identify and exploit vulnerabilities. The project will culminate in the preparation of a comprehensive audit report that details the findings, including identified risks and vulnerabilities, along with recommendations for remediation and security improvement. This report will serve as a roadmap for the institution to enhance its cybersecurity posture and protect against future security threats.

Overall, the IT Security Audit project aims to provide the institution with valuable insights into its current security posture and vulnerabilities, enabling it to strengthen its defenses and protect sensitive information. By implementing the recommendations outlined in the audit report, the institution can enhance its cybersecurity resilience and reduce the risk of data breaches and cyber-attacks. The project will ultimately contribute to the institution's ability to maintain a secure and trusted IT environment for its stakeholders.

Problem Statement

Institutions face significant challenges related to cybersecurity which threatens the confidentiality, integrity, and availability of sensitive information. These institutions often face vulnerabilities that can lead to data breaches. A common issue is the lack of comprehensive cybersecurity measures, including policies, and procedures, leaving an institution susceptible to cyber attacks. Additionally, there is often a lack of awareness among the institution about the best practices for cybersecurity which further increases security concerns. Addressing these challenges is crucial to protect the integrity, confidentiality, and availability of sensitive information within the institution.

Hypotheses

Based on the questionnaire and problem statement, the project has the following hypotheses:

HO1. ACLC fails in IT security assurance in the areas:

1. An updated and credible security software to prevent viruses, malware, cyber-attacks, and internal attacks.
2. To have institutionally published security policies to make all employees aware of security protocols.
3. A dedicated Information Assurance Security office to handle security aspects.
4. To regularly update security patches and vulnerabilities on devices that store or process sensitive information.
5. An industry standard logging and monitoring on devices that store or process sensitive information.

Conceptual Framework

The conceptual framework for this project revolves around the implementation of various cybersecurity strategies and protocols within the institution. This includes policies, procedures, technical solutions, and educational initiatives aimed at safeguarding sensitive information and preventing unauthorized access. The framework also considers the collaboration between different stakeholders within the university, including IT departments, administrative staff, faculty, and students, to ensure the effective implementation and enforcement of cybersecurity measures.

Significance of The Project

The significance of this project lies in advancing the cybersecurity practices within the institution. Recognizing the significant risk that cyberattacks pose to sensitive information, this study investigates the issues and proposes solutions. The project intends to empower the institution to establish a more secure environment by implementing comprehensive cybersecurity measures. This project will be particularly significant to the following users:

1. Institutions

The implementation of the project will benefit the institutions as it will significantly improve the protection of sensitive information. This study would also emphasize raising awareness and training on cybersecurity best practices, fostering a culture of security awareness among all personnel. This will allow the institution to encourage compliance with data security standards, reducing the risk of penalties and fostering trust with the stakeholders.

2. Students

This study aims to improve data protection for sensitive information such as personal information, minimizing the risk of exposure to data breaches. By establishing cybersecurity awareness through this project, students will be better equipped to identify and avoid cyber threats, allowing them to protect themselves both within the institution and in their personal lives.

3. Staff

Robust cybersecurity is a big advantage in easing the burden on employees or staff by mitigating the frequency and severity of cyberattacks. A secure environment fosters trust and minimizes concerns about future data breaches.

4. Administrators

This project will provide the administrators with valuable information about vulnerabilities and best practices, allowing them to make informed decisions regarding resource allocation and investments in cybersecurity solutions. By resolving

vulnerabilities and adhering to data security regulations, the administration minimizes the risk of legal and financial consequences from data breaches all the while protecting the institutions' reputation and fostering stakeholders' trust.

5. MIS Office

This project holds importance for the MIS Office, as they will be the driving force behind adopting the proposed cybersecurity solutions. The research will prepare them to effectively address institutional vulnerabilities by identifying the weaknesses in the current security system. By this, the MIS Office can strategically deploy resources to areas with the highest risk as well as evaluate and choose the most effective security tools based on the specific threats identified. Furthermore, the study's recommendations will serve as a guide for developing a comprehensive security plan that safeguards all aspects of data protection. Finally, ongoing monitoring and maintenance of these systems are crucial, and the study can provide the office with the best practices for maintaining long-term security vigilance.

Review of Related Projects

A. Audit for Information Systems Security

Authors: Suduc, Ana-Maria; Bizoi, Mihai; Filip, Florin Gheorghe; et al.

Copyright: 2010

Problem: The stated problem in the paper is the vulnerability of information systems to inside or outside attacks despite significant advances in information security. The authors argue that the existence of an internal audit for information system security can increase the probability of adopting adequate security measures and preventing these attacks or lowering their negative consequences.

Findings: The paper highlights the vulnerability of information systems to attacks despite advancements in security. It emphasizes the need for internal audits to increase the adoption of adequate security measures and prevent or mitigate the negative consequences of attacks. The digital world's benefits come with significant risks, including physical (equipment-related) and logical (unauthorized access and data destruction) risks. Organizations must address security, availability, performance, and compliance risks, which can cost millions in incidents. A study in Romania revealed high intentional misuse of information systems, driven by curiosity, personal gain, and intellectual challenge. Lack of awareness among users about ICT-related risks underscores the need for security education. Overall, the findings stress the importance of effective security measures and regular audits to protect information systems.

B. IT Security Audit

Author: Barzilay, Micky

Copyright: 2019

Problem: The study elaborated on the problems of cybercrime, fraud, and data breaches which are significant threats to organizations. Due to those problems, it leads to substantial losses. Companies need effective strategies to combat these threats and prevent further financial and reputational damage.

Findings: The research revealed that 50% of participants believed that security audits have a significant impact on improving an organization's IT security, while 36% believed they could yield some improvement. However, 14% thought that IT security audits, while important, have no impact on information security improvement. Additionally, 100% of participants were aware of cybercrime risks, with varying levels of personal engagement in cybersecurity activities. Furthermore, 57% of respondents claimed to be very familiar with IT security audit standards and guidelines, and their organizations follow these standards, highlighting the importance of regular security audits for enhancing information system security.

C. The IT Audit Objective Research Based on the Information System Success Model under the Big Data Environment

Authors: Li, Tingliao; Chen, Lianghua
Copyright: 2015

Problem: Information systems in the big data environment exhibit characteristics such as Volume, Velocity, Variety, and Value, presenting new challenges for auditing. However, current audit objectives often focus more on the characteristics of the information systems themselves and less on specific business objectives, leading to potential gaps in auditing practices.

Findings: The study analyzed the influence of information systems under big data conditions and identified potential risks. It proposed an information system audit target system based on the Information System Success Model (D&M model). The research revealed that big data has significantly changed various sectors, enhancing data resource value and management. However, it also highlighted challenges such as data management inefficiencies, safety risks, privacy leaks, and inaccurate data analysis. The study emphasized the importance of effective data management in leveraging big data's potential benefits while mitigating its associated risks.

D. A Security Audit Framework to Manage Information System Security

Authors: Pereira, Teresa; Santos, Henrique

Copyright: 2010

Problem: The increasing reliance on technology for business operations and transactions has made information systems security management a critical concern for organizations. However, current audit objectives often focus more on the characteristics of the information systems themselves and less on specific business objectives, leading to potential gaps in auditing practices.

Findings: The study proposes a conceptual framework to improve security management by classifying attacks, identifying assets, and mitigating vulnerabilities and threats. The framework is based on a conceptual model that represents semantic concepts and relationships in the information security domain, aligned with the ISO/IEC_JTC11 security standard. This approach aims to assist organizations in evaluating their security information management performance and reviewing existing security practices through regular security audits. The framework provides a structured approach to managing and auditing information systems security, enhancing organizations' ability to protect critical assets.

E. A Client-Centered Information Security and Cybersecurity Auditing Framework

Authors: Antunes, Mário; Maximiano, Marisa; Gomes, Ricardo

Copyright: 2022

Problem: Information security and cybersecurity management are crucial for modern enterprises, with standards like ISO 27000 and the NIST Cybersecurity Framework being widely used. However, implementing these standards can be challenging, especially for Small and Medium-sized Enterprises (SMEs), as existing frameworks may not fit their needs or be too complex for their scale. The auditing processes involved in assessing and mitigating information security risks are often time-consuming and require specialized teams, leading to a lack of flexibility and diversity in the auditing results.

Findings: To address these challenges, the paper proposes a generic and client-centered web-integrated cybersecurity auditing information system. This system aims to provide flexibility and adaptability to various auditing processes, allowing for the loading of predefined controls' checklists and mitigation tasks. The system was tested in an ISO 27001:2013 information security auditing project involving fifty SMEs. The results showed that the system's architecture and design were effective in meeting both SMEs' and large enterprises' auditing requirements. The system's flexibility allows it to accommodate checklists and mitigation lists based on other standards, such as NIST-CSF or ISO 22301:2012, making it a versatile tool for cybersecurity auditing. The system also includes features like a centralized auditing management dashboard and statistical analysis module to enhance auditing teams' effectiveness and provide SMEs with tools for self-assessment and self-auditing.

Definition of Terms

IT Security Audit: A comprehensive evaluation of an institution's IT systems, networks, applications, and security controls to identify vulnerabilities and risks, to enhance its cybersecurity posture.

Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks, often involving the prevention, detection, and response to cyber threats.

Vulnerabilities: Weaknesses in an institution's IT systems or security controls that could be exploited by attackers.

Risks: Potential events or incidents that could negatively impact an institution's IT systems, networks, or operations.

Stakeholders: Individuals or groups with an interest in the institution's IT security, including management, employees, customers, and regulatory bodies.

Compliance: Adherence to relevant laws, regulations, and standards related to IT security and data protection.

Risk Assessment: The process of identifying, analyzing, and evaluating potential risks to an institution's IT systems and data.

Security Controls: Measures implemented to protect an institution's IT systems and data, including technical, administrative, and physical controls.

Security Testing: Evaluation of an institution's IT systems and security controls to identify vulnerabilities and assess their effectiveness.

Audit Report: A document summarizing the findings of an IT security audit, including identified risks and vulnerabilities, and recommendations for remediation.

Data Breach: Unauthorized access, disclosure, or acquisition of sensitive information, potentially leading to harm or loss for the institution and individuals.

Cyber Attacks: Malicious activities aimed at disrupting, accessing, or damaging an institution's IT systems, networks, or data.

Sensitive Information: Information that requires protection due to its confidentiality, integrity, or availability requirements.

Security Awareness: Knowledge and understanding of cybersecurity risks and best practices among an institution's personnel.

Penalties: Punitive measures imposed on an institution for failing to comply with data security standards or regulations.

Data Security Regulations: Laws and guidelines governing the protection of data, including requirements for data encryption, access controls, and breach notification.

CHAPTER 2

METHODOLOGY AND IMPLEMENTATION

Research Design

The project will be adopting the use of a descriptive type of research design in collecting the data from respondents. This research aims to describe the current state of AMA Computer Learning Center's IT security posture. In addition, the proponents will focus on gathering in-depth information through the use of interviews and survey questionnaires in which these discussions will be designed to explore the perceptions of security vulnerabilities, awareness levels, and existing practices.

This project aims to determine and understand the institutions' perceptions of IT Security vulnerabilities and risks which might involve uncovering concerns about the specific weaknesses, the potential consequences of security breaches, and the likelihood of cyber attack. In addition, the project also aims to identify the challenges faced in maintaining good cybersecurity practices such as the limitations of technical knowledge within the institution that might hinder security awareness. Moreover, by understanding the current state of IT security in the institution, the project will be able to assess the level of awareness among the faculties regarding best practices and security policies. By these, the proponents can identify any gaps or inconsistencies between the actual practices as will be revealed through the interviews. By employing a qualitative approach for this research, this project aims to understand the institutions' perceptions, awareness, experiences, as well as security controls.

Data Collection Strategy and Sampling Method

To achieve this project, the proponents have formulated and produced survey questionnaires, which will be used to gather information for the security assurance audit. These questionnaires will be sent to the AMA Computer Learning Center. However, before sending out the questionnaires, the proponents must first ask for permission through a signed communication letter to the MIS director. This step is crucial to ensure that the audit process is conducted with the necessary cooperation and authorization from the institution.

The information gathered through the survey using the created questionnaire will be complemented by short interviews with the MIS faculty and personnel. These interviews will provide additional insights and context to the data collected through the survey, helping to ensure a comprehensive and accurate assessment of the institution's IS security posture.

A combination of purposive and convenience sampling will be used. The survey questionnaire will be distributed to the specific individuals within the ACLC that are directly involved in information security. By that, the data collected is relevant to the project audit.

Moreover, convenience sampling will be useful to gather data and information to those readily available and willing participants which can help expedite the data collection process.

Statistical Treatment Strategy

To analyze the data gathered through questionnaires, the proponents will use descriptive statistics. Descriptive statistics will help summarize the responses and provide an overall picture of the state of the cybersecurity practices at Bukidnon State University. To achieve this, both mean and standard deviation will be incorporated, the mean summarizes the dataset into a single value that is representative of the entire set of data. Furthermore, standard deviation provides a quantification of the variability or consistency of the data. A higher standard deviation indicates that data points are spread out over a wider range, while a lower standard deviation indicates that data points are clustered closer to the mean.

SPSS will be used to perform these statistical analyses. SPS provides an interface for conducting a wide range of statistical analyses. By using these statistical analyses and software tools, the proponents can gain valuable insights into the cybersecurity practices at Bukidnon State University and make informed recommendations for improvement.

CHAPTER 3

TABULATION AND PRESENTATION OF DATA

Data Gathering

The data collection initially started through an interview with Mr. Manuel T. Abarques Jr., the MIS Supervisor of AMA Computer Learning Center (ACLC). The interview was conducted to provide a qualitative understanding of the institution's present IT security practices and challenges. The interview allowed the researchers to collect necessary information critical for understanding the nuances of IT Security within the framework of ACLC.

Statistical Analysis

In the data processing stage, the collected data underwent quantification and cleaning as needed to ensure its accuracy and reliability for analysis. Quantification involved converting qualitative data, such as responses from interviews or surveys, into quantitative data that could be analyzed statistically. This process included assigning numerical values to qualitative responses or categorizing responses into predefined categories.

The statistical analysis of the data involved calculating descriptive statistics such as the mean, standard deviation, and skewness for each area of IT security assurance. These measures provided valuable insights into the central tendency, variability, and distribution of responses, respectively. The analysis helped identify areas of strength and weakness in IT security practices at ACLC, guiding future improvements and initiatives. The statistical analysis was conducted using Excel.

Descriptive Statistics

Descriptive statistics such as mean, standard deviation, and skewness were used to summarize and describe the data. The mean represented the average response for each area of IT security assurance, the standard deviation indicated the spread of responses around the mean, and skewness measured the asymmetry of the data distribution.

Computation

The mean was calculated as the sum of all responses divided by the number of responses. The standard deviation was calculated using the formula:

$$\bar{x} = \frac{\sum x}{n}$$

Where,

x = ith observation,

∑x = Sum of observations

n = Number of observations

The Standard Deviation was calculated as the square root of the sum of the squared differences between each response (xi) and the average response, divided by the number of responses minus one. This measure helps the researchers understand the average variability or spread of the responses from the average response. The standard deviation was calculated using the formula:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(X_i - \mu)^2}$$

Where,

σ = Population standard deviation symbol

μ = Population mean

N = total number of observations

The skewness was calculated as the sum of three times the difference between the average and the middle value divided by the standard deviation. The skewness was calculated using the formula:

$$\text{Skewness} = \frac{\sum_{i}^{N}(X_i - \bar{X})^3}{(N-1) * \sigma^3}$$

where;

N = number of variables in the distribution

Xi = random variable

X = mean of the distribution

σ = standard deviation

Data Visualization

Using Excel, the data were organized into spreadsheets format, with each row representing a respondent and each column representing a specific area of IT security assurance. The mean, standard deviation, and skewness for each area were calculated using Excel's built-in functions. Descriptive statistics were computed to summarize the data and identify patterns in security practices at ACLC. Additionally, Excel's charting capabilities were utilized to create graphs that visually displayed the data to further analyze and interpret the findings.

i. **Data Tabulation**

Area of IT Security Assurance	Mean	Standard Deviation	Skewness
Cyber Security Policies	**3.533**	**1.060**	**-0.515**
Data Transmission Protection	**3.533**	**0.990**	**-0.869**
Firewall Protection	**3.6**	**1.121**	**-0.463**
Cyber-security Personnel	**3.333**	**0.816**	**-1.649**
User Education Program	**3.667**	**1.113**	**-0.665**
External Audits	**3.333**	**0.900**	**-0.780**
Anti-Malware Software	**3.467**	**0.915**	**0.757**
Unique Usernames and Passwords	**3.267**	**1.033**	**-2.411**
Access Control	**3.667**	**0.724**	**0.628**
Vulnerability Scanning	**3.733**	**0.884**	**0.601**
Vulnerability Remediation	**3.667**	**1.345**	**-1.324**

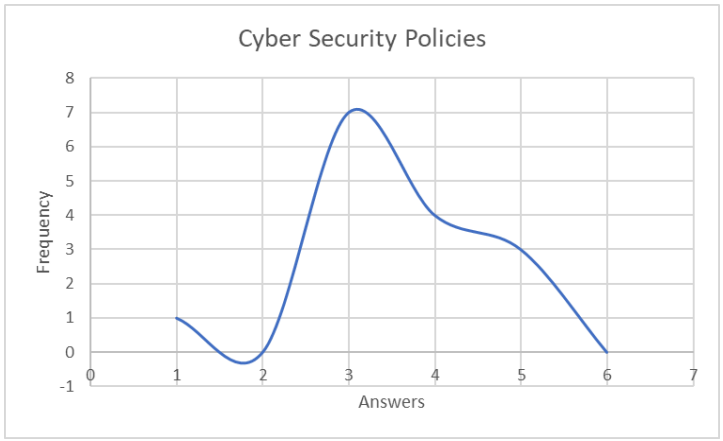
Ports and Services Control	**3.733**	**0.799**	**0.555**
Patch Deployment	**3.533**	**0.915**	**0.532**
Laptop Encryption	**3.333**	**0.976**	**0.276**
Mobile Device Management	**3.4**	**0.737**	**0.396**
Mobile Device Access Control	**3.6**	**0.910**	**0.315**
Incident Response Team	**3.333**	**1.234**	**-1.266**
Information Sharing Policies	**3.667**	**0.900**	**0.101**
2-Factor Authentication	**3.533**	**0.834**	**0.306**
Logging and Monitoring	**3.333**	**0.816**	**1.077**
Web Access Control	**3.467**	**0.834**	**0.547**
Email Protection	**3.733**	**0.884**	**-0.116**
Cyber-intel Sharing	**3.067**	**1.100**	**-1.263**
Phishing Testing	**2.667**	**1.291**	**-0.426**

Table 1. Result

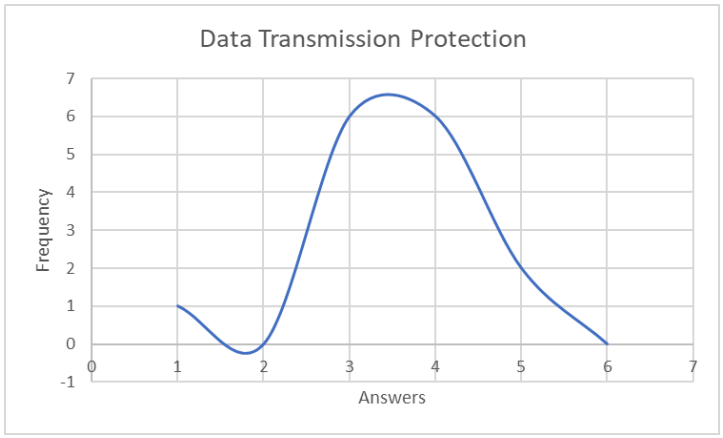
Tabulation and presentation of data for IT security assurance at AMA Computer Learning Center (ACLC) were essential for summarizing the findings of the study. A tabular form of data was used to organize the mean, standard deviation, and skewness for each area of assessment. This format allowed for a clear and concise presentation of the results, facilitating easy comparison and interpretation by stakeholders and decision-makers. The tabulated data was presented in a structured manner, highlighting key findings and trends in IT security practices at ACLC.

i. SKEWNESS

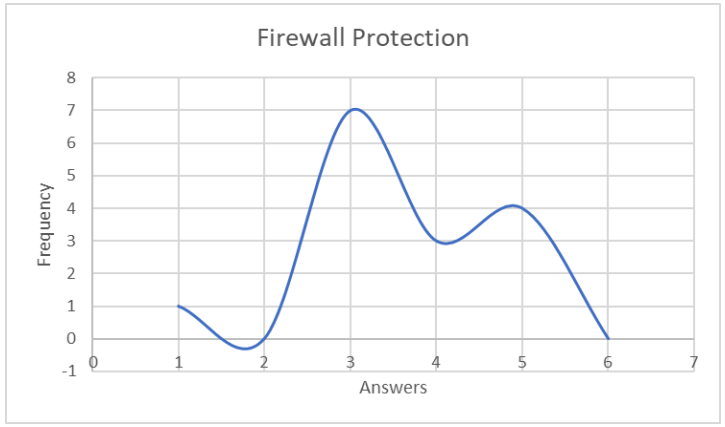
a. Cyber Security Policies



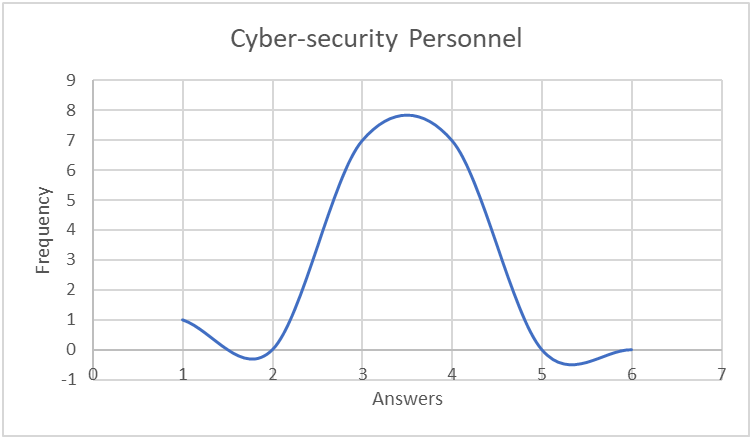
b. Data Transmission Protection



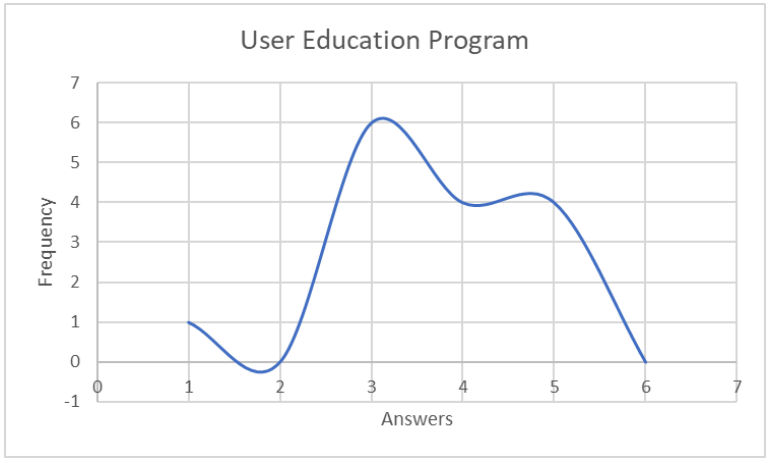
c. Firewall Protection



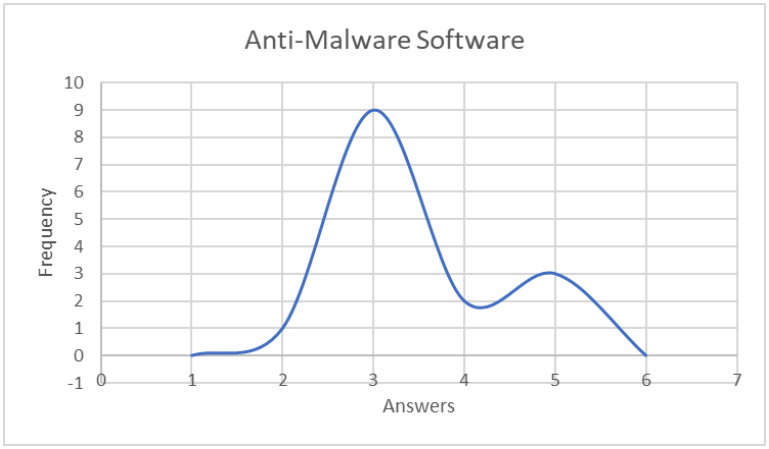
d. Cyber-security Personnel



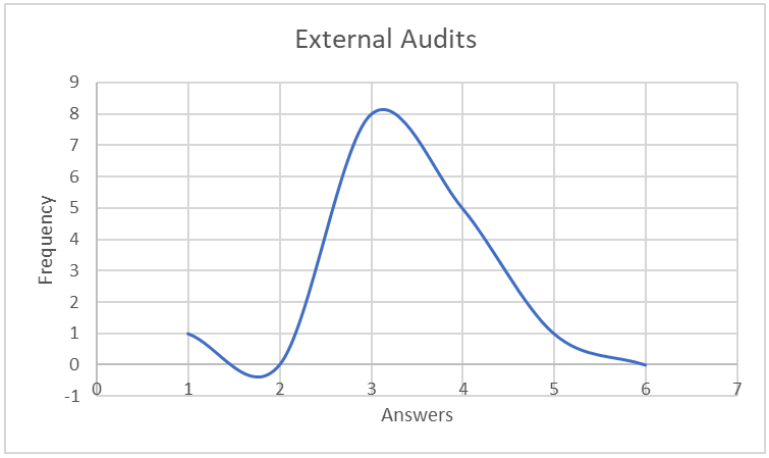
e. User Education Program



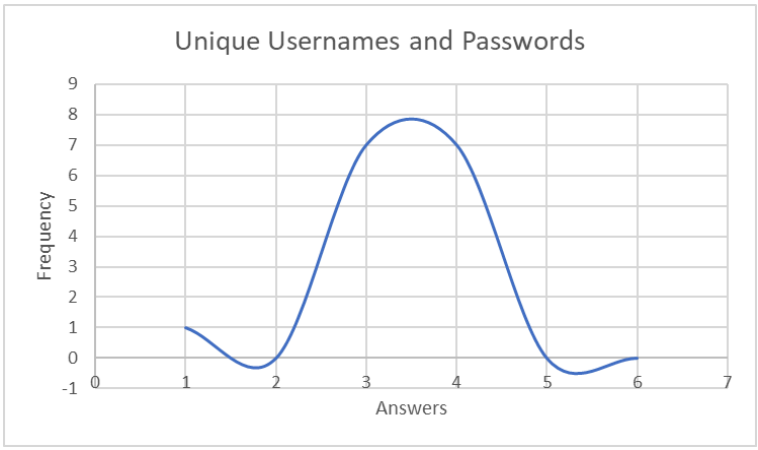
g. Anti-Malware Software



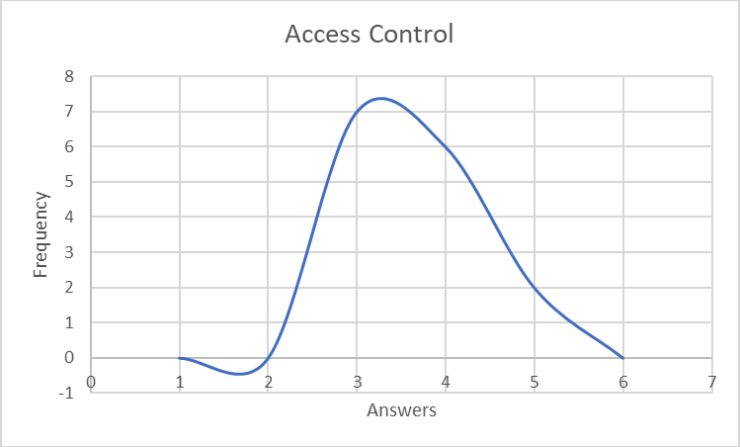
f. External Audits



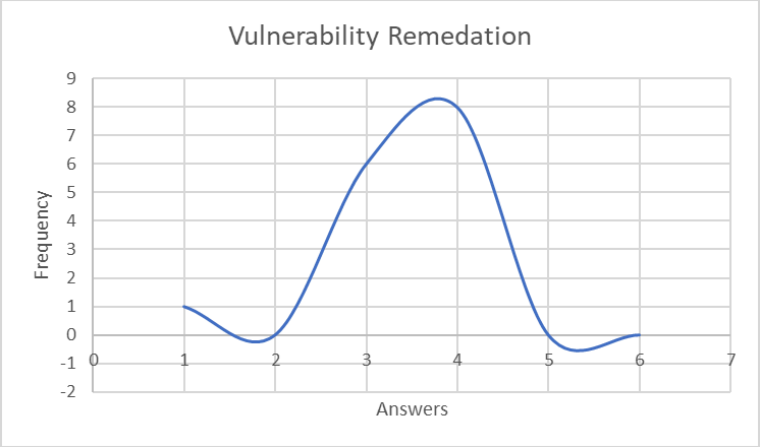
h. Unique Usernames and Passwords



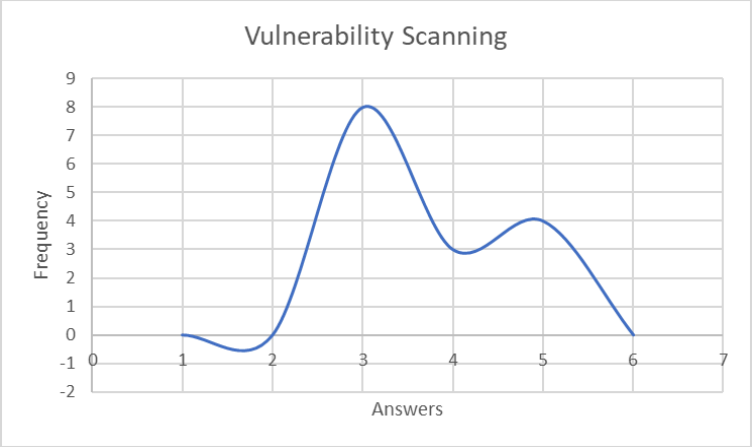
i. Access Control



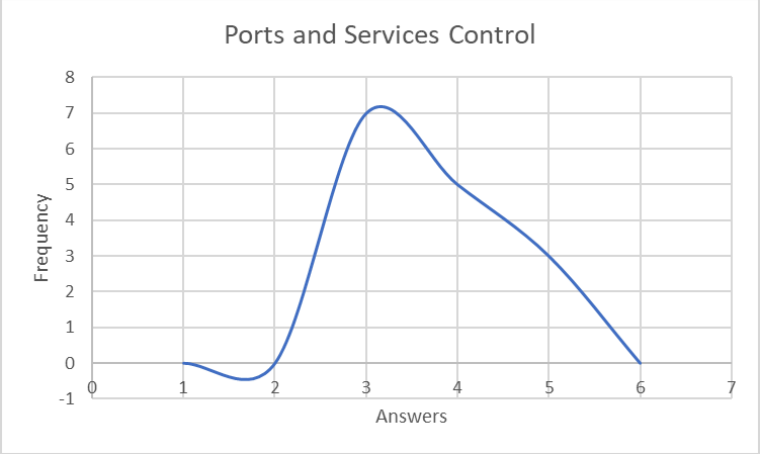
k. Vulnerability Remediation



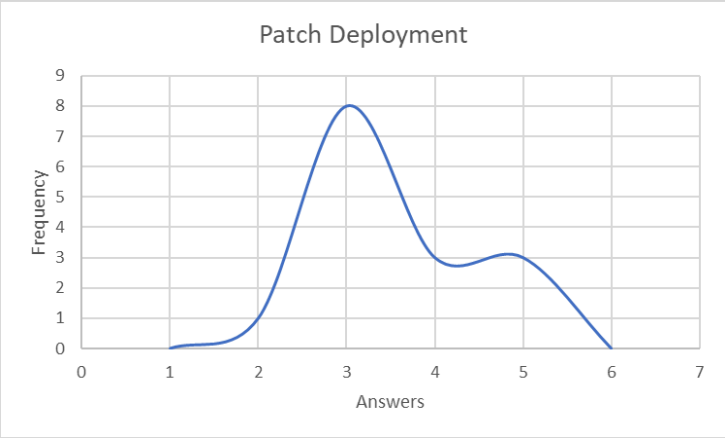
j. Vulnerability Scanning



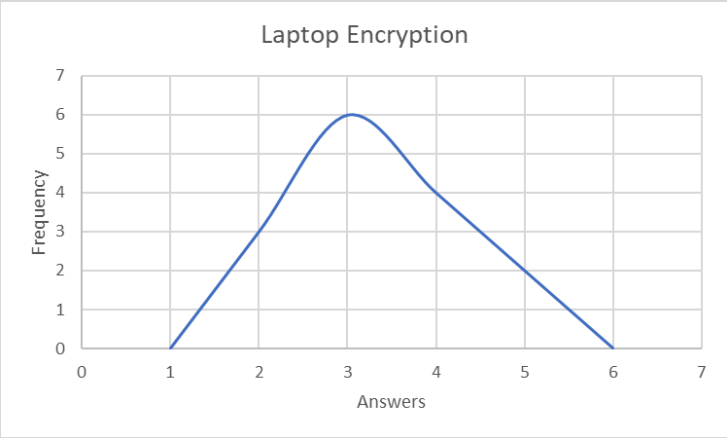
l. Ports and Services Control



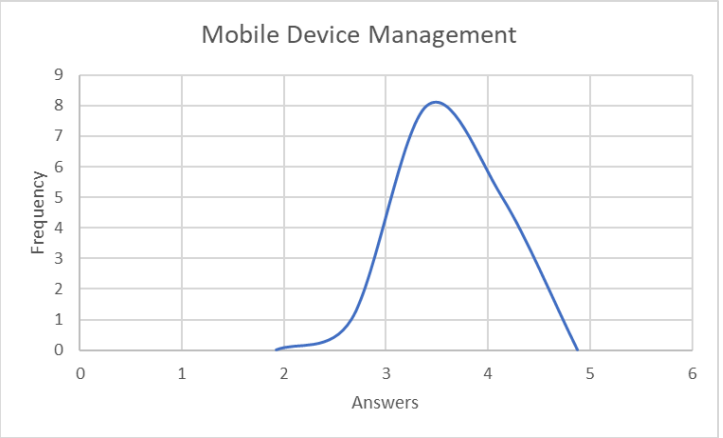
m. Patch Deployment



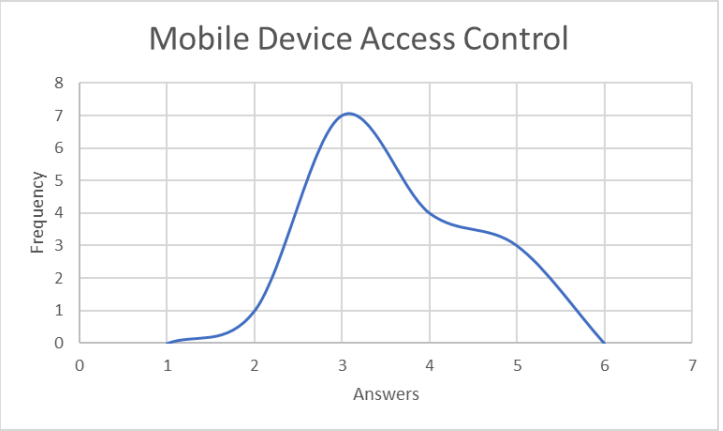
n. Laptop Encryption



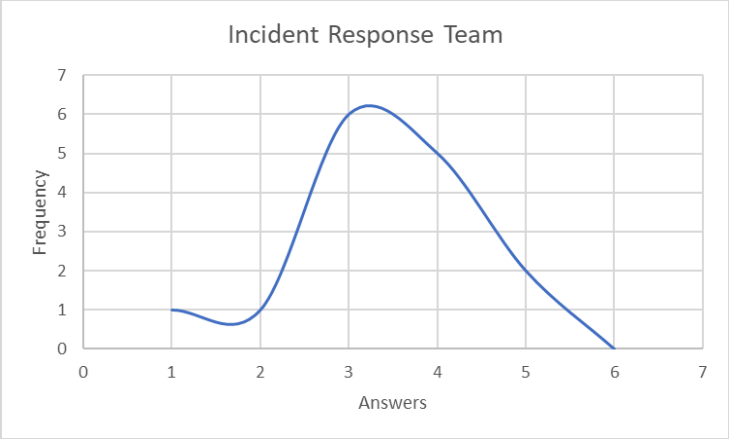
o. Mobile Device Management



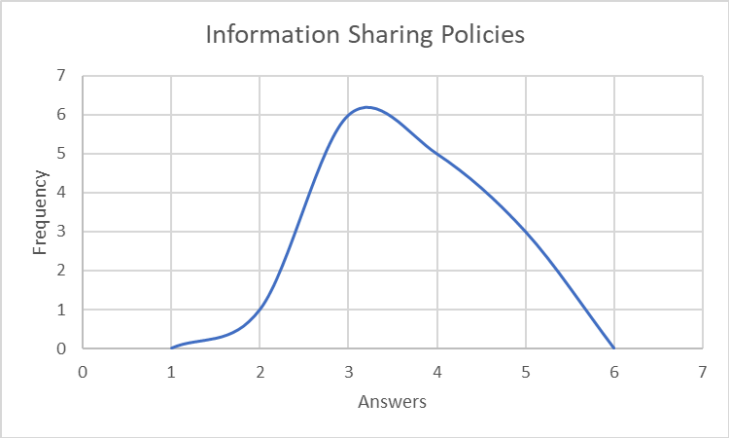
p. Mobile Device Access Control



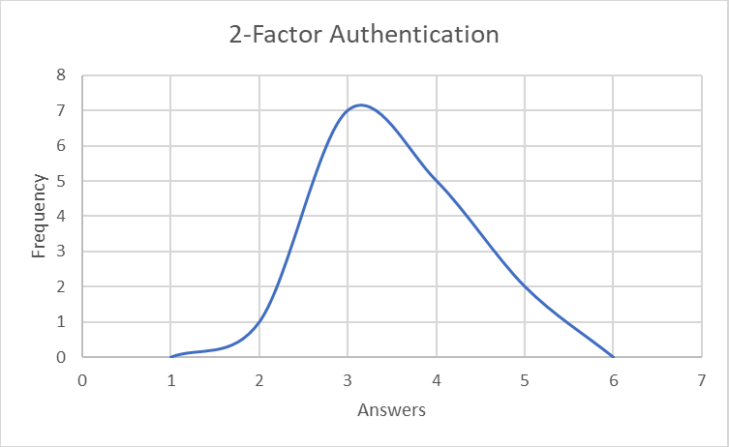
q. Incident Response Team



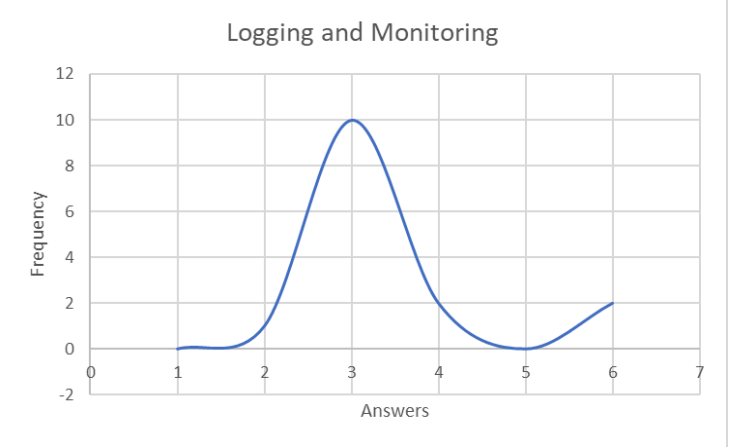
r. Information Sharing Policies



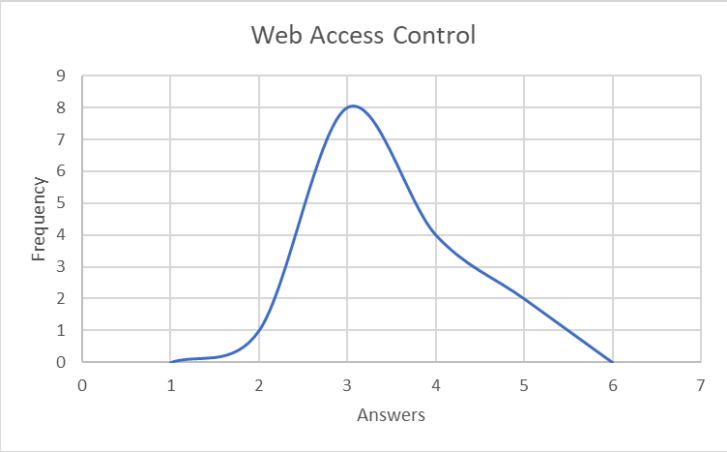
s. 2-Factor Authentication



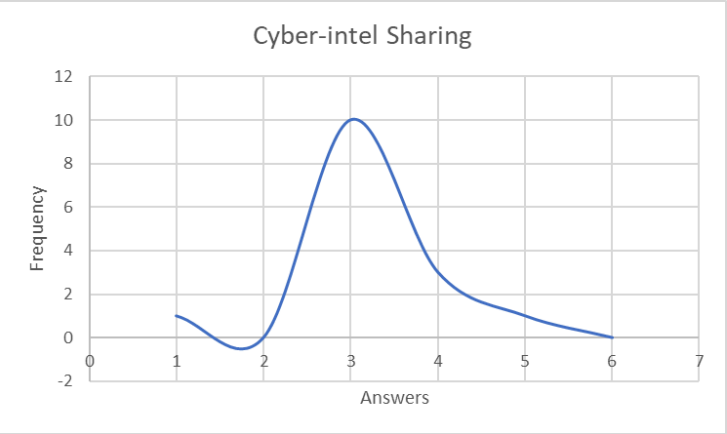
t. Logging and Monitoring



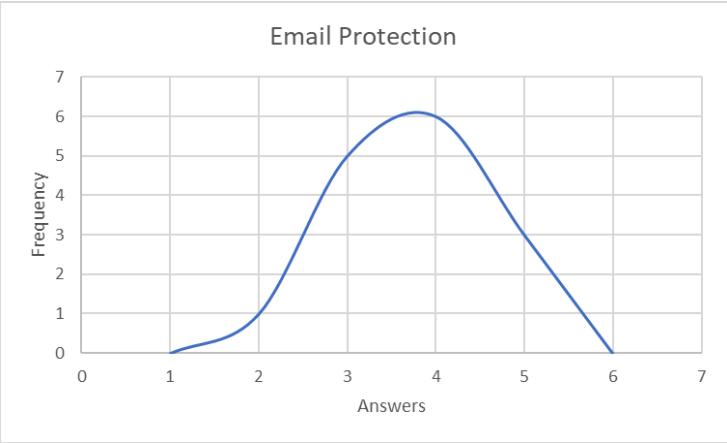
u. Web Access Control



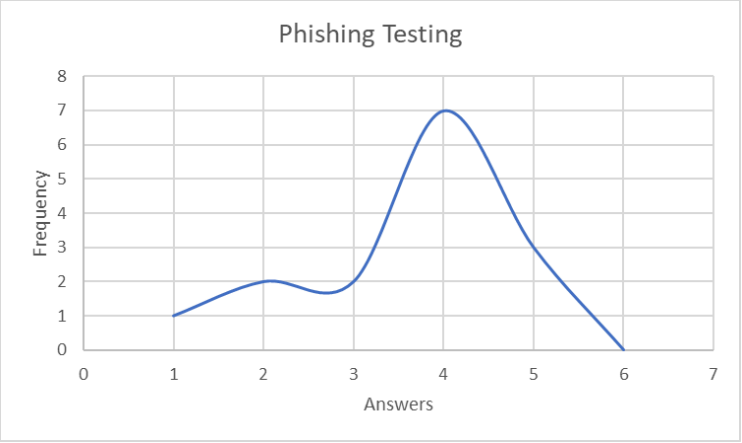
w. Cyber-intel Sharing



v. Email Protection



x. Phishing Testing



CHAPTER 4

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATION

After thoroughly analyzing the collected data and synthesizing the results, the summary of findings, conclusion, and recommendations have been meticulously formulated to address the key research objectives and provide actionable insights.

Based on the descriptive statistics provided, the following observations can be made regarding IT security assurance at ACLC: The mean scores for all areas of IT security assurance are above 3, indicating a generally positive assessment. The standard deviations range from 0.724 to 1.345, indicating varying levels of agreement among respondents, with some areas showing more consistency (e.g., Access Control) than others (e.g., Vulnerability Remediation). Most areas have negative skewness, indicating a distribution with a tail on the left side. This suggests that a majority of respondents rated these areas relatively high, but a few rated them much lower. Positive skewness is observed in areas such as Anti-Malware Software, Access Control, Vulnerability Scanning, and others, indicating a distribution with a tail on the right side, suggesting that a few respondents rated these areas significantly higher than the majority. Noteworthy areas include Phishing Testing, which has the lowest mean (2.667) and the highest standard deviation (1.291), indicating variability and a lower overall assessment compared to other areas. Vulnerability Scanning and Email Protection have relatively high means (3.733) with moderate standard deviations, indicating strong performance in these areas.

The findings indicate that ACLC has a generally positive outlook on its IT security assurance practices, with most areas scoring above average. The variability in responses suggests that while some practices are well-established and uniformly accepted, others may require further standardization and improvement. Negative skewness in many areas points to a few critical responses that highlight areas for potential improvement despite overall positive ratings.

Recommendations include focusing on lower-scoring areas such as Phishing Testing and Cyber-intel Sharing. Phishing Testing should be prioritized for improvement by implementing regular and comprehensive phishing awareness and testing programs. Cyber-intel Sharing may benefit from enhanced strategies to share cyber intelligence more effectively within the organization. Areas with high standard deviations, such as Vulnerability Remediation and Incident Response Team, should be reviewed to understand the reasons for the disparity in responses. Standardized procedures and training could help reduce variability and improve overall ratings. Practices in Vulnerability Scanning and Email Protection should continue to be strengthened, as they already show strong performance. Regular updates and maintaining high standards in these areas will help sustain their effectiveness. For areas with significant negative skewness, the underlying reasons for low ratings among some respondents should be investigated. This may involve targeted feedback sessions or additional support for specific departments or teams. Positive skewness areas should also be reviewed to ensure that the high

ratings are reflective of the actual security posture and not isolated incidents of high performance. By addressing these recommendations, ACLC can enhance its overall IT security assurance, ensuring a more robust and uniformly effective security posture across all areas.

APPENDICES

Table 2. Questionnaire

No.	Items	Scale				
1	AMA Computer Learning Center has cyber security policies, procedures, and standards based on industry standards	5	4	3	2	1
2	AMA Computer Learning Center protects sensitive information received from a third-party firm during transmission between the owning third-party as well as other parties with whom that data is shared (i.e. Encryption, SSL/TLS connections).	5	4	3	2	1
3	All devices that store or process a third-party firm's sensitive information is protected from the Internet by a firewall	5	4	3	2	1
4	AMA Computer Learning Center has a designated Cyber-security personnel	5	4	3	2	1
5	ACLC has a cyber-security user education and awareness program	5	4	3	2	1
6	ACLC performs cyber security audits by external 3rd parties at least annually	5	4	3	2	1
7	All devices that store or process sensitive information in ACLC utilizes anti malware software with current signature files	5	4	3	2	1
8	The users that can access devices that store or process sensitive information have a unique user name and complex password to access the system.	5	4	3	2	1
9	All devices that store or process sensitive information at a minimum have access control that is configured on a least privilege model (a person only has access to the data/device that they need)	5	4	3	2	1
10	All devices that store or process sensitive information at a minimum have vulnerability scanning performed at least monthly	5	4	3	2	1
11	The vulnerabilities are being remediated in a risk based priority (highest priority vulnerabilities are fixed first).	5	4	3	2	1

12	All devices that store or process sensitive information at a minimum have all unnecessary ports and services disabled and the device is used for limited functions (ex. A device acting solely as a file server vs. a file server, FTP server, and web server).	5	4	3	2	1
13	All devices that store or process sensitive information at a minimum have patches deployed for high risk operating systems and third-party application vulnerabilities within industry best practices (i.e. 48 hours) and medium/low risk patches to be deployed in <= 30 days	5	4	3	2	1
14	All laptop devices that store sensitive information are encrypted	5	4	3	2	1
15	All mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have configuration management provided by a firm owned centrally managed infrastructure including the ability to remote wipe the device	5	4	3	2	1
16	All mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have access control to the device (complex password to access device).	5	4	3	2	1
17	ACLC has a Computer Incident Response Team (CIRT) with a formal process to respond to cyberattacks.	5	4	3	2	1
18	When you must share sensitive information with other companies, you require those companies to follow policies, and procedures for cyber security based on industry standards	5	4	3	2	1
19	ACLC requires 2-factor authentication for remote access (e.g. token used in addition to a username and password for VPN login)	5	4	3	2	1
20	ACLC performs industry standard logging and monitoring on devices that store or process sensitive information	5	4	3	2	1

21	ACLC controls web access based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)	5	4	3	2	1
22	ACLC has capabilities of detecting and blocking malicious email prior to delivery to the end user.	5	4	3	2	1
23	ACLC actively participates in a cyber-intel sharing forum (e.g. ISAC, Infraguard)	5	4	3	2	1
24	ACLC performs phishing email testing of its employees	5	4	3	2	1

CURRICULUM VITAE OF THE PROJECT TEAM MEMBERS