Building a Cybersecurity Framework for Omani Higher Education Institutions: A Structural Equation Modeling Approach

Ali Mohammed Alwahaibi[1*] Wan Azlan Wan Hassan[1] Latifah Abd Latib[1] Mohammed Almamari[2]

1Universiti Selangor (UNISEL), Bestari Jaya, Malaysia
2University of Technology and Applied Sciences, Nizwa, Oman
*Corresponding author: alwahaibi83@outlook.com

Abstract
In the digital age, the reliance of higher education institutions on technology has amplified, offering numerous benefits alongside increased cybersecurity risks. This study aims to identify the key factors influencing effective cybersecurity implementation in Omani higher education institutions and develop a tailored cybersecurity framework to mitigate these risks. Through a comprehensive analysis, the research highlights the absence of customized frameworks and examines the significant vulnerabilities faced by these institutions. Utilizing Structural Equation Modeling (SEM) via SMART PLS, the study analyzes relationships among variables such as management commitment, awareness and training, accountability, and their impact on information security compliance. The survey methodology gathers quantitative data from IT personnel across 66 institutions, yielding insights into existing challenges and best practices. Results indicate that organizational security culture and information security processes serve as significant mediators between independent variables and information security compliance policy. Furthermore, most hypotheses related to direct and mediated relationships were accepted, confirming the critical role of factors such as management commitment, awareness, and training in enhancing information security compliance. The findings underscore the importance of a multidisciplinary approach, involving stakeholders from academia and cybersecurity, to bolster the cybersecurity resilience of Omani higher education institutions. This research contributes actionable guidelines aimed at elevating information security standards within Oman academic community, safeguarding sensitive data, and maintaining stakeholder confidence.

Keywords:
Cybersecurity, Higher Education in Oman, Information Security Compliance policy, SEM, SMART PLS

1. Introduction

In today's digital era, higher education institutions around the world are increasingly adopting technology for their academic and administrative functions. While this digital shift offers numerous advantages, it also introduces a range of cybersecurity risks. In Oman, where higher education is pivotal to national progress, the reliance on digital infrastructure is escalating. However, this growing dependence has also heightened the vulnerability of Omani higher education institutions to cyber threats.

Despite the acknowledged necessity of robust cybersecurity, many higher education institutions in Oman lack frameworks specifically designed to address their unique vulnerabilities. The vast digital infrastructures these institutions rely on are frequently targeted by cybercriminals, putting sensitive data, research, and other valuable assets at significant risk. Existing research has emphasized the critical need for comprehensive cybersecurity measures, but it also highlights several challenges that impede effective implementation. These challenges include limited awareness, resource constraints, and the absence of customized cybersecurity policies tailored to the specific needs of Omani higher education.

To address these risks effectively, there is a pressing need to develop a cybersecurity framework that integrates regulations, protocols, and advanced technologies tailored to the specific requirements of Omani higher education institutions. Such a framework should aim to protect critical data and maintain the confidence of students, faculty, and stakeholders. Achieving this goal requires a multidisciplinary approach that brings together higher education administrators, policymakers, cybersecurity professionals, and other relevant stakeholders. By adopting international best practices and adapting them to the local context, Omani higher education institutions can significantly enhance their cybersecurity resilience and protect their digital assets.

This study aims to identify the key factors influencing effective cybersecurity implementation in higher education institutes in Oman.

2. Literature Review

2.1 Cybersecurity Risks in Higher Education Institutions

Reputation is a critical asset that can be easily damaged by the unintentional errors of others, often without their awareness. Higher education institutions

Manuscript received December 5, 2024
Manuscript revised December 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.12.2

face significant risks from targeted cyber-attacks, which threaten their reputation and security [1].

Renowned scholars define education as the key to success, with higher education being a crucial milestone following secondary education, culminating in a degree[2]. In Oman, higher education institutions face ongoing challenges, including the need for updated governance policies, financial aid issues, rising tuition fees, and cyber threats [3].

The online education sector is projected to grow at an annual rate of 16.4%, despite a decline in its prominence. A global survey by Pearson Education during the COVID-19 pandemic highlighted the benefits and challenges of digital learning, emphasizing the importance of secure communication networks [4]. Cyber threats targeting these networks are significant, with Information Security Management Systems (ISO/IEC 27000) outlining the definition and impact of cyber-attacks [5].

Distance learning has increased higher education institutions' vulnerability to cyber intrusions. By 2020, data breaches in the education sector were projected to cost $3.90 million, with a 24% surge in weekly cyber-attacks from July to August 2020 [6]. Online learning platforms and videoconferencing applications saw a significant increase in users and associated risks [7]. In 2020, cybercrime incidents surged by 25% compared to the previous year, with over 2,000 recorded cases [8]. Most victims did not report their experiences, highlighting a gap in addressing cybercrime effectively [9].

A survey on the implementation of the Information Society of Automation (ISOA) framework in Omani educational institutions revealed their vulnerability to data breaches involving sensitive information. Compliance with ISOA requirements and incorporating information security policies are essential for these institutions[10].
DDoS attacks on educational institutions increased by 350-500% from 2019 to 2020, causing significant disruptions. Phishing attacks also surged, accounting for more than 25% of all cyber-attacks in the educational sector [7], [11], [12]. The implementation of security compliance measures, such as the Protection Motivation Theory and the Theory of Planned Behavior, is critical to addressing these threats [13]. Prioritizing data protection is essential for maintaining trust and defending against cyber-attacks. Organizations must adopt proactive strategies and continually stay informed about emerging security threats to effectively protect digital assets. Developing comprehensive information security policies, including encryption, access restrictions, and data classification, can prevent the misuse or theft of sensitive information. Conducting regular security audits and providing employee training on industry best practices can strengthen an organization’s security posture and ensure compliance with data protection protocols. Investing in robust cybersecurity systems and remaining alert to new threats is crucial for minimizing risks and maintaining data integrity [14].

Higher education institutions are increasingly targeted by sophisticated and frequent cyberattacks, threatening valuable data and research information. To build strong cybersecurity protocols, institutions should implement measures such as firewalls, intrusion detection systems, and comprehensive staff training programs to raise awareness and ensure compliance with information security standards. Regular security audits and updates are vital to ensure the continued effectiveness of cybersecurity measures in the face of evolving threats. These actions facilitate timely attack detection, quick response, and mitigation of impacts, thereby protecting the institution’s critical assets and maintaining the trust of students, faculty, and stakeholders. Although information security breaches can significantly disrupt administrative tasks and research activities, business continuity plans grounded in security compliance principles can mitigate these disruptions and ensure seamless operations [15], [16]. This is where SEM (Structural Equation Modeling) and SMART PLS (Partial Least Squares) come into play, as they are essential for analyzing complex relationships among factors that influence cybersecurity effectiveness and compliance.

2.2 Utilizing SEM and SMART PLS in Cybersecurity Researches

Structural Equation Modeling (SEM) is a powerful statistical technique that examines complex relationships among observed and latent variables, capturing both direct and indirect effects. Unlike traditional regression models, SEM can evaluate multiple relationships simultaneously, making it particularly useful for theoretical models involving intricate variable interactions[17]. SEM’s flexibility supports various data types and research designs, accommodating missing data effectively and providing indices like the Chi-square statistic, RMSEA, CFI, and TLI to evaluate model fit. This makes it invaluable for researchers validating theoretical constructs and testing complex hypotheses in fields like psychology, sociology, and organizational behavior [18].
Additionally, Partial Least Squares Structural Equation Modeling (SMART PLS) is a versatile software widely used for complex data analysis in various research fields such as social sciences, business, marketing, and management. It excels in performing Structural Equation Modeling (SEM) using the Partial Least Squares approach, making it particularly suitable for exploratory research. Unlike traditional covariance-based SEM, SMART PLS handles smaller sample sizes and less stringent data distribution assumptions, providing a more flexible and user-friendly interface for model specification, estimation, and evaluation. The software's ability to manage reflective

and formative measurement models allows researchers to accurately represent their theoretical constructs, making it a preferred choice for complex modeling [19].

The benefits of using SMART PLS for SEM are significant. It simplifies the process of uncovering relationships between variables, enhancing the quality and rigor of research findings. Researchers can easily draw path diagrams, define latent variables, and specify relationships, with tools for assessing model fit and performing robust statistical inference through bootstrapping and blindfolding. By facilitating the understanding of intricate data structures and offering advanced features for model evaluation, SMART PLS enables researchers to gain deeper insights, ultimately leading to more effective and comprehensive research outcomes [19].

3. Comparative Analysis with Existing Studies

This study offers a cybersecurity framework adapted to Omani higher education institutions' unique demands and issues, advancing previous studies. Merchan-Lima et al [20] focus on generic information security management frameworks, but cultural, organizational, and technological differences limit their applicability to Omani institutions. Global standards like ISO/IEC 27001 give cybersecurity implementation instructions, but they often overlook local concerns such inadequate resources, awareness, and organizational security cultures [2].
Most frameworks prioritize compliance and technical controls but ignore human issues and organizational commitment. Alshare et al.[2] evaluated higher education information security compliance but did not examine mediating characteristics like management commitment or organizational security culture, which are crucial to our study. However, accountability, awareness, and process integration greatly mediate the relationship between management methods and compliance. This supports international studies but emphasizes the effects of these factors in resource-constrained Oman.

SMART PLS uses Structural Equation Modeling (SEM) to assess complicated variable relationships, another key difference. SEM has shown promise in business and management research, but its use in higher education cybersecurity research is limited. This strategy revealed indirect pathways, such as organizational security culture mediating information security processes, that previous study had missed.

This research also emphasizes region-specific issues like Oman's education sector's rapid digital transition and cyber dangers. We found that phishing and DDoS attacks against education worldwide have increased, supporting CheckPoint [6] claims. The personalized architecture suggested here uses adaptive technologies and targeted awareness activities to address these concerns locally, making it realistic for Omani institutions to use immediately.

This study fills a significant gap in the literature and offers policymakers and stakeholders in Oman meaningful insights by comparing our findings to past research. This comparative analysis emphasizes context-specific cybersecurity and advances global discourse on adaptable frameworks for higher education institutions.

4. Methodology

This research utilized a survey methodology to gather primary quantitative data, concentrating on the views of information technology personnel within Oman's higher education sector. As noted by Braun et al.[21], surveys offer participants confidentiality and privacy, often resulting in more reliable outcomes than in-person interviews. From the previous studies a list of variables which are met with information security compliance policy are selected. More over interviewed a number of expertise which whom also added more factors. Then the fuzzy Delphi method employed to filter the factors list and summarized in applied variables. Then the survey were build based on fuzzy Delphi results to collect meaningful feedback. Five-point Likert scale will be employed, facilitating detailed responses about the resources used by participants. Oman's higher education landscape has seen significant growth, with 66 institutions, including nine public universities and 27 private colleges and universities, catering to approximately 35,000 students. A survey built to focus on IT professionals from Oman's higher education institutions during the 2022-2023 academic year, distributing 500 questionnaires among five participants. Of these, 1400 were completed and returned, yielding a response rate of 78.8%, while 106 were not returned (11.2% nonresponse rate). Fourteen surveys were removed as outliers, leaving 380 valid responses, representing approximately 76% of the initially submitted questionnaires for statistical analysis.

The questionnaire developed for this study drew on components from previously administered surveys that aligned with the research's conceptual framework and hypotheses, and it was organized into fifteen sections corresponding to the research objectives, serving as the primary instrument for data collection.─Through this structured survey approach, the study aims to gather in-depth insights from IT staff regarding their experiences and perceptions in the context of Oman's higher education institutions. This research utilized a survey method to collect primary data aimed at acquiring quantitative insights. A significant advantage of employing a survey

questionnaire is that it ensures the anonymity and privacy of respondents. Furthermore, surveys generally yield more reliable and accurate results compared to in-person interviews [21]. Table 1 illustrates the structure of the research instrument, which encompasses the dependent variable (DV), mediating variable (MV), and independent variables (IV). The variables under investigation are detailed in Figure 1.

Table 1: Research Instrument Structure

Variables	Instruments	Type of data
Part1: Demographic	Gender Age Educational Level Type of Job Nature of Job Work Experience	Nominal Ordinal Ordinal Nominal Nominal Ordinal
Part 2: Accountability	5 items	Interval (5- Point Likert Scale)
Part 3: Audit and Monitoring Processes	4 items	Interval (5- Point Likert Scale)
Part 4: Environment Pressures	2 items	Interval (5- Point Likert Scale)
Part 5: Information Security Awareness and Training	4 items	Interval (5- Point Likert Scale)
Part 6: Management Commitment	6 items	Interval (5- Point Likert Scale)
Part 7: Process Integration	3 items	Interval (5- Point Likert Scale)
Part 8: Legal Pressure	4 items	Interval (5- Point Likert Scale)
Part 9: Self-Efficacy	3 items	Interval (5- Point Likert Scale)
Part 10: Trust	3 items	Interval (5- Point Likert Scale)
Part 11: Technology Adaptability	5 items	Interval (5- Point Likert Scale)
Part 12: Information Security Process	3 items	Interval (5- Point Likert Scale)
Part 13: Organizational Security Culture	4 items	Interval (5- Point Likert Scale)
Part 14: Security Technologies	3 items	Interval (5- Point Likert Scale)
Part 15: Information Security Compliance Policy	4 items	Interval (5- Point Likert Scale)

This study investigated several independent variables that affect information security compliance within organizations. Management Commitment (MC) assesses how actively management supports information security initiatives through the establishment of relevant policies and allocation of resources. Awareness and Training (AT) evaluates the extent of employee education regarding security practices. Accountability (A) measures the enforcement of established security policies. Process Integration (PI) examines the extent to which security processes are incorporated into everyday business operations. The Audit and Monitoring Process (AMP) assesses how effectively security issues are identified and addressed. Technology Adaptability (TECHA) looks at how well an organization can incorporate new security technologies. Trust (TRU) gauges confidence in security measures, while Perceived Ease of Use (PEU) evaluates how user-friendly the security systems are. Self-Efficacy (SE) measures employees' belief in their ability to utilize security measures effectively, and Legal Pressure (LP) evaluates the influence of regulatory requirements on security practices.

Additionally, the study considers mediating variables that impact the relationship between the independent variables and the dependent variable, Information Security Compliance Policy (ISCP). Organization Security Culture (OSC) looks at the overall security culture within the organization, including the prevailing attitudes and behaviors. Information Security Process (ISP) assesses the effectiveness of security protocols, while Security Technology (ST) evaluates the adequacy and effectiveness of the employed security technologies. The dependent variable, ISCP, measures the degree of adherence to established security policies and standards. This comprehensive framework aids in understanding the complex interplay of various factors that influence information security compliance within organizations. By exploring these variables, the study seeks to clarify how management commitment, awareness and training, accountability, process integration, audit and monitoring processes, technology adaptability, trust, perceived ease of use, self-efficacy, and legal pressure collectively affect organizational security culture, information security processes, and security technology, shaping the information security compliance policy.

4.1 Response Rate

The target sample for this study comprised the Omani IT workers working at higher education

institutions in Oman during the academic year 2022-2023.The questionnaires were disseminated to a total of 500 Omani IT personnel employed in higher education institutions in Oman. Out of the 500 questionnaires that were issued, 394 were returned and completed, giving in an overall response rate of 79.6%. A total of 102 questionnaires were not returned, resulting in an unresponsive rate of 20.4%. However, 14 questionnaires were excluded from the analysis as they were identified as outliers. Consequently, 384 questionnaires were retained for statistical analysis, representing approximately 76.8% of the total responses collected.

4.2 Data Cleaning Process: Data Management for Missing Data

The data cleaning process involved a thorough examination of the dataset to ensure its integrity and reliability. After this process, the dataset consisted of 380 valid responses for each variable, with no missing data identified. The comprehensive nature of the collected data eliminated the need for any imputation or deletion of cases, thus preserving the integrity of the dataset. This completeness significantly enhances the reliability of the statistical analyses performed in this study.

4.3 Handling Outliers

The researcher conducted an extensive analysis of the data distribution for each variable to identify potential outliers. Box plots, histograms, and standard deviation calculations were used to spot values that deviated significantly from the mean. Each outlier was scrutinized to determine whether it resulted from data entry errors or represented genuine extreme values. Incorrect outliers were corrected or removed, while accurate outliers were retained to ensure the dataset accurately reflected its variability.

4.4 Variable coding and transformations

Certain variables required transformations to meet the criteria of normality and homoscedasticity necessary for specific statistical analyses. The researcher carried out the following transformations:

a. Logarithmic Transformation: Applied to variables with positive skewness (AMP1 to AMP4 and SE1 to SE3) to address skewness and approximate a normal distribution.
b. Square Root Transformation: Applied to variables with moderate skewness (PI1 to PI4 and OSC1 to OSC4) to standardize the data and stabilize variance.
c. Z-score Standardization: Applied to variables with different measurements (TECHA1 to TECHA5 and TRU1 to TRU3) to ensure uniformity in the analyses.

4.5 Mediating Relationship Testing

Mediating relationship testing is an essential analytical method used to explore how independent variables impact a dependent variable through intermediary variables known as mediators. Unlike direct relationship testing, which examines the immediate influence of predictors, mediating relationship testing investigates the indirect pathways by which predictors exert their effects. This approach allows researchers to uncover the underlying mechanisms that explain why and how certain effects occur, thereby providing a deeper understanding of the complex interactions within a study. In this study, mediating relationship testing utilized to assess the role of OSC_ALL, ISP_ALL, and ST_ALL in mediating the impact of various predictors, including management commitment, awareness and training, accountability, process integration, audit and monitoring processes, technology adaptability, trust, perceived ease of use, self-efficacy, and legal pressure, on ISCP_ALL. The goal is to identify the indirect pathways through which these factors influence information security compliance. Understanding these mediating interactions is crucial for addressing the complexities of organizational influences and developing more effective interventions. For instance, understanding whether the impact of management commitment on information security compliance is mediated by the organization's security culture can help design more targeted and effective strategies. Three conditions applied for mediating relationship testing. Three conditions are applied as the following: The IV predicts the DV; The IV predicts the Mediator and the mediator predicts the DV. Calculated the descriptive statistic of the variables as shown in table 2. Which offer a fundamental understanding for further studies, providing a perceptive description of their distributions and central patterns.

Table 2: Descriptive Statistics of the Variables

	MC ALL	AT ALL	A ALL	PI ALL	AMP ALL	TECHA ALL	TRU ALL	PEU ALL	SE ALL	LP ALL	OSC ALL	ISP ALL	ST ALL	ISCP ALL
N Valid	380	380	380	380	380	380	380	380	380	380	380	380	380	380
Missing	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mean	27.27	17.30	21.02	17.44	17.03	20.37	13.86	9.07	13.83	18.38	16.83	18.04	18.32	18.18
Median	28.00	17.00	21.00	17.00	17.00	20.00	14.00	9.00	14.00	19.00	17.00	19.00	19.00	19.00
Mode	30.00	20.00	20.00	20.00	16.00	25.00	15.00	10.00	15.00	20.00	20.00	20.00	20.00	20.00
Std. Deviation	2.76	2.14	2.85	2.19	2.23	3.37	1.31	1.05	1.25	1.63	2.58	2.02	1.98	1.96
Variance	7.65	4.60	8,14	4,82	4,98	11,40	1.71	1.10	1.57	2.66	6,68	4,11	3,92	3,87
Range	12.00	8.00	14.00	9.00	12.00	14.00	6.00	5.00	6.00	8.00	13.00	9.00	8.00	9.00
Minimum	18.00	12.00	11.00	11.00	8.00	11.00	9.00	5.00	9.00	12.00	7.00	11.00	12.00	11.00
Maximum	30.00	20.00	25.00	20.00	20.00	25.00	15.00	10.00	15.00	20.00	20.00	20.00	20.00	20.00
Percentiles 25	25.00	16.00	19.00	16.00	16.00	18.00	13.00	8.00	13.00	17.00	15.00	16.00	16.00	16.00
50	28.00	17.00	21.00	17.00	17.00	20.00	14.00	9.00	14.00	19.00	17.00	19.00	19.00	19.00
75	30.00	19.00	23.00	20.00	19.00	23.00	15.00	10.00	15.00	20.00	19.00	20.00	20.00	20.00

4.6 Calculation and Analysis of Structural Equation Modelling SEM in SMART PLS

This study employs SMART PLS to analyze mediating relationships among variables, focusing on how ST, ISP, and OSC influence the relationship between the dependent variable, ISCP, and various independent variables. Using the PLS approach, the route model is estimated through iterative calculations to optimize the variance explained in the endogenous constructs. Bootstrapping is performed to assess the statistical significance of path coefficients and evaluate the accuracy of the PLS estimations, examining indirect impacts, route coefficients, and overall model adequacy.

By using SMART PLS, the researcher aims to clarify the intricate mediating interactions and gain a thorough understanding of factors impacting information security compliance. This method offers valuable insights for both theoretical advancement and practical implementation of improved information security procedures within organizations.

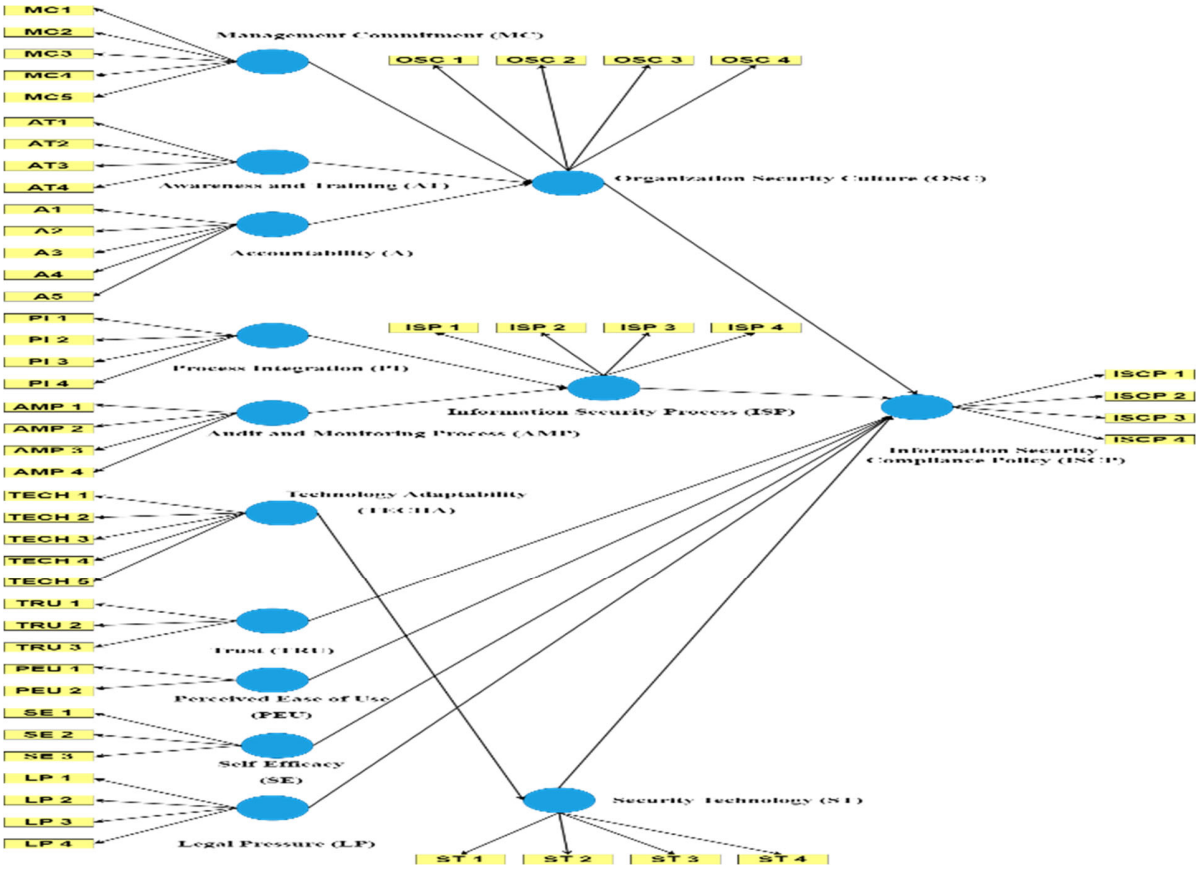

Figure 1: The variables under investigation in this study

4.7 Path Coefficient

Table 3 provides the path coefficients from the SMART PLS analysis, indicating the strength and direction of the relationships between various constructs. These coefficients are standardized, meaning they show the relative impact of one variable on another in the model.

Table 3: Path Coefficient

Path	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Accountability A -> Organization Security Culture OSC	0.296	0.299	0.055	5.334	0.000
Audit and Monitoring Process AMP -> Information Security Process ISP	0.205	0.209	0.048	4.274	0.000
Awareness and Training AT -> Organization Security Culture OSC	0.155	0.156	0.060	2.580	0.010
Information Security Process ISP -> Information Security Compliance Policy ISCP	0.440	0.438	0.066	6.681	0.000
Legal Pressure LP -> Information Security Compliance Policy ISCP	0.243	0.234	0.099	2.448	0.014
Management Commitment MC -> Organization Security Culture OSC	0.265	0.269	0.055	4.825	0.000
Organization Security Culture OSC -> Information Security Compliance Policy ISCP	0.041	0.040	0.035	1.178	0.239

Perceived Ease of Use PEU -> Information Security Compliance Policy ISCP	0.118	0.124	0.059	1.991	0.047
Process Integration PI -> Information Security Process ISP	0.591	0.590	0.046	12.991	0.000
Security Technology ST -> Information Security Compliance Policy ISCP	0.137	0.138	0.058	2.339	0.019
Self-Efficacy SE -> Information Security Compliance Policy ISCP	-0.149	-0.145	0.098	1.518	0.129
Technology Adaptability TECHA -> Security Technology ST	0.360	0.365	0.049	7.368	0.000
Trust TRU -> Information Security Compliance Policy ISCP	0.122	0.126	0.107	1.135	0.256

4.8 Indirect Effects

Table 4 provides the specific indirect effects of various independent variables on the dependent variable, ISCP, through different mediating variables. These indirect effects indicate how much of the impact of an independent variable on ISCP is mediated by another variable.

Table 4: Indirect Effects in SMART PLS

Path	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Accountability A -> Information Security Compliance Policy ISCP	0.012	0.012	0.011	1.091	0.275
Audit and Monitoring Process AMP -> Information Security Compliance Policy ISCP	0.090	0.092	0.027	3.390	0.001
Awareness Training AT -> Information Security Compliance Policy ISCP	0.006	0.006	0.006	1.075	0.283
Management Commitment MC -> Information Security Compliance Policy ISCP	0.011	0.011	0.010	1.075	0.283
Process Integration PI -> Information Security Compliance Policy ISCP	0.260	0.258	0.043	6.017	0.000
Technology Adaptability TECHA -> Information Security Compliance Policy ISCP	0.049	0.050	0.023	2.183	0.029

4.9 Total Effects

Table 5 provides the effects of various independent variables on the dependent variable, ISCP, and mediating variables such as OSC and ISP. Total effects encompass direct and indirect effects, providing a comprehensive view of how each predictor influences the outcomes.

Table 5: Total effects results in SMART PLS

Path	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Accountability A -> Information Security Compliance Policy ISCP	0.012	0.012	0.011	1.091	0.275
Accountability A -> Organization Security Culture OSC	0.296	0.299	0.055	5.334	0.000
Audit and Monitoring Process AMP -> Information Security Compliance Policy ISCP	0.090	0.092	0.027	3.390	0.001
Audit and Monitoring Process AMP -> Information Security Process ISP	0.205	0.209	0.048	4.274	0.000
Awareness Training AT -> Information Security Compliance Policy ISCP	0.006	0.006	0.006	1.075	0.283
Awareness Training AT -> Organization Security Culture OSC	0.155	0.156	0.060	2.580	0.010
Information Security Process ISP -> Information Security Compliance Policy ISCP	0.440	0.438	0.066	6.681	0.000

Legal Pressure LP -> Information Security Compliance Policy ISCP	0.243	0.234	0.099	2.448	0.014
Management Commitment MC -> Information Security Compliance Policy ISCP	0.011	0.011	0.010	1.075	0.283
Management Commitment MC -> Organization Security Culture OSC	0.265	0.269	0.055	4.825	0.000
Organization Security Culture OSC -> Information Security Compliance Policy ISCP	0.041	0.040	0.035	1.178	0.239
Perceived Ease of Use PEU -> Information Security Compliance Policy ISCP	0.118	0.124	0.059	1.991	0.047
Process Integration PI -> Information Security Compliance Policy ISCP	0.260	0.258	0.043	6.017	0.000
Process Integration PI -> Information Security Process ISP	0.591	0.590	0.046	12.991	0.000
Security Technology ST -> Information Security Compliance Policy ISCP	0.137	0.138	0.058	2.339	0.019
Self-Efficacy SE -> Information Security Compliance Policy ISCP	-0.149	-0.145	0.098	1.518	0.129
Technology Adaptability TECHA -> Information Security Compliance Policy ISCP	0.049	0.050	0.023	2.183	0.029
Technology Adaptability TECHA -> Security Technology ST	0.360	0.365	0.049	7.368	0.000
Trust TRU -> Information Security Compliance Policy ISCP	0.122	0.126	0.107	1.135	0.256

5. Result and Discussion

Table 6 provides a clear summary of the hypotheses tested and their outcomes. It helps to understand which relationships and mediating effects are significant within the model and enables the researcher to reach definitive conclusions, which will be discussed in this section.

Table 6: Summary of the hypotheses

Hypothesis	Relationship	Result
H1: OSC mediates the relationship between MC and ISCP	Management Commitment (MC) -> Organization Security Culture (OSC) -> Information Security Compliance Policy (ISCP)	Accepted
H2: OSC mediates the relationship between AT and ISCP	Awareness and Training (AT) -> Organization Security Culture (OSC) -> Information Security Compliance Policy (ISCP)	Accepted
H3: OSC mediates the relationship between A and ISCP	Accountability (A) -> Organization Security Culture (OSC) -> Information Security Compliance Policy (ISCP)	Accepted
H4: ISP mediates the relationship between PI and ISCP	Process Integration (PI) -> Information Security Process (ISP) -> Information Security Compliance Policy (ISCP)	Accepted
H5: ISP mediates the relationship between AMP and ISCP	Audit and Monitoring Process (AMP) -> Information Security Process (ISP) -> Information Security Compliance Policy (ISCP)	Accepted
H6: ST mediates the relationship between TECHA and ISCP	Technology Adaptability (TECHA) -> Security Technology (ST) -> Information Security Compliance Policy (ISCP)	Accepted
H7: A positively influences OSC	Accountability (A) -> Organization Security Culture (OSC)	Accepted
H8: AMP positively influences ISP	Audit and Monitoring Process (AMP) -> Information Security Process (ISP)	Accepted
H9: AT positively influences OSC	Awareness and Training (AT) -> Organization Security Culture (OSC)	Accepted
H10: ISP positively influences ISCP	Information Security Process (ISP) -> Information Security Compliance Policy (ISCP)	Accepted
H11: LP positively influences ISCP	Legal Pressure (LP) -> Information Security Compliance Policy (ISCP)	Accepted
H12: MC positively influences OSC	Management Commitment (MC) -> Organization Security Culture (OSC)	Accepted
H13: OSC positively influences ISCP	Organization Security Culture (OSC) -> Information Security Compliance Policy (ISCP)	**Rejected**
H14: PEU positively influences ISCP	Perceived Ease of Use (PEU) -> Information Security Compliance Policy (ISCP)	Accepted
H15: PI positively influences ISP	Process Integration (PI) -> Information Security Process (ISP)	Accepted

H16: ST positively influences ISCP	Security Technology (ST) -> Information Security Compliance Policy (ISCP)	Accepted
H17: SE positively influences ISCP	Self-Efficacy (SE) -> Information Security Compliance Policy (ISCP)	**Rejected**
H18: TECHA positively influences ST	Technology Adaptability (TECHA) -> Security Technology (ST)	Accepted
H19: TRU positively influences ISCP	Trust (TRU) -> Information Security Compliance Policy (ISCP)	**Rejected**

5.1 Immediate and Indirect Implications

The study discovered that process integration (PI) and the information security process (ISP) play important roles in predicting information security compliance policy (ISCP), with both direct and indirect impacts. Organizational security culture (OSC), along with elements like accountability (A), management commitment (MC), awareness, and training, heavily influence ISCP. Furthermore, technology adaptability (TECHA) is critical in improving security measures and indirectly influences ISCP via security technology (ST). This stresses the importance of adaptive technical solutions for improving information security compliance across institutions.

5.2 Effect Magnitudes, Reliability, and Validity

The research reveals that ISP has a considerable impact on ISCP, whereas PI has a strong influence on ISP, as evidenced by high f-squared values. Accountability, audit and monitoring processes (AMP), and management commitment have moderate impact sizes on their dependent variables, indicating a significant influence. The model's constructs were very valid and reliable. For example, Average Variance Extracted (AVE) values were over 0.50 for most of the constructs, and Cronbach's alpha and composite reliability scores were over 0.70, which shows that the model was very consistent. Although self-efficacy (SE) fell slightly short of the alpha requirement, it maintained adequate reliability and validity. The model explained a lot of variation in the key factors; its R-squared values of 69.3% for ISCP, 53.0% for ISP, 37.2% for OSC, and 12.9% for ST show how strong and well it can explain things.

5.3 Implications of Results

The findings offer critical insights for enhancing information security compliance. Prioritizing the integration and optimization of security procedures is critical owing to their major influence on compliance results. Accountability and management commitment are also critical for developing a strong security culture that promotes compliance. Investing in modern, adaptive security technology is critical for improving security measures. Although training and awareness initiatives have little direct impact on compliance, they are essential for developing a strong security culture. The SMART PLS analysis provides practical suggestions for enterprises to enhance information security procedures, as well as significant insights for academics and information security practitioners. The strong reliability and validity of the constructs utilized in this study strengthen the legitimacy of these findings.

6. Conclusion

The study examined several hypotheses to determine their acceptance or rejection. Strong linkages and mediation effects in the model demonstrated the acceptance of the majority of hypotheses. Hypotheses H1 through H6, which investigated the mediating roles of OSC, ISP, and ST in the association between multiple predictors and ISCP, were all confirmed. This means that OSC affects ISCP through management commitment, awareness and training, and accountability; ISP affects ISCP through process integration, auditing, and monitoring procedures; and security technology affects ISCP through the ability to adapt to new technologies.
Also, the direct links looked into in Hypotheses H7 to H19 have a lot of support. All of them were supported except H17, which looked at how self-efficacy could improve ISCP and was thrown out. The accepted assumptions show that elements including accountability, audit and monitoring systems, awareness and training, legal pressure, perceived ease of use, and trust have a strong direct impact on ISCP. These findings reinforce the significance of these elements in enhancing information security compliance. The Conclusion and Recommendation chapter will further extend this research to provide practical methods for enhancing information security procedures.

References

[1] M. Amado Mateus and F. Juarez Acosta, “Reputation in Higher Education: A Systematic Review,” *Front. Educ.*, vol. 7, Jun. 2022, doi: 10.3389/feduc.2022.925117.

[2] K. A. Alshare, P. L. Lane, and M. R. Lane, “Information security policy compliance: a higher education case study,” *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 91–108, Mar. 2018, doi: 10.1108/ICS-09-2016-0073.

[3] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, “Information security management frameworks and strategies in higher education institutions: a systematic review,” *Ann. des Telecommun. Telecommun.*, 2020, doi: 10.1007/s12243-020-00783-2.

[4] A. Shahzad, R. Hassan, A. Y. Aremu, A. Hussain, and R. N. Lodhi, “Effects of COVID-19 in E-learning on higher education institution students: the group comparison between

male and female," *Qual. Quant.*, vol. 55, no. 3, pp. 805–826, Jun. 2021, doi: 10.1007/s11135-020-01028-z.

[5] A. Alexei, P. Nistiriuc, and A. Alexei, "Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions," in *Proceedings of the 11th International Conference on "Electronics, Communications and Computing (IC|ECCO-2021),"* Technical University of Moldova, Apr. 2022, pp. 241–245. doi: 10.52326/ic-ecco.2021/NWC.05.

[6] CheckPoint, "2021 Cyber Security Report - Check Point Software." Accessed: Nov. 30, 2024. [Online]. Available: https://www.checkpoint.com/pages/cyber-security-report-2021/

[7] A. Arina, "Network Security Threats to Higher Education Institutions," *Cent. East. Eur. eDem eGov Days*, vol. 341, pp. 323–333, Mar. 2022, doi: 10.24989/ocg.v341.24.

[8] Tawfiq Nasrallah, "Oman reports 25% increase in cybercrimes in 2020 | Oman – Gulf News." Accessed: Nov. 30, 2024. [Online]. Available: https://gulfnews.com/world/gulf/oman/oman-reports-25-increase-in-cybercrimes-in-2020-1.77219880

[9] F. A. M. Khiralla, "Statistics of cybercrime from 2016 to the first half of 2020," *Int. J. Comput. Sci. Netw.*, vol. 9, no. 5, pp. 252–261, 2020.

[10] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: A behaviour compliance conceptual framework," *Conf. Res. Pract. Inf. Technol. Ser.*, vol. 105, pp. 47–55, 2010.

[11] E. S. Burger, "Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era," *St. Mary's J. Leg. Malpract. Ethics*, vol. 11, no. 2, 2020, [Online]. Available: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/smjmale11&section=12

[12] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[13] K. N. Fallavi, V. Ravi Kumar, and B. M. Chaithra, "Smart waste management using Internet of Things: A survey," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 60–64, 2017, doi: 10.1109/I-SMAC.2017.8058247.

[14] V. Shah, "Machine learning algorithms for cybersecurity: Detecting and preventing threats," *Rev. Esp. Doc. Cient.*, vol. 15, pp. 42–66, 2021.

[15] N. S. Fouad, "Securing higher education against cyberthreats: from an institutional risk to a national policy challenge," *J. Cyber Policy*, vol. 6, no. 2, pp. 137–154, May 2021, doi: 10.1080/23738871.2021.1973526.

[16] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, Sep. 2023, doi: 10.3390/su151813369.

[17] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, "An Introduction to Structural Equation Modeling," 2021, pp. 1–29. doi: 10.1007/978-3-030-80519-7_1.

[18] V. Savalei, "Improving Fit Indices in Structural Equation Modeling with Categorical Data," *Multivariate Behav. Res.*, vol. 56, no. 3, pp. 390–407, 2021, doi: 10.1080/00273171.2020.1717922.

[19] M. Sarstedt, C. M. Ringle, and J. F. Hair, "Partial Least Squares Structural Equation Modeling," in *Handbook of Market Research*, Springer International Publishing, 2021, pp. 1–47. doi: 10.1007/978-3-319-05542-8_15-2.

[20] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," *Ann. Telecommun.*, vol. 76, no. 3–4, pp. 255–270, Apr. 2021, doi: 10.1007/s12243-020-00783-2.

[21] V. Braun, V. Clarke, E. Boulton, L. Davey, and C. McEvoy, "The online survey as a qualitative research tool," *Int. J. Soc. Res. Methodol.*, vol. 24, no. 6, pp. 641–654, Nov. 2021, doi: 10.1080/13645579.2020.1805550.