Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Cybersecurity Awareness, Policy Compliance, and Financial Data Protection in Accounting Information Systems: Evidence from Somali Financial Institutions

Nasro Khalif Abdullahi

nasro11@simad.edu.so

SIMAD University

Abdullahi Salad Abdi

SIMAD University

Article

Keywords: accounting information systems, cybersecurity awareness, financial data protection, internal control, policy compliance, Somalia

Posted Date: July 9th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10034791/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

This study examines whether employee cybersecurity awareness predicts financial data protection in accounting information systems. Using survey evidence from 415 employees in Somali banking and financial institutions, the study links cyber awareness to accounting control reliability, financial data integrity, and policy compliance. Overall awareness is positively associated with financial data protection ($r = 0.447$, $p < 0.001$). In the adjusted regression model, general cybersecurity awareness and policy compliance remain significant positive predictors, while password security, phishing awareness, and device security practices do not have independent effects. The findings suggest that financial data protection is supported less by isolated security habits than by broad cyber-risk understanding and rule-consistent conduct embedded in the control environment. The study contributes field evidence from an under-researched financial setting and positions cybersecurity compliance as a behavioral internal-control mechanism within accounting information systems.

1. Introduction

Financial data protection has become a core accounting problem. Accounting information systems (AIS) no longer operate as isolated record-keeping tools; they are connected to payment channels, customer databases, authentication layers, reporting workflows, audit trails, and compliance monitoring. In that environment, the protection of financial records depends not only on technical controls but also on the everyday conduct of employees who enter, approve, transmit, reconcile, and review financial information. A control can be well designed on paper and still fail if employees misunderstand cyber risk, bypass security procedures, or treat information-security rules as separate from accounting work.

This paper examines employee cybersecurity awareness and policy compliance as behavioral components of AIS control reliability. The focus is deliberately accounting-centered. Financial data protection is not treated here as a general information-technology outcome; it is treated as a condition for preserving the confidentiality, integrity, availability, and auditability of financial information. Recent accounting and AIS research has increasingly connected cybersecurity incidents, cyber disclosures, internal controls, audit work, technology adoption, and data governance (Amani, 2025; Blakely et al., 2022; Kelton & Yang, 2024; Slapničar et al., 2022; Wang et al., 2022; Zhou & Huang, 2024). Yet the employee-level control behavior that occurs before a breach or disclosure event remains less visible in accounting research.

The issue is especially relevant in financial institutions. Employees in banks, mobile-money providers, microfinance institutions, and related financial service organizations handle customer balances, payment records, account documentation, audit evidence, reconciliations, and compliance files. These records are sensitive in both financial and accounting terms. If employees fail to follow access controls, ignore phishing warnings, share credentials, use devices insecurely, or bypass reporting procedures, the result may be more than a technology weakness. It may become a financial data integrity problem and, in severe cases, a breakdown in the control environment.

Somali financial institutions provide a useful setting for examining this problem. The sector is rapidly digitalizing, relies heavily on electronic financial services, and combines banking, mobile money, and microfinance activities in a regulatory environment still developing formal digital-control capacity. The purpose of using this setting is not to claim that Somalia is unique, but to provide evidence from a low-resource and under-researched financial environment where employee conduct is likely to matter because institutions rely heavily on people, procedures, and policy compliance to protect financial data.

The study asks two questions. First, is overall cybersecurity awareness associated with financial data protection among employees in Somali financial institutions? Second, which specific awareness dimensions independently predict financial data protection when considered together? The empirical analysis uses a survey of 415 employees across financial institutions and tests the relationship between financial data protection and five awareness-related dimensions: general cybersecurity awareness, password security practices, phishing awareness, device security practices, and policy compliance.

The results show a moderate positive association between overall cybersecurity awareness and financial data protection. In the multivariable regression model, general cybersecurity awareness and policy compliance remain significant positive predictors. Password security practices, phishing awareness, and device security practices are positively associated with financial data protection in the correlation analysis, but they do not remain significant after adjustment. This pattern suggests that specific practices matter, but that their independent explanatory power is weaker once broader risk understanding and formal compliance behavior are included.

The paper contributes to accounting research in three ways. First, it reframes cybersecurity awareness as part of the AIS control environment rather than as a narrow technical training issue. Second, it provides employee-level evidence on financial data protection, a control outcome that sits between system security and accounting information reliability. Third, it identifies policy compliance as the strongest predictor in the model, supporting the view that cyber knowledge protects financial records most effectively when it is translated into formal rules, routines, and accountability mechanisms.

2 Literature review and hypothesis development

2.1 Financial data protection as an AIS control outcome

AIS research increasingly studies accounting systems as digital, data-intensive, and control-dependent environments. The literature on digital accounting, audit technology, blockchain, artificial intelligence, process mining, continuous monitoring, and new technology adoption shows that accounting work is changing from periodic record processing toward continuous data capture, automated review, and technology-mediated judgment (Föhr et al., 2025; Han et al., 2023; Jackson & Allen, 2024; Murphy et al., 2024; Vitali & Giuliani, 2024; Wang & Vasarhelyi, 2024). These developments increase the importance of data protection because accounting outputs are only credible when the underlying data are complete, accurate, authorized, and traceable.

Financial data protection is therefore an AIS control outcome. It reflects whether employees and systems protect financial and customer information from unauthorized access, improper modification, leakage, misuse, or loss. This outcome is broader than cybersecurity incident prevention, but narrower than general organizational security culture. It concerns the protection of accounting-relevant information that supports internal reporting, external reporting, audit evidence, management monitoring, compliance work, and customer trust.

Recent accounting studies show that cyber risks and data breaches are connected to internal controls, disclosure, investor perceptions, and audit governance. Cyber breach reports contain information about internal-control conditions (Blakely et al., 2022). Internal controls shape the interpretation of breach contagion effects (Kelton & Yang, 2024). Data breaches are associated with subsequent internal-control responses (Zhou & Huang, 2024). Cybersecurity audit effectiveness and cybersecurity governance have become important topics in AIS and internal audit research (Alzeban et al., 2026; Slapničar et al., 2022, 2023). These studies justify treating cybersecurity not as a peripheral technology concern, but as a control issue relevant to accounting scholarship.

2.2 Cybersecurity awareness and employee control behavior

Cybersecurity awareness refers to an employee's practical understanding of cyber threats, vulnerabilities, institutional exposure, secure conduct, and the consequences of insecure behavior. In financial institutions, such awareness matters because employees routinely make decisions that affect financial records: whether to verify a request, report suspicious activity, protect credentials, follow approval channels, use devices securely, or handle customer data through approved systems.

Recent security-behavior studies indicate that awareness, policy clarity, protection motivation, compliance norms, and organizational citizenship behavior influence whether employees follow information-security requirements (Alrawhani et al., 2025; Balagopal & Mathew, 2024; Nwankpa & Datta, 2023; Vedadi et al., 2024). Evidence from banking also suggests that cybersecurity awareness is not simply a technical skill but a behavioral and organizational capability shaped by perceived threats, training, policy expectations, and institutional support (Chanda et al., 2025). This is relevant to accounting because financial data protection depends heavily on how employees behave when technical and procedural controls meet daily work.

Policy compliance is particularly important. Formal policies translate broad control objectives into concrete routines: how financial data should be accessed, stored, shared, approved, reported, escalated, and audited. In the absence of compliance, specific knowledge about phishing, passwords, or devices may not translate into protected financial records. Conversely, when compliance is strong, employee awareness can become part of a wider control environment. The accounting implication is that cybersecurity awareness should be examined not only as knowledge, but as behavior embedded in internal control.

2.3 Hypotheses

Overall cybersecurity awareness is expected to be positively associated with financial data protection because employees who better understand cyber risk should be more careful when handling customer information, transaction records, account credentials, and internal documents.

H1: Overall cybersecurity awareness is positively associated with financial data protection.

General cybersecurity awareness captures broad understanding of institutional cyber exposure, common attack patterns, and the consequences of insecure conduct. Employees with stronger general awareness should be more likely to recognize financial-data risks across different work situations.

H2: General cybersecurity awareness positively predicts financial data protection.

Password security practices represent basic access-control discipline. In AIS environments, weak password behavior can compromise authorization boundaries and expose financial records to unauthorized access.

H3: Password security practices positively predict financial data protection.

Phishing awareness reflects the ability to identify deceptive messages, malicious links, false instructions, and social-engineering attempts. Because phishing may target payment approval, customer information, and account credentials, stronger phishing awareness should support financial data protection.

H4: Phishing awareness positively predicts financial data protection.

Device security practices involve secure endpoint use, update discipline, access protection, and safe handling of institutional devices. Such practices should reduce exposure to leakage, unauthorized access, or data compromise.

H5: Device security practices positively predict financial data protection.

Policy compliance reflects adherence to formal security and data-handling rules. Because policies convert control objectives into repeatable routines, policy compliance should be a direct predictor of financial data protection.

H6: Policy compliance positively predicts financial data protection.

3 Research methodology

3.1 Research design and accounting setting

This study adopts a quantitative, cross-sectional survey design to examine whether employee cybersecurity awareness and policy-compliance behavior are associated with financial data protection in accounting information systems. The design is appropriate because the study investigates variation in employee-level control behavior across a broad financial-sector sample rather than the effect of a single intervention. The dependent construct, financial data protection, is treated as an accounting information system control outcome because financial records, transaction histories, customer account data, reconciliations, audit trails, and compliance documentation depend on secure access, accurate processing, and disciplined information handling.

The empirical setting is Somalia's banking and financial-services sector. This context is relevant for accounting research because financial institutions operate in a rapidly digitalizing environment where accounting records and customer financial information are increasingly processed through digital platforms, core banking systems, payment channels, mobile money interfaces, and branch-level operational systems. In such settings, the reliability of accounting information does not depend only on formal system design; it also depends on employees' day-to-day compliance with access, password, device, phishing, reporting, and data-handling rules. The study therefore positions cybersecurity awareness as part of the human and organizational control environment surrounding accounting information systems.

The research question is whether cybersecurity awareness and policy compliance predict stronger financial data protection among employees who handle, process, review, or supervise financial information. The paper does not claim to measure actual cyber incidents or externally audited control failures. Instead, it measures employee-reported protection behavior and perceived data-handling discipline, which are appropriate for studying human control behavior but should be interpreted as behavioral control evidence rather than archival evidence of breach reduction.

3.2 Population, sampling strategy, and respondents

The target population consisted of permanent employees working in Somali banking and financial institutions whose roles involved access to financial records, transaction systems, customer information, accounting documents, compliance records, or operational data. The institutional population covered Islamic banks, conventional banks, mobile money and financial-service providers, and microfinance institutions. These institution types were included because they represent the main formal and semi-formal financial channels through which sensitive financial information is collected, processed, stored, and reported in Somalia.

Data were collected from 415 respondents between 15 February 2025 and 30 March 2025. Respondents represented operational, accounting, finance, customer service, ICT, compliance, risk, branch-management, and internal-audit functions. This range of roles is important because financial data protection is not performed by ICT staff alone. Accounting and operational employees create, approve, reconcile, transmit, review, and archive financial information, while compliance and audit staff monitor

whether institutional rules are followed. The sample therefore captures employees positioned at different points in the accounting information-processing chain.

The sampling strategy was stratified by institution type. Stratification was used to reduce the risk that the sample would be dominated by one type of financial institution and to improve coverage across banks, mobile money and financial-service providers, and microfinance institutions. Within the accessible institutions and branches, eligible employees were invited to complete the questionnaire if they met the inclusion criteria. The inclusion criteria were: permanent employment status, at least three months of work experience in the institution, and a role involving access to financial data, customer information, transaction records, or related operational systems. Interns, temporary staff, and employees on extended leave during the data-collection period were excluded.

The final sample size of 415 is adequate for the correlation and multiple-regression analyses reported in the study. The regression model includes five main predictors, which gives a high respondent-to-predictor ratio and allows stable estimation of the main associations. The demographic and institutional profile of the sample is reported in Table 1 to show the distribution of respondents across gender, age, position, department, experience, and institution type.

3.3 Survey administration and data-collection procedure

The study used a self-administered paper questionnaire. Paper administration was selected because it allowed branch-based distribution and collection while avoiding dependence on email response rates or online survey access. Questionnaires were distributed at branch offices and collected after one week. Respondents completed the questionnaire anonymously and were not asked to provide names, staff identification numbers, phone numbers, or other direct personal identifiers. This procedure was intended to reduce fear of employer monitoring and encourage more honest responses about security behavior and compliance practice.

Before completing the questionnaire, respondents were informed about the purpose of the study, the voluntary nature of participation, the confidentiality of responses, and their right not to participate. Completed questionnaires were screened before analysis for eligibility and usability. The analytical dataset used in the manuscript contains only valid responses used to compute the study constructs and statistical outputs. No institution-specific or respondent-identifying information is reported in the manuscript.

3.4 Measurement instrument and construct operationalization

All main constructs were measured using multi-item scales on a five-point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree. Multi-item scales were used because cybersecurity awareness, compliance behavior, and financial data protection are latent behavioral constructs that cannot be captured reliably by a single item. Construct scores were computed by averaging the retained items for

each scale, so higher scores indicate stronger agreement with the relevant awareness, practice, compliance, or protection statements.

The independent variables consist of five cybersecurity-awareness and security-behavior dimensions. General Cybersecurity Awareness measures broad understanding of cyber threats, secure work behavior, institutional exposure, and the consequences of weak security conduct. Password Security Practices captures password discipline, credential protection, and secure access behavior. Phishing Awareness measures the ability to recognize deceptive messages, suspicious links, and social-engineering attempts. Device Security Practices captures secure endpoint use, software-update discipline, and safe handling of institutional devices. Policy Compliance measures adherence to formal cybersecurity, data-handling, and internal-control rules.

The dependent variable is Financial Data Protection. It captures employee-reported behavior and perceived control discipline related to safeguarding financial and customer information. The construct covers careful handling of financial records, protection against unauthorized access, safe sharing and storage of data, respect for institutional procedures, and practices that support confidentiality, integrity, and auditability of financial information. In accounting terms, the construct represents a behavioral proxy for the quality of the human control environment surrounding accounting information systems, rather than a direct archival measure of reporting quality or fraud incidence.

Overall Cybersecurity Awareness was computed as a composite across the awareness dimensions and is used in the correlation analysis to test the broad association between cybersecurity awareness and financial data protection. The regression model then separates the dimensions to identify which specific components remain significant after mutual adjustment. This distinction is important because a simple overall score can hide whether protection is mainly associated with general awareness, specific technical habits, or formal policy compliance.

3.5 Reliability and measurement quality

Internal consistency was assessed using Cronbach's alpha for each multi-item construct. The reliability results support the use of the scales in subsequent analysis. Cronbach's alpha values were 0.853 for General Cybersecurity Awareness, 0.840 for Password Security Practices, 0.822 for Phishing Awareness, 0.839 for Device Security Practices, 0.912 for Policy Compliance, and 0.931 for Financial Data Protection. These values indicate acceptable to excellent internal consistency and suggest that the items within each scale measure coherent constructs.

The descriptive statistics and reliability results are reported in Table 2. The analysis also reports minimum and maximum values to show the observed range of responses for each construct. Because the study uses self-reported survey data, the results should be interpreted as evidence of perceived and reported control behavior. The design does not eliminate the possibility of social-desirability bias or common-method bias, and these issues are explicitly discussed as limitations rather than hidden in the interpretation.

3.6 Empirical model and statistical analysis

The empirical analysis was conducted in Python. The analysis proceeded in four stages. First, descriptive statistics summarized respondent characteristics and the distribution of the main constructs. Second, Pearson correlation analysis examined bivariate relationships between cybersecurity-awareness dimensions, overall cybersecurity awareness, and financial data protection. Third, multiple linear regression estimated the independent association between each awareness dimension and financial data protection. Fourth, diagnostic tests evaluated whether the regression model satisfied core statistical assumptions.

The main regression model is specified as follows:

FDPi = beta0 + beta1GCAi + beta2PSPi + beta3PAi + beta4DSPi + beta5PCi + epsiloni

where FDP is Financial Data Protection, GCA is General Cybersecurity Awareness, PSP is Password Security Practices, PA is Phishing Awareness, DSP is Device Security Practices, PC is Policy Compliance, and epsiloni is the error term. The model tests whether each cybersecurity-awareness dimension predicts financial data protection after the other dimensions are held constant. The coefficient on Policy Compliance is especially important for the accounting interpretation because it captures whether formal rule-following behavior contributes to the protection of financial information beyond general awareness and isolated security habits.

The hypotheses were evaluated using statistical significance, coefficient direction, standardized effect size, confidence intervals, and overall model fit. The study reports unstandardized coefficients, standard errors, standardized beta coefficients, t-statistics, p-values, and 95% confidence intervals. Model fit is assessed using R-squared and adjusted R-squared. The paper interprets statistically significant positive coefficients as evidence that a construct is associated with stronger financial data protection, while avoiding causal language because the study is cross-sectional.

3.7 Regression diagnostics and assumption checks

Regression diagnostics were conducted to assess whether the multiple regression model could be interpreted without serious statistical violations. Multicollinearity was evaluated using variance inflation factors. Residual normality was assessed using the Shapiro-Wilk test, a histogram of residuals, and a Q-Q plot. Homoscedasticity was assessed using the Breusch-Pagan test and a residuals-versus-fitted plot. Residual independence was assessed using the Durbin-Watson statistic. These diagnostics are reported in the results section and supplementary tables so that readers can evaluate the stability and credibility of the regression estimates.

This diagnostic approach is important for the present study because the paper relies on primary survey data rather than archival financial statements, system logs, or externally audited control records. The study therefore makes the estimation assumptions transparent and reports whether the empirical model shows serious problems of multicollinearity, non-normality, heteroscedasticity, or autocorrelation.

3.8 Ethical considerations and anonymity

The study involved an anonymous, non-clinical employee survey about workplace cybersecurity and financial data-protection practices. It did not involve medical information, minors, vulnerable populations, or direct personal identifiers in the analytical dataset. Participation was voluntary, and respondents were informed that they could decline participation. The survey collected perceptions and workplace-practice responses rather than confidential institutional breach records or customer-level financial data.

Because the manuscript is prepared for double-anonymous peer review, author-identifying details, acknowledgements, and institution-identifying information are excluded from the blinded manuscript. Funding, competing interests, author contributions, ethics-related statements, and any identifying details should be supplied separately through the journal submission system or title-page file according to the journal's instructions.

3.9 Methodological boundaries

The methodology has boundaries that should be considered when interpreting the findings. The cross-sectional design supports association testing but does not establish causality. The use of self-reported measures may introduce response bias. The absence of externally verified incident records means the study cannot determine whether awareness or compliance reduces actual breach frequency. The model also focuses on employee awareness and compliance rather than technical security maturity, investment level, system architecture, or formal audit outcomes. These limitations do not invalidate the study, but they define the scope of the evidence and are addressed again in the limitations section.

4 Results

4.1 Sample characteristics

Table 1 reports the sample characteristics. The sample includes employees across financial institution types and roles that directly interact with transaction processing, customer data, accounting records, compliance documentation, technology systems, and internal audit activities. This composition is appropriate for examining financial data protection as a behavioral AIS control outcome.

Table 1
Sample characteristics of respondents (N = 415)

Variable	Category	n	Percentage
Gender	Male	251	60.48
	Female	164	39.52
Age Group	26–35	184	44.34
	18–25	96	23.13
	36–45	89	21.45
	46 and above	46	11.08
Current Position	Operations Officer	74	17.83
	Customer Service Officer	71	17.11
	Teller	58	13.98
	IT / ICT Officer	53	12.77
	Accountant / Finance Officer	48	11.57
	Branch Manager	40	9.64
	Compliance / Risk Officer	38	9.16
	Internal Auditor	33	7.95
Department	Operations	96	23.13
	Finance / Accounting	75	18.07
	Customer Service	59	14.22
	Compliance / Risk	55	13.25
	ICT / Information Security	53	12.77
	Internal Audit	44	10.60
	Administration	33	7.95
Years of Experience	1–3 years	123	29.64
	4–6 years	113	27.23
	7–10 years	79	19.04
	More than 10 years	53	12.77
	Less than 1 year	47	11.33
Bank Type	Islamic Bank	228	54.94

Variable	Category	n	Percentage
	Conventional Bank	85	20.48
	Mobile Money / Financial Service Provider	56	13.49
	Microfinance Institution	46	11.08

4.2 Descriptive statistics and reliability

Table 2 shows that mean values for the study constructs are concentrated in the upper-middle range of the five-point scale. Financial Data Protection has a mean of 3.790 and a standard deviation of 0.553. Overall Cybersecurity Awareness has a mean of 3.794 and a standard deviation of 0.376. The reliability statistics support the use of the retained constructs in the regression analysis.

Table 2
Descriptive statistics and reliability of study constructs

Construct	Items	Mean	SD	Min	Max	Cronbach's α
General Cybersecurity Awareness	6	3.791	0.572	2.167	5.000	0.853
Password Security Practices	5	3.799	0.570	2.400	5.000	0.840
Phishing Awareness	5	3.791	0.561	2.000	5.000	0.822
Device Security Practices	5	3.790	0.579	2.200	5.000	0.839
Policy Compliance	9	3.797	0.565	1.889	5.000	0.912
Overall Cybersecurity Awareness	5 dimensions	3.794	0.376	2.484	4.960	—
Financial Data Protection	12	3.790	0.553	2.167	5.000	0.931
Perceived Effectiveness of Cybersecurity Measures	6	3.803	0.560	2.333	5.000	0.851

4.3 Correlation analysis

Table 3 reports the Pearson correlations. Financial Data Protection is positively and significantly correlated with General Cybersecurity Awareness, Password Security Practices, Phishing Awareness, Device Security Practices, Policy Compliance, and Overall Cybersecurity Awareness. The strongest bivariate association is between Policy Compliance and Financial Data Protection, followed by Overall Cybersecurity Awareness and General Cybersecurity Awareness. These results support H1 at the bivariate level.

Table 3
Pearson correlation matrix

No.	Variable	1	2	3	4	5	6	7
1	General Cybersecurity Awareness	—						
2	Password Security Practices	0.391***	—					
3	Phishing Awareness	0.404***	0.181***	—				
4	Device Security Practices	0.412***	0.297***	0.122*	—			
5	Policy Compliance	0.447***	0.221***	0.191***	0.278***	—		
6	Overall Cybersecurity Awareness	0.805***	0.634***	0.571***	0.643***	0.646***	—	
7	Financial Data Protection	0.439***	0.178***	0.240***	0.161**	0.460***	0.447***	—

Notes: *, **, and *** indicate statistical significance at the 0.05, 0.01, and 0.001 levels, respectively.

Figure 1 visualizes the positive association between overall cybersecurity awareness and financial data protection. The fitted line is upward sloping, consistent with the correlation result.

4.4 Regression results

Table 4 reports the multiple regression results. The overall model is statistically significant, $F(5, 409) = 32.851$, $p < 0.001$, and explains 28.7% of the variance in Financial Data Protection ($R^2 = 0.287$; adjusted $R^2 = 0.278$). General Cybersecurity Awareness is a positive and significant predictor. Policy Compliance is also positive and significant and has the largest standardized coefficient in the model. Password Security Practices, Phishing Awareness, and Device Security Practices are not statistically significant after adjustment.

The regression evidence supports H2 and H6. H3, H4, and H5 are not supported in the adjusted model. The non-significant adjusted effects should not be read as evidence that password, phishing, or device behaviors are irrelevant. Rather, these practices appear to overlap with broader awareness and compliance behavior when the predictors are entered together.

Table 4
Multiple regression predicting financial data protection

Predictor	Unstandardized B	SE	Standardized β	t	p	95% CI	Sig.
General Cybersecurity Awareness	0.277	0.053	0.287	5.236	< 0.001	[0.173, 0.381]	***
Password Security Practices	-0.003	0.045	-0.003	-0.061	0.951	[-0.091, 0.085]	
Phishing Awareness	0.067	0.045	0.068	1.484	0.138	[-0.022, 0.156]	
Device Security Practices	-0.055	0.045	-0.058	-1.237	0.217	[-0.143, 0.033]	
Policy Compliance	0.328	0.046	0.335	7.119	< 0.001	[0.238, 0.419]	***

Notes: Dependent variable = Financial Data Protection. ***, p < 0.001. Confidence intervals are 95% intervals.

Figure 2 shows that the confidence intervals for General Cybersecurity Awareness and Policy Compliance do not cross zero, while the confidence intervals for the other predictors do cross zero.

4.5 Regression diagnostics

Tables 5 and 6 report the diagnostic checks. VIF values range from 1.200 to 1.722, which does not indicate problematic multicollinearity. The Shapiro-Wilk and Breusch-Pagan tests are non-significant, and the Durbin-Watson statistic is close to 2. The diagnostic plots in Figs. 3–5 are consistent with the statistical tests and do not indicate serious violations of the model assumptions.

Table 5
Variance inflation factor diagnostics

Predictor	VIF
General Cybersecurity Awareness	1.722
Password Security Practices	1.215
Phishing Awareness	1.200
Device Security Practices	1.256
Policy Compliance	1.269

Table 6
Regression assumption checks

Test	Statistic	p
Shapiro-Wilk normality	0.998	0.927
Breusch-Pagan homoscedasticity	3.671	0.598
Durbin-Watson independence	2.025	—

5 Discussion

5.1 Main interpretation

The findings show that cybersecurity awareness matters for financial data protection, but not all awareness dimensions matter in the same way. At the bivariate level, each awareness-related variable is positively associated with financial data protection. In the adjusted model, however, only General Cybersecurity Awareness and Policy Compliance remain significant. This pattern suggests that financial data protection is linked more strongly to broad risk understanding and rule-consistent behavior than to isolated security habits considered separately.

Policy Compliance is the strongest predictor in the regression model. This result is important for accounting because formal policies are the mechanism through which the control environment becomes operational. Policies define who may access financial data, how records should be handled, when exceptions should be escalated, how suspicious activity should be reported, and how evidence should be preserved. When employees comply with such policies, cybersecurity awareness becomes part of the internal-control system rather than a detached training outcome.

The non-significant adjusted effects for password security, phishing awareness, and device security should be interpreted cautiously. These practices are still necessary. Their positive bivariate correlations indicate that they move in the expected direction. The regression model suggests, however, that their independent contribution is limited after broader awareness and compliance behavior are included. A plausible explanation is that employees who have stronger specific practices are also those who possess stronger general awareness and are more likely to comply with policy.

5.2 Practical implications

For financial institutions, the findings suggest that cybersecurity training should be linked directly to accounting workflows. Training should not be limited to general password or phishing modules. It should be role-based and tied to customer onboarding, payment authorization, cash and bank reconciliation, exception handling, document retention, audit-trail preservation, and incident escalation.

For internal audit and compliance units, the findings support treating cybersecurity policy compliance as part of the control environment. Internal auditors should assess whether staff understand information-

security procedures, whether policy exceptions are documented, whether incident reporting is timely, and whether data-handling practices preserve audit evidence. Cybersecurity compliance failures should be treated as control deviations, not only as ICT issues.

For regulators and sector supervisors, the study suggests that cyber resilience in financial institutions should include staff awareness, policy enforcement, internal-control integration, and incident-reporting discipline. Technical safeguards remain necessary, but the evidence here indicates that behavioral controls and policy compliance are central to protecting financial information.

5.3 Limitations and future research

The study has limitations. First, the cross-sectional design prevents causal inference. The results should be interpreted as associations, not proof that awareness causes financial data protection. Second, the measures are self-reported and may be affected by social-desirability bias. Third, common method bias was not formally tested. Fourth, the dependent variable captures reported financial data protection rather than observed incidents, audit exceptions, system logs, or forensic evidence. Fifth, the model explains 28.7% of the variance, which means other technical, governance, cultural, and institutional factors remain important.

Future research should use longitudinal designs, field experiments, audit evidence, system logs, incident reports, or objective control-testing data. Future studies could test whether policy compliance mediates the relationship between cybersecurity awareness and financial data protection, whether internal audit maturity moderates the relationship, and whether the effects differ across banks, mobile money providers, and microfinance institutions. Scenario-based experiments could also examine how accounting and finance employees respond to cyber-risk situations involving payment approvals, customer data, or audit evidence preservation.

6 Conclusion

This study examines cybersecurity awareness, policy compliance, and financial data protection in the AIS environment of Somali financial institutions. The results show that overall cybersecurity awareness is positively associated with financial data protection. In the multivariable model, General Cybersecurity Awareness and Policy Compliance are significant positive predictors, while Password Security Practices, Phishing Awareness, and Device Security Practices do not have independent adjusted effects.

The central conclusion is that financial data protection is not secured mainly through isolated employee habits. It is better supported by broad cyber-risk understanding and compliance behavior embedded in the accounting-control environment. For accounting research, this means cybersecurity should be studied not only as an external disclosure risk or technology problem, but also as an employee-level control issue inside AIS. For financial institutions, it means that cyber awareness becomes valuable when it is translated into policies, monitoring, accountability routines, and protection of financial records.

Declarations

Competing interests

The author(s) declare no competing interests.

Ethics declaration

This study was reviewed and approved by the Ethics Committee of the Center for Research and Development (CRD), SIMAD University, Mogadishu, Somalia (Approval No. EC000173; approved on 16 May 2026).

The research was conducted in accordance with the ethical principles of respect for persons, beneficence, and justice, as outlined in the ethical guidelines of SIMAD University and internationally recognized standards for human-subject research.

Prior to participation, all respondents were provided with an information sheet explaining the purpose of the study, the voluntary nature of participation, the procedures involved, the expected duration, potential risks and benefits, and the measures taken to ensure confidentiality and anonymity. Informed consent was obtained from all participants before data collection commenced. Consent was secured through voluntary agreement to participate after participants had been fully informed about the study and their rights, including the right to decline participation or withdraw from the study at any time without penalty.

No personally identifiable information was collected, and all data were analyzed and reported in aggregate form to protect participant privacy and confidentiality.

Author Contribution

Nasro Khalif Abdullahi conceived the study, designed the methodology, conducted the investigation, administered the survey, curated the data, performed the formal analysis, prepared the original draft of the manuscript, managed the project administration, and served as the corresponding author.Abdullahi Salad Abdi contributed to the conceptualization of the study, supervised the research process, reviewed the methodology, validated the empirical interpretation, reviewed and edited the manuscript, and provided overall academic guidance and support.Both authors reviewed and approved the final version of the manuscript and agree to be accountable for all aspects of the work.

Acknowledgement

The authors thank SIMAD University for its financial and institutional support. The authors also acknowledge the valuable feedback from colleagues during the preparation of this manuscript.

Data Availability

The data generated and analysed during the current study are not publicly available because they contain participant-level responses from employees of financial institutions and are subject to confidentiality and ethical restrictions. An anonymised version of the dataset may be made available from the corresponding author upon reasonable request, subject to institutional approval and appropriate data-sharing conditions.

Code availability

The Python code used for the statistical analyses can be made available from the corresponding author on reasonable request, subject to anonymization and institutional permission.

References

1. Alrawhani EM, Romli A, Al-Sharafi MA (2025) Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. J Open Innovation: Technol Market Complex 11(1):100463. https://doi.org/10.1016/j.joitmc.2024.100463
2. Alzeban A, Al-Hajaya K, Sawan N (2026) The quality of cybersecurity audits: Do synergies among the chief audit executive, IT governance and internal audit functions matter? Managerial Auditing Journal. https://doi.org/10.1108/MAJ-05-2025-4825. Advance online publication
3. Amani FA (2025) Cybersecurity risks and incidents disclosure: A literature review. Contemp Acc Res. https://doi.org/10.1111/1911-3838.12411. Advance online publication
4. Balagopal N, Mathew SK (2024) Exploring the factors influencing information security policy compliance and violations: A systematic literature review. Computers Secur 147:104062. https://doi.org/10.1016/j.cose.2024.104062
5. Blakely B, Kurtenbach J, Nowak L (2022) Exploring the information content of cyber breach reports and the relationship to internal controls. Int J Acc Inform Syst 46:100568. https://doi.org/10.1016/j.accinf.2022.100568
6. Borrero-Domínguez C, Cortijo-Gallego V, Escobar-Rodríguez T (2024) Digital transformation voluntary disclosure: Insights from leading European companies. Int J Acc Inform Syst 55:100711. https://doi.org/10.1016/j.accinf.2024.100711
7. Cebi S, Karakurt NF, Kurtulus E, Tokgoz B (2024) Development of a decision support system for client acceptance in independent audit process. Int J Acc Inform Syst 53:100683. https://doi.org/10.1016/j.accinf.2024.100683
8. Chanda RC, Vafaei-Zadeh A, Hanifah H, Nikbin D (2025) Assessing cybersecurity awareness among bank employees: A multi-stage analytical approach using PLS-SEM, ANN, and fsQCA in a developing country context. Computers Secur 149:104208. https://doi.org/10.1016/j.cose.2024.104208

9. Föhr TL, Reichelt V, Marten K-U, Eulerich M (2025) A framework for the structured implementation of process mining for audit tasks. Int J Acc Inform Syst 56:100727. https://doi.org/10.1016/j.accinf.2025.100727
10. Haapamäki E, Sihvonen J (2026) Mandatory cybersecurity disclosure: Early evidence from 10-K reports. Int J Acc Inform Syst 60:100775. https://doi.org/10.1016/j.accinf.2026.100775
11. Han H, Shiwakoti RK, Jarvis R, Mordi C, Botchie D (2023) Accounting and auditing with blockchain technology and artificial intelligence: A literature review. Int J Acc Inform Syst 48:100598. https://doi.org/10.1016/j.accinf.2022.100598
12. Jackson D, Allen C (2024) Enablers, barriers and strategies for adopting new technology in accounting. Int J Acc Inform Syst 52:100666. https://doi.org/10.1016/j.accinf.2023.100666
13. Kelton AS, Yang Y-W (2024) Understanding cybersecurity breach contagion effects: The role of the loss heuristic and internal controls. Int J Acc Inform Syst 55:100714. https://doi.org/10.1016/j.accinf.2024.100714
14. Liu C, Babar MA (2025) Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Aust J Manage 51(1):1–31. https://doi.org/10.1177/03128962241293658
15. Morshed A, Khrais LT (2025) Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region. J Risk Financial Manage 18(1):41. https://doi.org/10.3390/jrfm18010041
16. Murphy B, Feeney O, Rosati P, Lynn T (2024) Exploring accounting and AI using topic modelling. Int J Acc Inform Syst 55:100709. https://doi.org/10.1016/j.accinf.2024.100709
17. Nhan VTT, Dung NNK, Phuoc T (2025) A study on the impact of accounting information security controls on the effectiveness of internal controls in Vietnamese enterprises. J Open Innovation: Technol Market Complex 11(1):100470. https://doi.org/10.1016/j.joitmc.2025.100470
18. Nwankpa JK, Datta PM (2023) Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers Secur 130:103266. https://doi.org/10.1016/j.cose.2023.103266
19. Plant OH, van Hillegersberg J, Aldea A (2022) Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment. Int J Acc Inform Syst 45:100560. https://doi.org/10.1016/j.accinf.2022.100560
20. Slapničar S, Axelsen M, Bongiovanni I, Stockdale D (2023) A pathway model to five lines of accountability in cybersecurity governance. Int J Acc Inform Syst 51:100642. https://doi.org/10.1016/j.accinf.2023.100642
21. Slapničar S, Vuko T, Čular M, Drašček M (2022) Effectiveness of cybersecurity audit. Int J Acc Inform Syst 44:100548. https://doi.org/10.1016/j.accinf.2021.100548
22. Song JM, Wang T, Yen J-C, Chen Y-H (2024) Does cybersecurity maturity level assurance improve cybersecurity risk management in supply chains? Int J Acc Inform Syst 54:100695. https://doi.org/10.1016/j.accinf.2024.100695
23. Vedadi A, Warkentin M, Straub DW, Shropshire J (2024) Fostering information security compliance as organizational citizenship behavior. Inf Manag 61(5):103968.

https://doi.org/10.1016/j.im.2024.103968

24. Vitali S, Giuliani M (2024) Emerging digital technologies and auditing firms: Opportunities and challenges. Int J Acc Inform Syst 53:100676. https://doi.org/10.1016/j.accinf.2024.100676
25. Wang T, Yen J-C, Yoon K (2022) Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. Int J Acc Inform Syst 46:100567. https://doi.org/10.1016/j.accinf.2022.100567
26. Wang W, Vasarhelyi MA (2024) The application of continuous audit and monitoring methodology: A government medication procurement case. Int J Acc Inform Syst 55:100713. https://doi.org/10.1016/j.accinf.2024.100713
27. Wu T-H, Huang S-Y, Chiu A-A, Yen DC (2024) IT governance and IT controls: Analysis from an internal auditing perspective. Int J Acc Inform Syst 52:100663. https://doi.org/10.1016/j.accinf.2023.100663
28. Zhou F, Huang J (2024) Cybersecurity data breaches and internal control. Int Rev Financial Anal 93:103174. https://doi.org/10.1016/j.irfa.2024.103174
29. Zhu J, Hu X, Gao J, Tan H (2024) Internal control risk disclosure, media coverage and stock price crash risk: Evidence from China. Int J Acc Inform Syst 55:100710. https://doi.org/10.1016/j.accinf.2024.100710

Figures

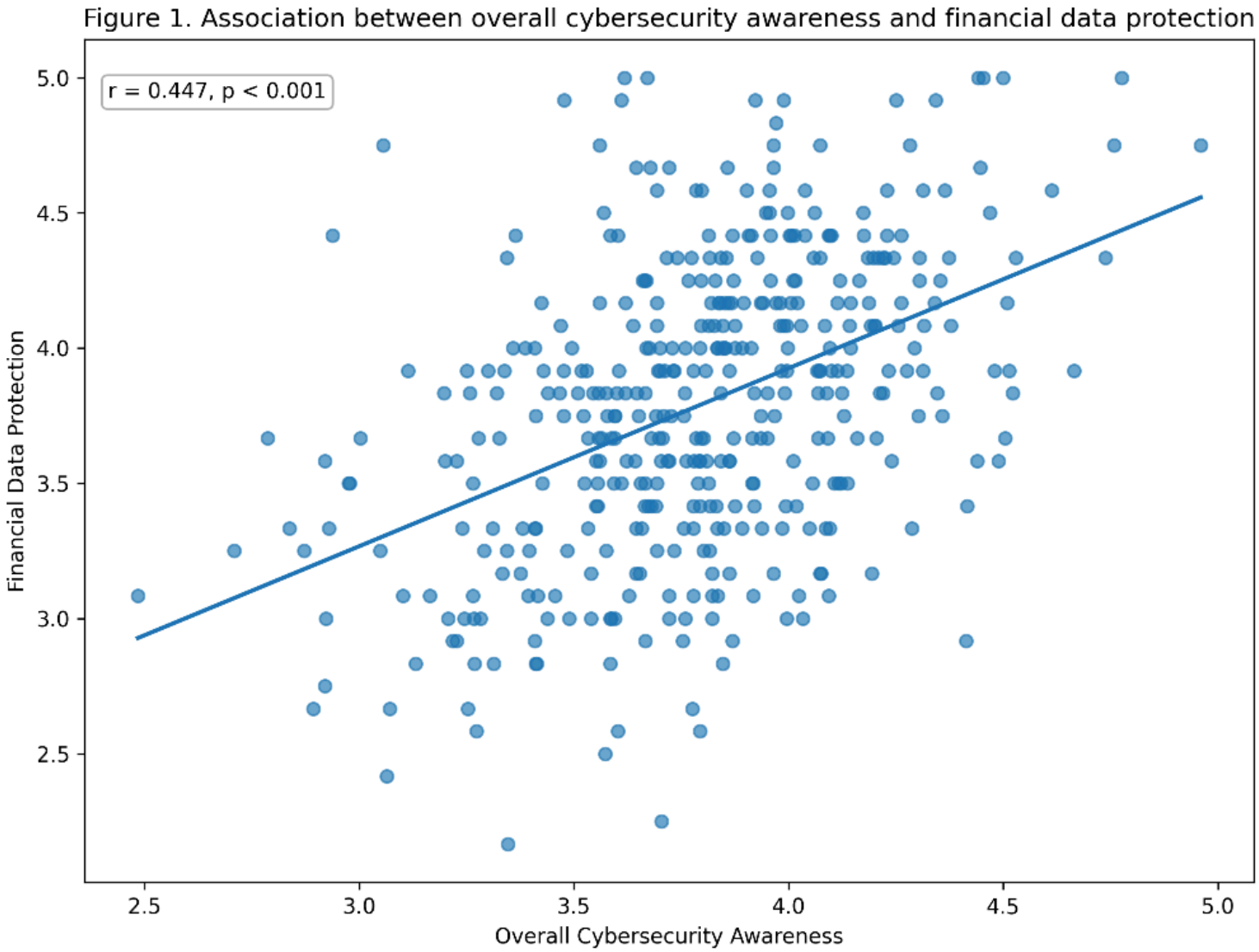


Figure 1

Association between overall cybersecurity awareness and financial data protection

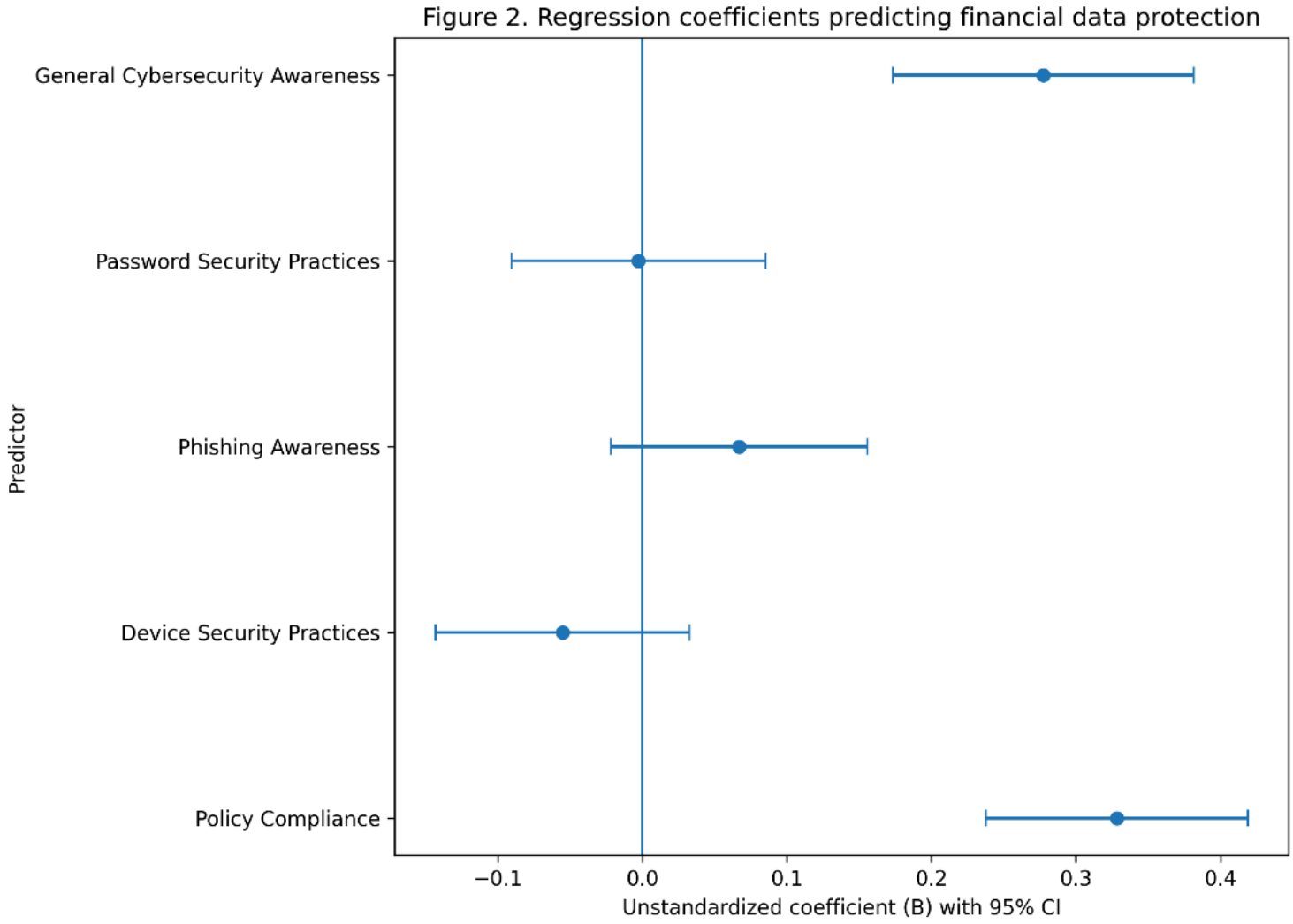


Figure 2

Regression coefficients predicting financial data protection

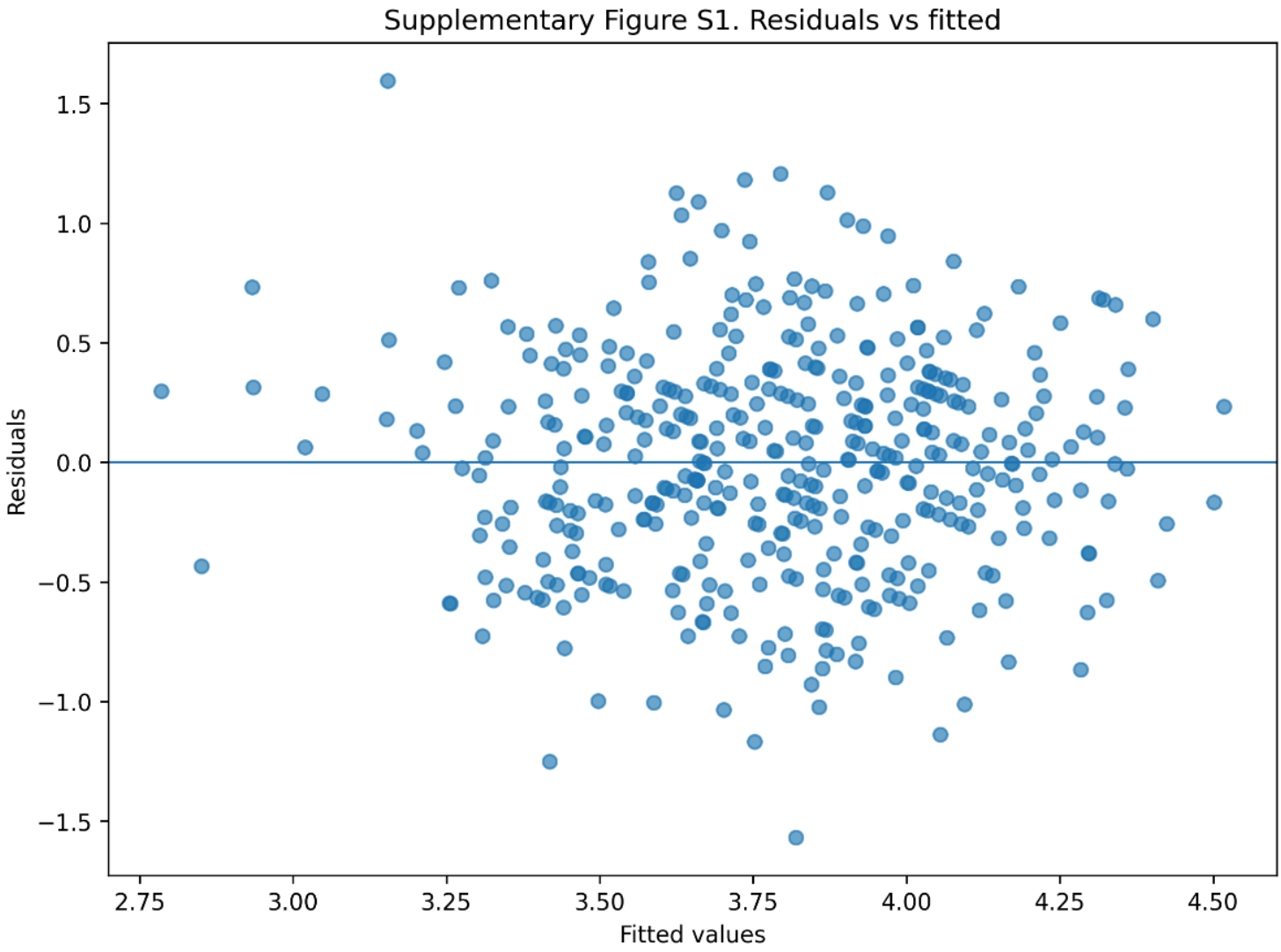


Figure 3

Residuals versus fitted values

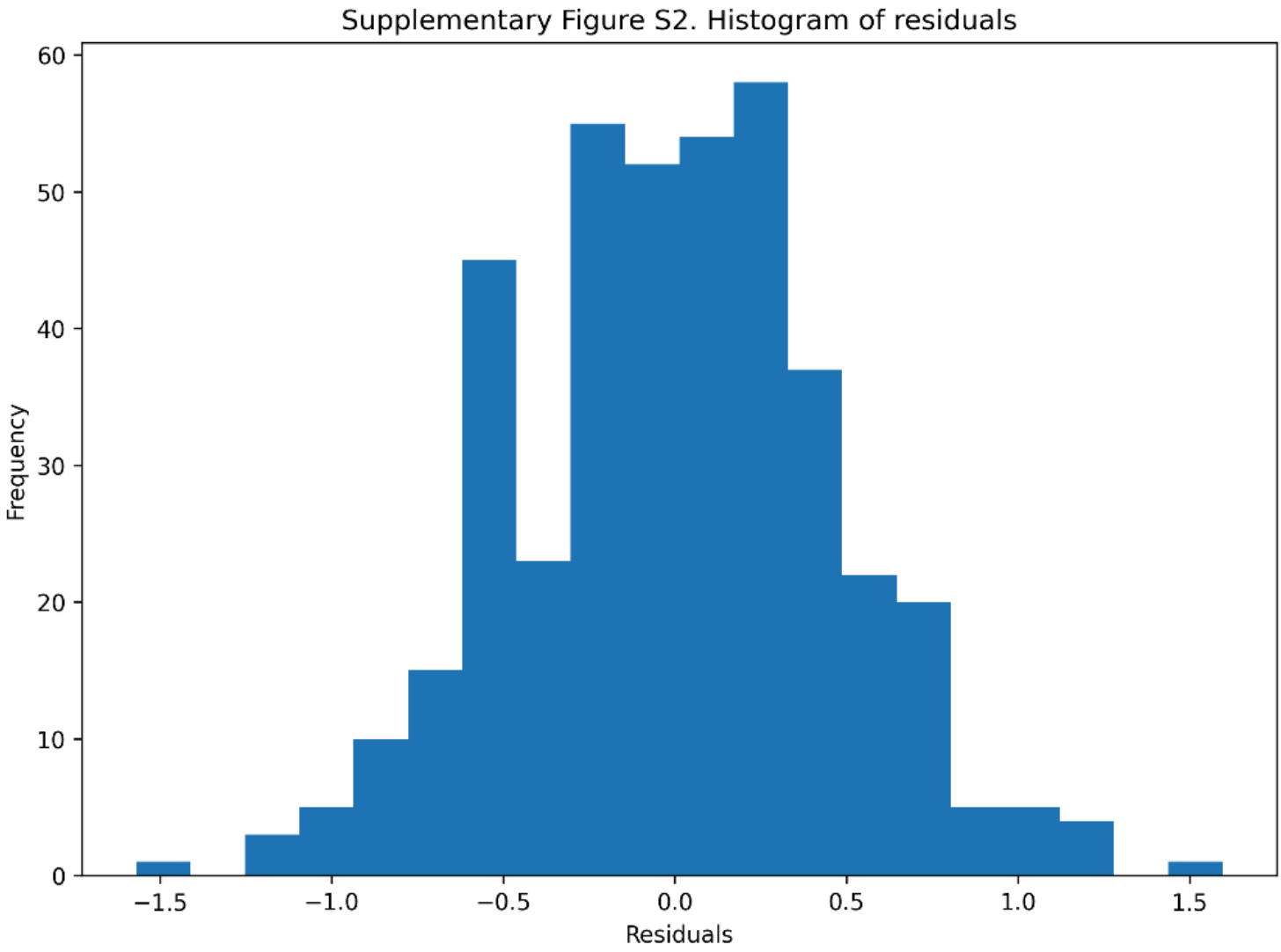


Figure 4

Histogram of residuals

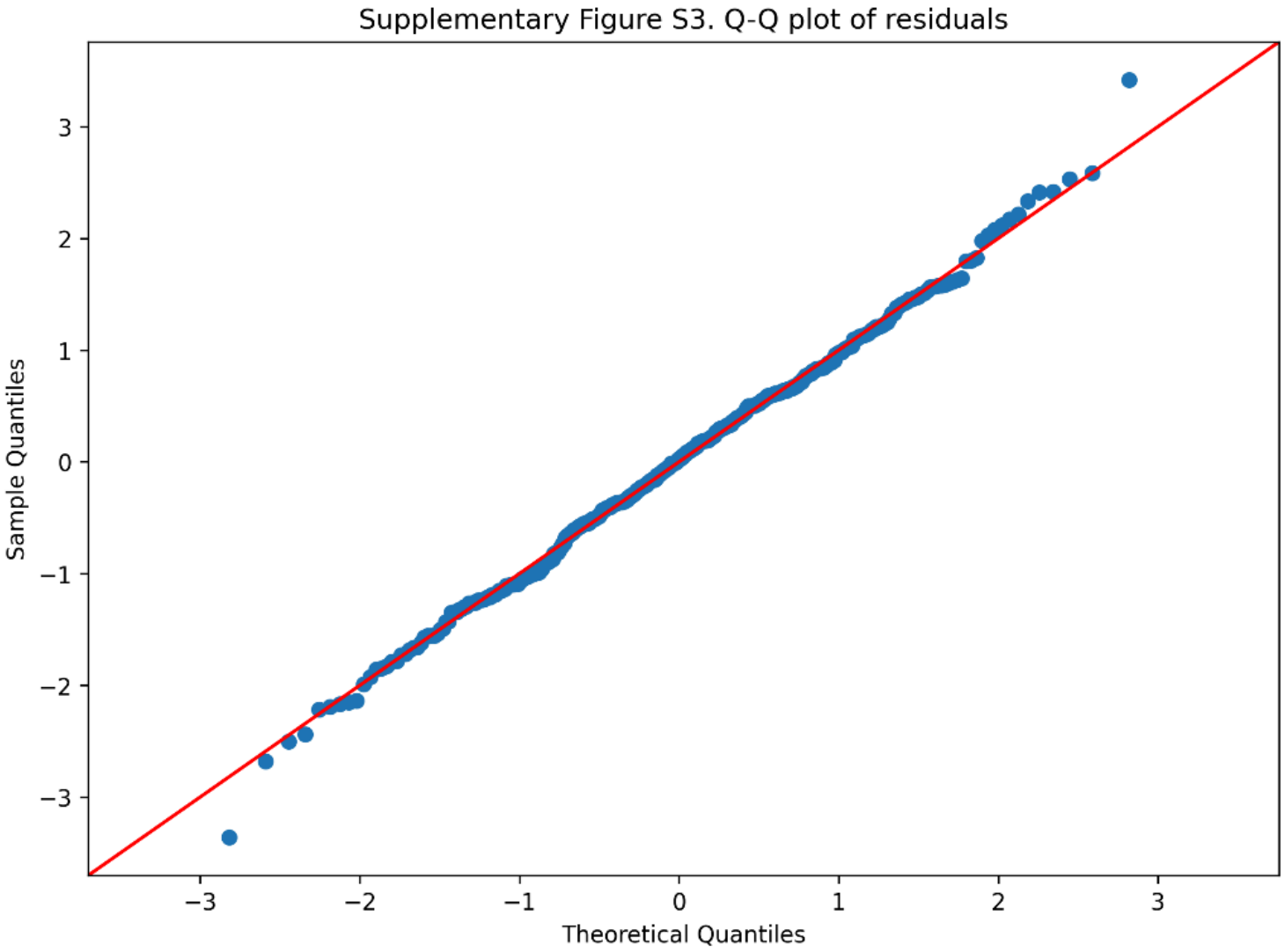


Figure 5

Q-Q plot of residuals

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- myRealDataSet.csv
- SupplementarySurveyQuestionnaire.docx
- AppendixAMeasurementdomains.docx