Al Tijarah: Vol. 12 No. 1, June 2026 (131-143)
p-ISSN: 2460-4089 e-ISSN: 2528-2948
Available at: http://ejournal.unida.gontor.ac.id/index.php/altijarah

Supportive Organizational Culture, User Involvement, And Islamic Bank Security Compliance: Mediating Role Of Attitude

Laura Puti Anggini
Department of Management, Faculty of Economics and Business, University of Swadaya Gunung Jati, Cirebon, Indonesia
laura.122020309@ugj.ac.id

Sandi Nasrudin Wibowo
Department of Management, Faculty of Economics and Business, University of Swadaya Gunung Jati, Cirebon, Indonesia
sandi.nwibowo@ugj.ac.id

Abstract

Effective information security policy compliance is nevertheless hampered by human-related concerns, especially in Islamic banking, which handles extremely sensitive financial and personal data. Non-compliance by employees still poses a danger. This study uses compliance attitude as a mediating variable to investigate how user involvement and a supportive organisational culture affect security policy compliance culture. All 91 workers of the Bank BJB Syariah Cirebon Branch were given structured questionnaires as part of a quantitative approach. Partial Least Squares Structural Equation Modelling was used to analyse the data. The findings show that user involvement and supportive organisational culture both directly and indirectly have a positive and significant impact on the culture of security policy compliance. The relevance of workers' psychological internalisation in fostering long-lasting compliance behaviour is highlighted by compliance attitude, which also exhibits a strong mediating effect. This study adds to the body of knowledge on information security by including behavioural, organisational, participative viewpoints into a thorough compliance framework. To promote good compliance attitudes and information security governance, Islamic financial organisations should, practically speaking, go beyond just technical legal procedures by fostering a supportive culture and enhancing staff participation.
Keywords: *information security policy compliance; supportive organizational culture; user involvement; compliance attitudes; Islamic banking.*

A. INTRODUCTION

The banking industry currently manages client financial data more carefully due to the rapid growth of information technology, which makes information security an important component of business. In this context, Security Policy compliance Culture can be optimally achieved through the creation of a Supportive Organizational Culture, a key strategy for minimizing employee non-compliance. This culture is fostered by a conducive work environment, active user involvement, and leadership that demonstrates a strong commitment to compliance, thereby shaping employees' attitudes and motivation towards security practices in the company (Amankwa et al., 2018). In an effort to identify the root causes of non-compliance, research Herath & Rao (2009), reveals that the implementation of procedures and enforcement of data security regulations are influenced by organizational, external, and behavioral factors, grounded in protection motivation theory and prevention theory. Delving deeper into organizational aspects, the study findings show that an inward-focused corporate Culture has a favorable relationship with employee compliance with information

security regulations (Karlsson et al., 2022). In addition, increasing comprehension of the importance of data protection also creates institutional pressure for organizations to comply with security standards, whether through coercive, normative, or imitative pressure (AlKalbani et al., 2017). Therefore, to improve user compliance, information security Programs for information security awareness have been put in place by managers, and they are a methodically structured approach to consistently convey security data to target groups (Bauer et al., 2017).

Intentional compliance behavior by employees is complexly influenced by internal and external factors, including corporate culture, knowledge levels, and the important role of governance, risk management, and adequate incentives. Intentional compliance behavior by employees is known to be impacted by a number of elements, like as corporate culture, knowledge of information security, and sanctions (Wang, 2024). In this context, employee accountability is greatly influenced by user interaction and a culture of support inside the company. An inclusive culture and active employee involvement in information systems promote a better understanding of risk, which in turn encourages the development of a compliant attitude, a psychological mechanism that links organizational values to concrete compliant behavior. Personal characteristics like confidence and the impression of the reaction effectiveness, as well as more general organizational factors such as governance, risk management, and institutional context, often impact employee compliance. Because good governance procedures promote a culture of responsibility and compliance with rules, including for ISPs, it has been shown that governance in the banking industry greatly influences compliance behavior (Alrawhani et al., 2025). If information security policies are clearly stated and internal evaluation processes are well implemented, compliance may be slightly affected if there are no appropriate incentives, such as rewards (Wang et al., 2023). Therefore, managers of information security want a methodological framework to analyze and comprehend the various issues within their organizations. The aforementioned support will help them bridge the gap between information security policies and organizational work practices (Kolkowska et al., 2017).

Research on information security compliance still has crucial developmental limitations, particularly in formulating integrated behavior change mechanisms and examining cultural variations through identical comparative studies. Nevertheless, this research has developmental limitations that can be the focus of future research, one of which deserves special attention: the possibility of future studies using identical comparison strategies to explain how cultural variations shape and regulate compliance behavior towards ISPs (Alraja et al., 2023). This is crucial considering that previous studies have not attempted to formulate an integrated process that explains how information security behavior can change from non-compliance to compliance, thus necessitating an exploration of behavioral change mechanisms that integrate key behavioral theories and various factors that influence user actions in the information security context (Ali et al., 2021). Thus, future research needs to fill in and test the components of this framework through case studies that examine security culture across organizations with varying levels of security (Lim et al., 2009). With these limitations, this study makes an unprecedented contribution to the literature, given that there has been no previous research that explicitly examines the same variables in the context of developing a Security Policy compliance Culture in a business setting, and the ability to fill this knowledge gap is an important point that distinguishes and expands the scope of this study (Amankwa et al., 2018).

The gap phenomenon, which shows the contradiction between theoretical demands and the reality of security policy implementation, urges organizations to adopt behavior-centered solutions (Stafford et al., 2018). The banking sector, as a key industry in IS implementation, is highly vulnerable to security threats due to its reliance on sensitive financial data and complex operational systems (Alrawhani et al., 2025; Matkovskaya et al., 2022). The implementation of effective security protocols in banking institutions depends on technological readiness, institutional support , and external factors (Alrawhani et al., 2025; Al-Sharafi et al., 2018).

The issue of personal data confidentiality has become a major concern in the financial business in this digital age. As controllers of personal data, banks are required to ensure data security throughout the collection and processing of personal data. Implementing this obligation requires not only sophisticated technical tools such as encryption, but also a strong ethical and philosophical foundation through a Supportive Organizational Culture. This dedication to data protection is supported by inherent values such as amanah (trust) and maslahah (benefit), which serve as moral guidelines for consumer privacy. Building a collective attitude of compliance requires not only internal procedures but also user involvement through frequent socialization. Although research on security compliance is still developing, there is still a lack of studies that combine organizational culture, user involvement, and compliance attitudes as mediators, especially in the Islamic banking industry.This study aims to close this disparity by looking at the impact of these factors at the Cirebon Branch of

Bank BJB Syariah in order to improve information security governance based on behavior and ethical principles in addition to systems.

B. LITERATURE REVIEW

Theories of Organizational Behavior (JOHN B MINER, 1980)

Focusing on scientific theories because they can be tested through research projects. The ability to influence or manage the future is the third goal that unites understanding and prediction in applied disciplines such as organizational behavior. In fact, much scientific research is conducted with the specific intention of influencing the world to achieve certain goals. Applied science does achieve significant goals (JOHN B MINER, 1980). While systems theory explains that there is no single ideal way to manage an organization, but rather that strategies must be adapted to specific circumstances it highlights the importance of viewing organizations as entities consisting of interacting parts (Aditia Fradito et al., 2025). The systemic perspective develops a general theory of organizational behavior that views organizations as entities consisting of interconnected parts; each part interacts with and influences the another, which is in line with the idea that there is no universal management strategy but must be adapted to the context and dynamics of the organization (Glushchenko, 2022).

Supportive Organizational Culture

This variable is based on Organizational Support Theory, which was further created by Rhoades & Eisenberger (2002). According to this theory, employees develop the belief that the organization values their contributions and cares about their well-being. Employees perception of organizational support is perception of the support provided by the organization as a whole, including attention to welfare, fair treatment, recognition of achievements, and appreciation of contributions. This theory is rooted in Social Exchange Theory, which maintains that the connection between the organization and employees is based on the principle of reciprocity, whereby organizational support elicit loyalty and positive behavior from employees.

Organizational culture is very important for the behavior of individuals and natural resources within an organization or company (Adinda Putri et al., 2025) For example, research by Niza & Putra (2024) found that perceptions of organizational support have a significant effect on employee commitment and work motivation in the public sector. In fact, every organization has a unique organizational culture, companies need to implement this culture in operate efficiently and effectively (Siswondo et al., 2022). Another study by Sulistiyani et al (2022) confirms that POS not only increases work engagement, but also facilitates a balance between work and personal life through social exchange mechanisms.

Furthermore, this theory asserts that perceptions of organizational support are formed from individuals' experiences with fair organizational policies and treatment. In the context of information security, a strong sense of support will encourage staff members to abide by internal policies as a form of responsibility and sense of belonging to the organization. Thus, this theory is used to explain how Supportive Organizational Culture (X1) can influence Security Policy Compliance Culture (Y) through increased employee commitment and sense of responsibility in the context of public organizations and the service sector.

User Involvement

This variable is based on the Behavioral Theory of Information Systems Success as reinforced by Kappelman & McLean (1991). According to this theory, the success of an information system depends not only on its technical quality but also on the level of user involvement, both physical and psychological, in the process of developing and using the system. User involvement is the mental and emotional engagement of individuals with the system they use, fostering a sense of responsibility and ownership for its results.

For example, research by Astuti et al (2022), found that users who actively participated in system development activities tended to have a higher sense of responsibility and satisfaction with system performance. These findings are consistent with the view of Kappelman & McLean (1991), which states that user involvement is a psychological condition, not just a formal participatory action. In addition, (Irmawan & Azis Muslim, 2023) emphasized that many e-government studies use the IS Success model to evaluate the effectiveness of digital government systems, in which user participation is a major factor in determining the success of system implementation.

Furthermore, this theory asserts that User Involvement has a psychological influence on attitudes and conduct associated with adherence to information security policies. Thus, this theory explains how User Involvement (X2) can influence Security Policy compliance Culture (Y) by increasing understanding, responsibility, and a sense of ownership of the security systems used in public organizations and the digital government sector.

Security Policy Compliance Culture

The Y variable in this study is Security Policy Compliance Culture, which as a dependent variable influenced by organizational factors and individual behavior. The conceptual basis of this variable is derived from Protection Motivation Theory (PMT) developed by Rogers (1975) and refined by Maddux & Rogers (1983). This theory explains that a person's the inclination to adhere to security policies is impacted by two main components: assessment of threat and assessment of coping. Threat appraisal involves an individual's perception of the level of vulnerability and severity of the threat faced, while coping appraisal includes the ability to cope with threats through self-efficacy (self-confidence), response efficacy (belief that compliance is effective), and response cost (perception of the burden of compliance).

According to research by (Sulaiman et al., 2022), threat perception and threat coping ability play an important role in encouraging compliance with information security policies in the government sector. Similar research by (Haag et al., 2021) shows that Protection Motivation Theory (PMT) can be used to explain individual security behavior and provide a new direction for research in the field of organizational information security.

This theory is relevant to this study because it provides a conceptual framework for understanding how threat perception and risk coping abilities affect compliance with information security policies.Thus, this theory explains how Supportive Organizational Culture (X1) and User Involvement (X2) can influence Security Policy compliance Culture (Y) through a motivational process involving threat perception, self-efficacy, and compliance burden in the context of public organizations.

Compliance Attitude

Variable Z in this study is Compliance Attitude, which serves as a mediating variable explaining the relationship between Supportive Organizational Culture and Security Policy compliance. The theoretical basis for this variable refers to the Theory of Planned Behavior (TPB) proposed by Ajzen (1991). According to this theory, a person's behavior is determined by their behavioral intention, which is formed from three main constructs: attitude toward behavior, subjective norm (social influence), and perceived behavioral control. The Theory of Planned Behavior (TPB) explains that individuals with positive attitudes toward policies, supportive social norms, and confidence in their ability to comply with them will have a stronger intention to comply.

Research by (Sommestad et al., 2019) menemukan bahwa konstruk *Theory of Planned Behavior (TPB)* found that the Theory of Planned Behavior (TPB) construct significantly influences the intention to comply with information security policies in the government sector. Without strong discipline, it will be difficult to achieve the organization's goal of enforcing information security policies. Discipline reflects the attitudes, behaviors, and actions of employees that are consistent with organizational rules and policies, both written and unwritten (Wibowo et al., 2023). Similar outcomes were also reported by (Delso-Vicente et al., 2025), who confirmed that the main Perceived behavioral control, attitudes, and subjective standards all affect intentions to abide with workplace security measures. In addition, Lee et al (2023), showed that violations of psychological contracts in organizations can reduce intrinsic motivation, which has an adverse effect on Security Policy compliance Culture intentions.

Therefore, TPB theory explains how Compliance Attitude (Z) mediates the connection between Supportive Organizational Culture (X1) and Security Policy Compliance Culture (Y). Positive attitudes toward compliance will increase when organizations create a supportive and participative environment. This will strengthen the intention and behavior of compliance with information security policies.

Research Framework and Hypothesis Development

Considering an analysis of the literature and observed phenomena, this study develops a conceptual framework that links organizational and individual factors to the formation of a culture of safety compliance. This model's primary goal is to look at how individual attitudes can strengthen

relationships through mediation. Broadly speaking, the line of thinking behind this study can be described as follows:

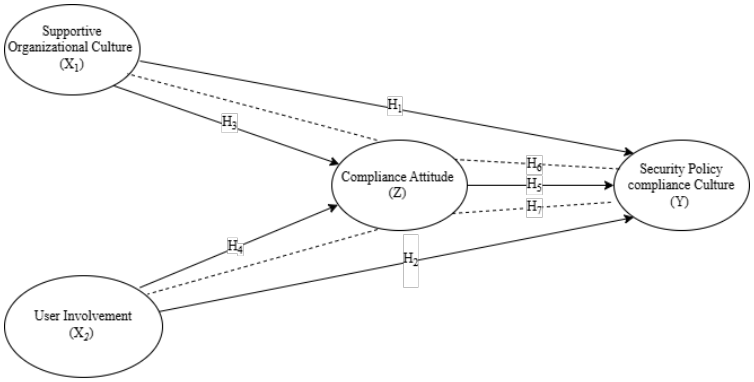


Figure 1. Conceptual Structure

Based on the visualization of the framework above, there are 7 main hypotheses to be tested:
H_1: Supportive Organizational Culture (X_1) influences Security Policy Compliance Culture (Y).
H_2: Supportive Organizational Culture (X_1) influences Security Policy Compliance Attitude (Z).
H_3: User Involvement (X_2) affects Security Policy Compliance Culture (Y).
H_4: User Involvement (X_2) affects Compliance Attitude (Z).
H_5: Compliance Attitude (Z) affects Security Policy Compliance Culture (Y).
H_6: Compliance Attitude (Z) mediates the relationship between Supportive Organizational Culture (X_1) and Security Policy Compliance Culture
H_7: Compliance Attitude (Z) mediates the relationship between User Involvement (X_2) and Security Policy Compliance Culture (Y).

C. METHODOLOGY OF RESEARCH

This study used an associative quantitative approach, as described by Sugiyono (2013), which aims to determine the connection between two or more factors. Respondents' opinions regarding the research variable indicators were measured using quantitative data in the form of numerical scores on a Likert scale from 1 to 5.

The population in this study comprised all 91 employees of the Bank BJB Cirebon Branch. All 91 employees were selected as respondents using the Total Sampling technique because the population was smaller than the 100-person limit. The core data came from an online survey administered via Google Forms, along with secondary data from internal organizational records, such as personnel data and general company information. According to Hair et al (2014),

For this investigation, the data were examined Using the partial least squares approach to structural equation modelling. This technique was chosen because it works well with very tiny sample sizes, which are not necessary normality, and can simultaneously study intricate causal connections between latent variables. To guarantee the reliability and validity of the research tool, the initial step was to evaluate the Measurement Model (External Model). This was done by using values for composite reliability (above 0.70) to verify Internal Consistency Reliability. Next, a Convergent Validity test was conducted by examining Outer Loadings (ideally > 0.70) and Average Variance Extracted, which must be > 0.50Discriminant Validity was ultimately evaluated utilising the Fornell-Larcker criterion or Cross Loading criteria in order to guarantee that every build was empirically distinct from the others.

To answer the hypothesis, the second step involves assessing the Structural Model (Internal Model). The main focus is on R2 (Coefficient of Determination) to estimate the model's predictive power. Researchers must also use the bootstrapping process to evaluate the significance of relationships through the Path Coefficient and t-value. In addition, testing is enhanced by examining the Q2 value to assess the prognostic utility of the model and the Effect Size (f2) to ensure the definite contribution of exogenous factors.

D. RESULT AND DISCUSSION

Result

The first test conducted in the measuring framework evaluation (outer model) was the convergent validity and indicator reliability test, which aimed to determine the extent to which indicators within a construct were strongly related to one another. In accordance with the criteria of Hair et al (2011),. the reliability of indicators is considered adequate if each indicator's loading is higher than 0.70. Convergent validity is also is considered to be met if For every build, the Ave Variance Extracted value exceeds 0.50.

Table 1. Validity and Reliability Test Results

Variable	Items	Outer Loading	Cronbach's Alpha	Composite Reliability	Avarage Variance Extracted (AVE)
Supportive Organizational Culture	SOC.1.2	0.849	0.753	0.859	0.670
	SOC.1.3	0.827			
	SOC.3.1	0.778			
User Involvement	UI.1.1	0.842	0.873	0.913	0.724
	UI.2.1	0.842			
	UI.3.1	0.869			
	UI.3.2	0.850			
Security Policy Compliance Culture	SPCC.1.2	0.863	0.795	0.880	0.711
	SPCC.2.1	0.901			
	SPCC.2.2	0.759			
Compliance Attitude	CA.1.1	0.703	0.844	0.889	0.617
	CA.2.1	0.781			
	CA.2.2	0.822			
	CA..3.1	0.831			
	CA.3.2	0.785			

Source : Processed Data from SmartPLS Version 4 (2025)

The test results in Table 1 demonstrate that the outer loading values of all indicators are greater than 0.70 AVE values ranging from 0.617 to 0.724. Thus, all indicators are considered reliable and meet the convergent validity requirements because they exceed the minimum threshold set.

Next is the Internal Consistency Reliability test using Cronbach's Alpha and Composite Reliability (CR). According to the criteria set by Hair et al (2011), composite reliability should be greater than 0.70 to be considered good; Values in the range of 0.60 to 0.70 are still appropriate for exploratory study. Both parameters are generally considered reliable if their values exceed 0.70.

As shown in Table 2, all research Cronbach's Alpha ratings for the constructs ranged from 0.753 to 0.873, indicating strong internal consistency and Composite Reliability values ranging from 0.859 to 0.913. Specifically, the User Involvement (X2) construct has the highest reliability, with a Composite Reliability of 0.913, which far exceeds the minimum required limit. These observations lead to the conclusion that all research instruments are reliable, and the data in this study are highly reliable for further inferential analysis. All constructs have met the strict reliability testing requirements in accordance with composite reliability criteria.

To guarantee that every build was empirically different from the other models, convergent validity and reliability were confirmed, and then a discriminant validity test was performed using the Fornell-Larcker criterion. Referring to the criteria of Hair et al (2011), The principle behind the assessment of discriminant validity was that the AVE value of each latent the build must exceed the highest correlation the square of that construct and other latent constructs. Technically, According to the Fornell-Larcker criterion, a latent construct is considered to be more correlated in conjunction with other latent constructs if the square root of its Average Variance Extracted value is higher in the structural mode, then the construct is discriminant valid.

Table 2. Fornell-Larcker Discriminant Validity

Variable	SOC	UI	SPCC	CA
Supportive Organizational Culture (X_1)	**0.818**			

User Involvement (X_2)	0.704	**0.851**		
Security Policy Compliance Culture (Y)	0.727	0.697	**0.843**	
Compliance Attitude (Z)	0.759	0.748	0.760	**0.786**

Source : Processed Data from SmartPLS Version 4 (2025)

Table 3 findings indicate that the AVE root values (diagonal entries) for Supportive Organizational Culture (0.818), User Involvement (0.851), Security Policy Compliance Culture (0.843), and Compliance Attitude (0.786) are all higher than the corresponding correlation values within the same column. These results prove that the with its own indicators, the variation shared by each concept is less than the variance shared by with other construct.

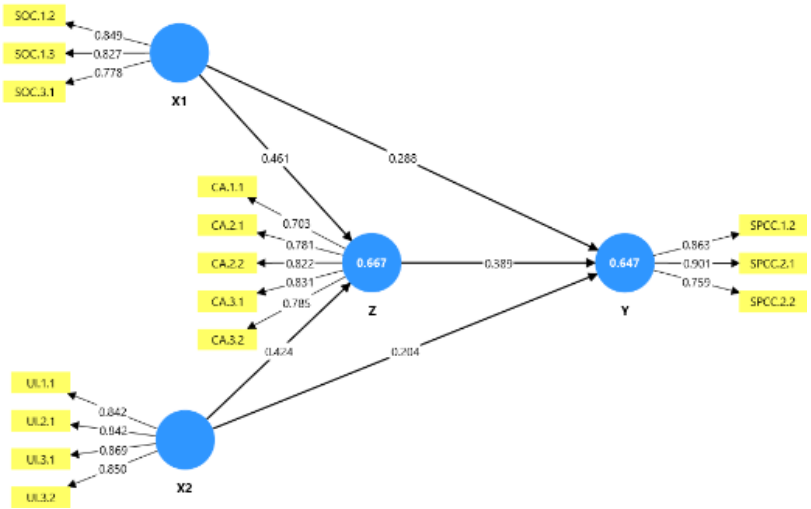
The final step in model evaluation is to use the Coefficient of Determination (R2) to evaluate the structural model (inner model). This value measures the extent to which exogeneous variables explain the variance of endogenous variables. As a basis for evaluation, Hair et al (2011) set criteria R2 In a structural model, endogenous latent variables with values of 0.75, 0.50, or 0.25 are deemed substantial, moderate, or weak, respectively.

Table 3. Coefficient of determination (R^2)

Variables	R Square
Security Policy compliance Culture (Y)	0.647
Compliance Attitude (Z)	0.667

Sumber : Data Olahan SmartPLS Versi 4 (2025)

Based on the results of data processing in Table 4, the Security Policy Compliance Culture (Y) variable has an R2 value of 0.647, indicating that the variable can be explained by the exogenous construct by 64.7%. Meanwhile, the Compliance Attitude (Z) variable has an R2value of 0.667, which indicates an explanation level of 66.7%. These values indicate that this research model has strong predictive power in explaining the phenomenon of security compliance under study. The structural model, referred to as the inner model, must next be assessed in order to verify the proposed connections between variables. This stage is carried out through a bootstrapping process in SmartPLS 4, with the results shown in Figure 2 for the Bootstrapping Test. The arrows in this model illustrate the structure of causality, where the numbers listed on each path determine whether the proposed hypothesis is accepted or rejected based on its statistical significance.



According to the hypothesis test results presentedin the table above, an evaluation concerning the link between the variables in the research model can be conducted by referring to the significance values (P values). If the p value for a connection is statistically significant, it is below of 0.05.

Table 5. Bootstrapping Test

Hypothesis	Direction Of Influence	Original Sample	T Statistic	P Values	Decision
H1	Supportive Organizational Culture (X_1) → Security Policy Compliance Culture (Y)	0.288	2.672	0.008	Accepted
H2	Supportive Organizational Culture (X_1) → Compliance Attitude (Z)	0.461	4.853	0.000	Accepted
H3	User Involvement (X_2)→ Security Policy Compliance Culture (Y)	0.204	2.247	0.025	Accepted
H4	User Involvement (X_2) → Compliance Attitude (Z)	0.424	3.966	0.000	Accepted
H5	Compliance Attitude (Z) → Security Policy Compliance Culture (Y)	0.389	3.019	0.003	Accepted
H6	Supportive Organizational Culture (X_1) → Compliance Attitude (Z) → Security Policy Compliance Culture (Y)	0.179	2.371	0. 018	Accepted
H7	User Involvement (X_2)→ Compliance Attitude (Z) → Security Policy Compliance Culture (Y)	0.165	2.344	0. 019	Accepted

The outcomes of hypothesis testing with the bootstrap technique suggest that all direct effect hypotheses (H1-H5) are supported, with positive relationships. In detail, Supportive Organizational Culture (X1) was determined to exert a substantial influence on Security Policy Compliance Culture (Y) with a coefficient of 0.288 (T=2.672; P=0.008) and on Compliance Attitude (Z) with a coefficient of 0.461 (T=4.853; P=0.000). Similarly, the User Involvement (X2) variable had a significant effect on Security Policy Compliance Culture (Y) of 0.204 (T=2.247; P=0.025) and on Compliance Attitude (Z) of 0.424 (T=3.966; P=0.000). Furthermore, Compliance Attitude (Z) as a mediating variable has a strong influence on Security Policy Compliance Culture (Y) with a coefficient of 0.389 and a significance of 0.003.

Meanwhile, in the indirect effect test, the Compliance Attitude variable (Z) was found to mediate significantly (H6 and H7 accepted). This is indicated by the relationship path of Supportive Organizational Culture (X1) to Security Policy Compliance Culture (Y) through Compliance Attitude (Z) with a significance value of 0.018 (T=2.371), as well as the path of User Involvement (X2) to Security Policy Compliance Culture (Y) through the same mediating variable with a significance value of 0.019 (T=2.344). These findings confirm that organizational culture and user involvement factors not only have a direct impact but are also significantly reinforced through the formation of individual compliance attitudes in efforts to build a sustainable security policy compliance culture.

Discuisson

The Influence of Supportive Organizational Culture (X1) on Security Policy Compliance Culture (Y)

According to the outcomes of hypothesis testing, this study proves that organizational culture has a significant effect on information security compliance culture, with a significance value of 0.008. This finding indicates the beliefs, norms, and work methods that develop within an organization play a strategic role in shaping employee compkience behavior. A work environment that provides tangible support for information security, whether through leadership commitment, clear policies, or exemplary behavior, can encourage employee to consistently comply with security policies. Theoretically, this finding is consistent with the view that organizational culture is the main foundation for building a culture of information security.

These results align with the view of Solomon & Brown (2020), who state The organisational culture significantly impacts the information security culture In addition, the findings of Ejigu et al

(2024) reinforce those of studies showing that organizational culture significantly affects employee compliance levels.

The Influence of Supportive Organizational Culture (X1) on Compliance Attitude (Z)

The test results indicate that organizational culture has a highly significant impact on employee attitudes, with a p-value of 0.000. This finding confirms that a supportive work environment can shape individuals' perspectives and beliefs regardings the importance of information security compliance. Employees who feel organizational support tend to develop positive attitudes toward security policies because they view them as a collective effort to protect the organization rather than an additional burden.

This is in the with the findings of Parsons et al (2015), the association between supportive organisational culture and attitudes toward compliance is statistically significant. Furthermore, Amankwa et al (2018) state that when employee attitudes toward compliance are improved through culture building, the risk to organizational information assets and data will ultimately be reduced.

The Influence of User Involvement (X2) on Security Policy Compliance Culture (Y)

The Hypothesis test findings indicate that user interaction exerts a considerable influence on information security compliance, with a p-value of 0.025. Active employee involvement in the use, development, and socialization of information systems fosters a sense of responsibility and ownership for the systems. When employees feel involved, security policies are no longer perceived as rules that hinder work, but rather as part of a safe and efficient work process. These findings indicate that a participatory approach is more effective than a top-down approach. In Islamic banking practices, user involvement also reflects the principles of deliberation and participation, which with Islamic values in organizational decision-making.

The findings of this study align with the conclusions AlKalbani et al (2015), understanding employee behavior through the involvement process significantly increases compliance in organizations. In line with this, Vahlevy et al (2023) emphasize that involving users in the advancement of accounting information systems ensures that the systems are user-friendly and fulfil user requirements, which provides a basis for management to assess internal control compliance with standard operating procedures.

The Influence of User Involvement (X2) on Compliance Attitude (Z)

Hypothesis testing shows the aforementioned user involved has a highly significant effect on employee attitudes, p-value of 0.000. Employees involved in security systems and policies tend to have a better understanding and a more positive attitude toward the applicable rules. Participation in policy development fosters transparency and trust. From a behavioral perspective, these findings indicate that compliance attitudes are shaped not only by knowledge but also by participatory experiences.

The findings of this study align with the conclusions of Amankwa et al (2018), end-user involvement significantly influences their attitudes toward security policy compliance. It also reinforces the research by And & Mirza (2014), which states that user involvement in the information security decision-making process is very important for increasing employee ownership of existing policies.

The Influence of Compliance Attitude (Z) on Security Policy Compliance Culture (Y)

According to the outcomes of the statistical tests, employee attitudes were found to have a significant effect on information security compliance (p=0.003). This finding confirms that compliant behavior reflects an individual's internal beliefs and attitudes. Employees exhibiting favourable views towards information security are inclined to exhibit consistent compliance, even in situations with minimal supervision. This reinforces the argument that the success of information security policies depends not only on written rules and sanctions, but also on the psychological readiness of individuals.

The findings of this study align with the conclusions of Amankwa et al (2018), who demonstrate that attitudes toward ISP compliance significantly influence an organization's overall compliance culture. This is also in line with research by (D'Arcy & Greene, 2014), they discovered a strong and significant causal association between information security consciousness and actual compliance levels.

The Influence of Supportive Organizational Culture (X1) on Security Policy Compliance Culture (Y) through Compliance Attitude (Z)

Based on the outcomes of the mediation test, this Research demonstrates that organisational culture significantly influences information security compliance through the mediation of employee attitudes with a significance value of 0.018. This finding explains that the influence of organizational culture on compliance behavior does but requires a process of internalization within each individual first. A supportive work environment will shape employees' positive perspectives and beliefs about the importance of security values. It is these attitudes or mental dispositions that then become a natural driver for employees to implement every security policy with full awareness and consistency, not merely out of formal compliance with organizational coercion.

The results of this investigation are consistent with the conclusions of Solomon & Brown (2020b), who argue that the effects of attitudes, normative beliefs, self-efficacy is essential components in encouraging compliance with security policies. In addition, research by Kim et al (2014), supports this hypothesis by emphasizing that this approach is very appropriate for explaining the phenomenon of attitudes toward information security. This confirms that the more positive the attitudes of organization members toward existing rules, the higher their intention and commitment to comply with information security policies.

The Influence of User Involvement (X2) on **Security Policy Compliance Culture (Y) through Compliance Attitude (Z)**

Based on the outcomes of the mediation hypothesis test, it was found that user involvement has a significant effect on information security compliance mediated by employee attitudes with a significance value of 0.019. These results indicated that user involvement in operational processes and system development does not automatically create compliance; it must first address the psychological side or perspective of employees. When users are actively involved, they feel appreciated and gain a deeper understanding of the policy's urgency, which in turn shapes a positive attitude. It is this proactive attitude that ultimately becomes a strong driver of employees' consistent adherence to the information security policies of the company.

These findigs are in line with research consucated by Da Silva (2013), who contends that consumers must participate through a number of routes in the information security decision-making process to enhance their understanding and feeling of ownership exiting policies. This involvement is crucial in building a mental disposition that supports security. In (Ochieng Otieno, Mwaura, et al (2021), in their researchemphasized that individual attitude emerged as the second most influential parameter after direct relationships with the culture of information security compliance culture. These results indicate that perceptions the simplicity of comprehension policies (ISP) through engagement are an important factor that strengthens the correlation between attitudes and actual employee behaviour compliance.

E. CONCLUSION

The findings of this study indicate that the development of a security policy compliance culture at Bank BJB Syariah's Cirebon branch is greatly influenced by the synergy between organizational factors and employee psychological factors. Empirically, a supportive organizational culture and user involeent have been shown to have a favourable, significant impact on security policy compliance culture. This findings indicate that compliance is not solely determined by the presence of formal policies and security technology, but rather depends heavily on a supportive work environment and the level of active employee participation in the system. Along with direct influence, This study supports the vital role of compliance attitudeas a ediating variable. Compliance attitude has been shown to strengthen the impact of corporate culture and user involvement in data protection compliance. This indicates that sustainable compliance behavior is formed through a process of internalizing individual values, beliefs, and awareness, rather than simply as a result of structural pressure or organizational supervision. Thus, an approach that focuses on shaping employees' internal attitudes and awareness is more effective than one that emphasizes only regulatory aspects and sanctions. In the context of Islamic banking, these findings have implications for the principles of trust and moral responsibility in customer data management. The implementation of a supportive, participatory organizational culture aligns with Islamic values that emphasize trust, justice, and benefit. Therefore, Islamic banking management is advised to integrate information security policies into everyday organizational values, increase employee involvement in decision-making related to information systems, and develop educational programs to foster a sustainable culture of compliance.

F. REFERENCES

Adinda Putri, A., Salsabila Nur, M., Nasrudin Wibowo, S., Swadaya Gunung Jati, U., Author, C., Artikel, R., & Kunci, K. (2025). PENGARUH BUDAYA ORGANISASI DAN MOTIVASI INTRINSIK TERHADAP KETERIKATAN SURVEI PADA MAHASISWA KOMUNITAS GENBI CIREBON. https://journal.stiem.ac.id/index.php/jureq

Aditia Fradito, Ferunika, Subandi, Deden Makbuloh, & Encep Syarifudin. (2025). DAMPAK TEORI ORGANISASI SISTEM DAN KONTINGENSI TERHADAP SISTEM MANAJEMEN DAN KEPEMIMPINAN.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. In Applied Sciences (Switzerland) (Vol. 11, Number 8). MDPI AG. https://doi.org/10.3390/app11083383

AlKalbani, A., Deng, H., & Kam, B. (2015). Australasian Conference on Information Systems Investigating the Role of Socio-organizational Factors in the Information Security Compliance in Organizations.

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security Compliance in Organizations: An Institutional Perspective. Data and Information Management, 1(2), 104–114. https://doi.org/10.1515/dim-2017-0006

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. Computers and Security, 129. https://doi.org/10.1016/j.cose.2023.103208

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. Journal of Open Innovation: Technology, Market, and Complexity, 11(1). https://doi.org/10.1016/j.joitmc.2024.100463

Al-Sharafi, M. A., Arshah, R. A., Alajmi, Q., Herzallah, F. A., & Qasem, Y. A. M. (2018). The Influence of Trust in Consumer Perception to Accept Internet Banking Services: An Empirical Evidence. Indian Journal of Science and Technology, 11(20), 1–9. https://doi.org/10.17485/ijst/2018/v11i20/91928

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. Information and Computer Security, 26(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063
Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. Information and Computer Security, 26(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. Information and Computer Security, 26(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. Information and Computer Security, 26(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063
And, A. A., & Mirza, D. A. (2014). A FRAMEWORK OF INFORMATION SECURITY CULTURE CHANGE. Journal of Theoretical and Applied Information Technology, 20(2). www.jatit.org

Astuti, F., Nusron, L. A., & Khamainy, A. H. (2022). Can user involvement, training and internal control improve information system performance? Journal of Business and Information Systems (e-ISSN: 2685-2543), 4(1), 42–53. https://doi.org/10.36067/jbis.v4i1.124

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers and Security, 68, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Da Silva, F. Q. B. . (2013). Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering. ACM.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management and Computer Security, 22(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal, 11(1). https://doi.org/10.1186/s43093-025-00452-7

Ejigu, K., Siponen, M., & Muluneh, T. (2024). Impact of Organizational Culture on Information Security Policy Compliance. SINET: Ethiopian Journal of Science, 47(1), 17–32. https://doi.org/10.4314/sinet.v47i1.2

Glushchenko, V. V. (2022). A General Theory of Organizational Behavior: An Educational Perspective. https://doi.org/10.17509/xxxx.xxx

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. Data Base for Advances in Information Systems, 52(2), 25–67. https://doi.org/10.1145/3462766.3462770

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. Journal of Marketing Theory and Practice, 19(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. In European Business Review (Vol. 26, Number 2, pp. 106–121). Emerald Group Publishing Ltd. https://doi.org/10.1108/EBR-10-2013-0128

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Irmawan, I., & Azis Muslim, M. (2023). Literature review of information system success models in e-government evaluation. In IJOBSOR (Vol. 11, Number 1). www.ijobsor.pelnus.ac.id

JOHN B MINER. (1980). Theories of organizational behavior.

Kappelman, & McLean. (1991). Promoting Information System Success : The Respective Roles of User Participatiom and User Involvement.

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. Information and Computer Security, 30(3), 382–401. https://doi.org/10.1108/ICS-06-2021-0073

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. Scientific World Journal, 2014. https://doi.org/10.1155/2014/463870

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. Journal of Strategic Information Systems, 26(1), 39–57. https://doi.org/10.1016/j.jsis.2016.08.005

Lee, D., Lallie, H. S., & Michaelides, N. (2023). The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation. http://arxiv.org/abs/2307.02916

Lim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. https://www.researchgate.net/publication/49282874

Matkovskaya, Y. S., Vechkinzova, E., & Biryukov, V. (2022). Banking Ecosystems: Identification Latent Innovation Opportunities Increasing Their Long-Term Competitiveness Based on a Model the Technological Increment. Journal of Open Innovation: Technology, Market, and Complexity, 8(3). https://doi.org/10.3390/joitmc8030143

Niza, U., & Putra, M. S. (2024). PENGARUH PERCEIVED ORGANIZATIONAL SUPPORT DAN EMPLOYEE ENGAGEMENT TERHADAP EMPLOYEE WELL-BEING. E-Jurnal Manajemen Universitas Udayana, 13(8), 1292. https://doi.org/10.24843/EJMUNUD.2024.v13.i08.p04

Ochieng Otieno, E., Mwaura, A. M., & Wausi, A. N. (2021). THE UNIVERSITY OF NAIROBI SCHOOL OF COMPUTING AND INFORMATICS THE IMPACT OF ORGANIZATIONAL CULTURE ON INFORMATION SECURITY COMPLIANCE CULTURE: A CASE OF KENYAN UNIVERSITIES.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. Journal of Cognitive Engineering and Decision Making, 9(2), 117–129. https://doi.org/10.1177/1555343415575152

Rhoades, L., & Eisenberger, R. (2002). Perceived organizational support: A review of the literature. Journal of Applied Psychology, 87(4), 698–714. https://doi.org/10.1037/0021-9010.87.4.698

Siswondo, S., Sudrajat, D., Solahudin, A., & Wibowo, S. N. (2022). The Influence of Organizational Culture and Organizational Commitment on OCB (Organizational Citizenship Behavior) Employees. Daengku: Journal of Humanities and Social Sciences Innovation, 2(5), 741–748. https://doi.org/10.35877/454ri.daengku1277

Solomon, G., & Brown, I. (2020a). The influence of organisational culture and information security culture on employee compliance behaviour. Journal of Enterprise Information Management, 34(4), 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217

Solomon, G., & Brown, I. (2020b). The influence of organisational culture and information security culture on employee compliance behaviour. Journal of Enterprise Information Management, 34(4), 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The Theory of Planned Behavior and Information Security Policy Compliance. Journal of Computer Information Systems, 59(4), 344–353. https://doi.org/10.1080/08874417.2017.1368421

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, 33(4), 410–424. https://doi.org/10.1108/MAJ-07-2017-1596

Sugiyono. (2013). METODE PENELITIAN KUANTITATIF KUALITATIF DAN R&D.

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. In Social Sciences (Vol. 11, Number 9). MDPI. https://doi.org/10.3390/socsci11090386

Sulistiyani, E., Ardhi Hidayat, Y., & Setiawan, A. (2022). 33 15 (2) (2022) 133-143 Perceived organizational support, employee work engagement and work life balance: Social exchange theory perspective.

Vahlevy, M. R., Noormansyah, I., & Lovita, E. (2023). Utilizing Organizational Culture to Form User Compliance through Systems Development. International Journal of Religious and Cultural Studies, 5(1). https://doi.org/10.34199/ijracs.2023.04.07

Wang, X. (2024). Simulation of the role of emphasis on scheduling in the optimal incentive scheme for marine engineering employee's routine job and information security compliance. Journal of Ocean Engineering and Science, 9(1), 1–8. https://doi.org/10.1016/j.joes.2022.05.024

Wang, X., Wang, Changlin, Sun, Z., & Wang, Chunhui. (2023). An optimal coupling incentive mechanism concerning insider's compliance behavior towards marine information security policy. Journal of Ocean Engineering and Science, 8(5), 573–575. https://doi.org/10.1016/j.joes.2022.05.023

Wibowo, S. N., Solahudin, A., Haryanto, E., Widawati, Y., & Haryanto, B. E. (2023). The Effect of Reward and Punishment on Work Discipline. In Research Trend in Management and Technology (Vol. 1, Number 1).