JLHR: Journal of Law and Humanities Review
P-ISSN: : XXXX-XXXX
E-ISSN : 3110-245X
GREENATION PUBLISHER
+62 812-1046-7572 https://greenationpublisher.org/JLHR greenation.info@gmail.com
DOI: https://doi.org/10.38035/jlhr.v1i2

Religiosity as an Ethical Infrastructure for Preventing Fraud in Digital Business: Integrating Interfaith, Legal, and Forensic Accounting Perspectives

Robertus Suraji[1], Lintang Putri Estiarto[2], Istianingsih Sastrodiharjo[3]
[1]Faculty of Computer Science, Universitas Bhayangkara Jakarta Raya, Indonesia; email: robertus.suraji@dsn.ubharajaya.ac.id
[2]Digital Business Study Program, Universitas Terbuka, Indonesia; email: lintangputri@ecampus.ut.ac.id
[3]Faculty of Economics and Business, Universitas Bhayangkara Jakarta Raya, Indonesia; email: istianingsih@dsn.ubharajaya.ac.id

Corresponding Author: robertus.suraji@dsn.ubharajaya.ac.id[1]

Abstract: Digital business expands access and efficiency while simultaneously creating new opportunities for fraud through platform opacity, automated decisions, data asymmetry, and cross-border transactions. Existing studies commonly examine religiosity, legal compliance, digital governance, and forensic accounting separately, leaving their complementary relationship underdeveloped. This article aims to formulate an inclusive ethical governance model that positions religiosity as an internal moral infrastructure and combines it with law, organizational controls, and digital forensic accounting. An integrative literature review and normative juridical analysis were applied to recent scholarly works, professional standards, and Indonesian regulations, supported by foundational behavioral theories. The synthesis shows that intrinsic and inclusive religiosity can strengthen moral awareness and inhibit fraud rationalization, but symbolic religiosity cannot substitute for enforceable controls. Effective prevention requires the simultaneous operation of value internalization, accountable digital governance, privacy-respecting analytics, protected reporting channels, and evidence-preserving investigation procedures. The article proposes the Religious Integrity–Forensic Accounting in Digital Ecosystems model, which links moral prevention, structural constraint, technological detection, and corrective response. Its novelty lies in treating religiosity neither as a ceremonial variable nor a stand-alone control, but as one component of a pluralistic, rights-based, and auditable anti-fraud architecture.

Keywords: religiosity; digital business; forensic accounting; fraud prevention; law

INTRODUCTION

Digital transformation has changed how organizations form contracts, process payments, manage identities, preserve evidence, and make decisions. Although these changes increase the speed and scale of business, they also broaden the fraud risk surface. Identity manipulation, social engineering, account takeover, data misuse, concealed related-party transactions, and the

falsification of electronic evidence can occur across organizational units and jurisdictions. The Association of Certified Fraud Examiners reports that occupational fraud continues to cause material organizational losses and is frequently uncovered through reports or tips rather than routine audits alone (ACFE, 2024). In digital environments, the issue is not merely whether controls exist, but whether automated decisions, data trails, access rights, and human accountability can be meaningfully examined.

Recent studies emphasize the dual nature of technology. Data analytics, artificial intelligence, machine learning, blockchain, and continuous auditing can identify anomalies at a scale unattainable through manual procedures. At the same time, these technologies may increase the speed, anonymity, complexity, and replicability of fraud. Tiron-Tudor et al. (2025) conclude that the accounting profession must combine digital competence, professional skepticism, governance, and investigative capability. Pianoschi and Mierlita (2025) likewise demonstrate the interdependence among technology, stakeholder interests, and the evolution of auditing standards. Consequently, digital fraud prevention cannot be reduced to the procurement of detection software.

A further weakness lies in the assumption that formal compliance is always equivalent to ethical conduct. Law establishes minimum boundaries, procedures, authority, rights, and sanctions; however, day-to-day decisions often occur within areas of discretion that are not yet, or not fully, governed by rules. Professional codes of ethics also require judgment in complex situations. Technology-related revisions to the IESBA Code reinforce integrity, objectivity, professional competence and due care, confidentiality, and professional behavior when accountants use technology (IESBA, 2023, 2024). ISA 240 (Revised) strengthens the fraud lens in auditors' risk assessment and responses while emphasizing the need for greater transparency (IAASB, 2025). These developments demonstrate that technology does not eliminate the moral dimension; instead, it amplifies the consequences of flawed moral judgment.

In this context, religiosity is relevant as a source of moral orientation, meaning, self-control, and accountability beyond external supervision. Research on accounting practices indicates that religiosity can strengthen the relationship between ethical accounting judgments and financial reporting quality (Koufie et al., 2025). Research in Indonesia also reveals a negative association between Islamic religiosity and the propensity for asset misappropriation, although pressure, opportunity, rationalization, and capability remain influential (Darsono et al., 2024). At the cross-national organizational level, cultural-religious values are associated with small multinational corporations' decisions to use audited financial statements (Kontesa et al., 2024). These findings provide an empirical basis for incorporating religiosity into fraud-prevention architecture.

Nevertheless, religiosity should not be treated naively. Declarative religious identity differs from internalized intrinsic religiosity. An extrinsic orientation may use religion as a means of status, legitimacy, or social acceptance, whereas an intrinsic orientation treats religious values as a way of life (Allport & Ross, 1967). Even individuals who actively engage in religious rituals may rationalize misconduct, yield to pressure, or abuse power. Weaver and Agle (2002) explain that religious identity influences ethical behavior through role formation, but the strength of its influence depends on its salience within self-identity. This article therefore does not propose religion as a substitute for law or internal controls.

Indonesia provides a distinctive normative context. Belief in the One and Only God is placed alongside humanity, unity, democracy, and social justice within Pancasila. Accordingly, religiosity in organizational governance must be translated inclusively, without discrimination, and with respect for freedom of religion or belief. In the digital domain, Law Number 27 of 2022 on Personal Data Protection requires lawful grounds for data processing and safeguards the rights of data subjects. The Electronic Information and Transactions Law and its amendments provide a framework for electronic information, documents, and transactions. In

the financial services sector, Financial Services Authority Regulation Number 12 of 2024 establishes an anti-fraud strategy encompassing prevention; detection; investigation, reporting, and sanctions; and monitoring, evaluation, and follow-up (OJK, 2024). Religious values used to prevent fraud must therefore operate within—not outside—the rule of law and the protection of rights.

A research gap arises because four streams of literature—religiosity and ethics, digital law, anti-fraud governance, and forensic accounting—more often develop independently. Religiosity studies frequently test correlations with individual behavior but have not sufficiently translated these findings into digital control design. Forensic accounting research emphasizes analytics and evidence but risks overlooking motivation, rationalization, and culture. Legal scholarship establishes certainty regarding rights and obligations, yet formal compliance does not necessarily foster moral awareness. Meanwhile, digital governance often prioritizes system efficiency without examining who is accountable when algorithms, data, and human decisions become intertwined.

This article aims to: first, explain the mechanisms through which religiosity can contribute to preventing fraud in digital business; second, determine normative boundaries so that the use of religiosity does not become symbolism, discrimination, or a substitute for controls; and third, formulate an integrative model connecting religiosity, law, governance, and digital forensic accounting. It addresses three research questions: (1) How does intrinsic religiosity influence moral awareness and the rationalization of fraud in digital business? (2) How do law, organizational controls, and forensic accounting compensate for the limitations of religiosity? and (3) What constitutes an ethical, pluralistic, and auditable fraud-prevention architecture?

METHOD

This study adopts a qualitative approach combining an integrative literature review with normative juridical analysis. An integrative review was selected because the research questions require the synthesis of ideas across religious and ethical studies, law, organizational behavior, forensic accounting, auditing, and digital business, rather than the estimation of a single effect size. Normative juridical analysis was used to assess the conceptual model's alignment with the rule of law, personal data protection, accountability for electronic transactions, and anti-fraud strategy.

The materials examined include peer-reviewed scholarly articles, professional standards, reports issued by professional organizations, and laws and regulations. Recent literature published from 2021 to July 2026 was prioritized to capture developments in digital fraud and auditing, while seminal works were used selectively to ground the concepts of intrinsic-extrinsic religiosity, planned behavior, rationalization, and fraud theory. The search focused on combinations of the keywords religiosity, religious ethics, fraud prevention, forensic accounting, digital fraud, digital business, ethical accounting, audit technology, data protection, and anti-fraud governance. Sources were included when they directly explained ethical mechanisms, fraud risk factors, controls, detection technologies, professional standards, or relevant legal obligations.

The analysis proceeded in four stages. First, each source was examined to identify units of meaning related to moral prevention, pressure and rationalization, opportunity and capability, formal controls, digital detection, rights protection, and investigative response. Second, these units were compared to identify reinforcing relationships and contradictions. Third, the findings were organized into individual, organizational, technological, and legal layers. Fourth, the relationships across layers were synthesized into the Religious Integrity–Forensic Accounting in Digital Ecosystems (RIFAD) Model. Argumentative validity was maintained through triangulation among empirical findings, theory, professional standards, and regulations; causal claims were avoided where the available evidence was merely associational.

The object of analysis is neither a particular religion nor a particular religious community, but religiosity as the internalization of transcendent values that promote honesty, justice, responsibility, concern for victims, and self-control. This interfaith approach was deliberately adopted to enable application in pluralistic organizations. The model's success is not assessed by the intensity of symbols or rituals, but by observable conduct: explainable decisions, reduced conflicts of interest, whistleblower protection, evidence preservation, loss remediation, and accountability for digital systems.

RESULTS AND DISCUSSION

Religiosity as Moral Infrastructure, Not a Stand-Alone Control

The literature synthesis indicates that religiosity contributes most strongly before misconduct occurs by shaping how individuals recognize moral issues, evaluate consequences for others, and restrain the impulse to obtain illegitimate benefits. Under the theory of planned behavior, intention is influenced by attitudes, subjective norms, and perceived behavioral control (Ajzen, 1991). Internalized religiosity can operate through all three by fostering negative attitudes toward dishonesty, sustaining a moral community that rejects abuse, and strengthening self-control. Koufie et al. (2025) support the role of religiosity in strengthening the relationship between ethical accounting practices and financial reporting quality. Recent Indonesian evidence also shows that stronger organizational integrity is associated with higher financial reporting quality, reflected in cleaner audit opinions and fewer audit findings (Wibowo et al., 2026).

Within fraud theory, religiosity primarily constrains rationalization, although its influence may extend to responses to pressure and the use of capability. Cressey (1953) identifies pressure, opportunity, and rationalization as elements of fraud, while Wolfe and Hermanson (2004) add capability. Individuals may know that a particular act is wrong yet frame it as a temporary loan, compensation for injustice, an instruction from a superior, or a customary practice. Intrinsic religious values provide a moral vocabulary for dismantling such justifications and making victims' interests a substantive consideration. Darsono et al.'s (2024) finding of a negative relationship between religiosity and asset misappropriation is consistent with this mechanism.

Clear limitations nevertheless remain. Religiosity does not remove opportunities arising from weak segregation of duties, excessive access rights, fictitious vendors, or opaque algorithmic models. Nor does religiosity automatically produce admissible evidence. When leaders invoke religious language while offering incentives that encourage manipulation, moral licensing may occur: an image of virtue is used to reduce guilt. Accordingly, measuring organizational religiosity through the number of religious events, attire, slogans, or rituals constitutes a weak and potentially discriminatory proxy.

An interfaith approach shifts attention from uniformity of belief toward shared ethical principles: honesty, trustworthiness, the prohibition against taking others' rights, justice, compassion, accountability, and remediation of harm. These common principles are compatible with professional ethics and human rights. Organizations need not assess employees' personal faith; they should assess whether their systems and workplace conduct embody integrity. Religiosity thus serves as a voluntary source of internal motivation, while standards of conduct remain expressed in professional, universal, and verifiable terms.

Table 1. Synthesis of the Roles and Limitations of Religiosity in Fraud Prevention

Dimension	Potential Contribution	Risk of Misapplication	Required Safeguard
Moral awareness	Recognizes victims, conflicts of interest, and dishonesty.	Ethics remains merely rhetorical.	Realistic dilemmas, decision reflection, and exemplary leadership.
Rationalization	Rejects justifications that fraud is a loan, customary practice, or instruction.	Moral licensing after symbolic activities.	Documentation of decision rationales and independent review.
Self-control	Restrains opportunistic conduct when oversight is limited.	Blames individuals while ignoring system design.	Segregation of duties, least privilege, rotation, and mandatory leave.
Moral community	Fosters norms of mutual accountability and the courage to report.	Conformity, exclusivity, or concealment of misconduct by influential figures.	Independent channels, anti-retaliation safeguards, and minority protection.
Remediation	Encourages acknowledgment, restitution, and correction.	Forgiveness replaces legal process.	Victim remediation alongside investigation and proportionate sanctions.

Source: Authors' synthesis based on Allport and Ross (1967), Weaver and Agle (2002), Darsono et al. (2024), and Koufie et al. (2025).

Characteristics of Fraud in Digital Business Ecosystems

Digital fraud differs from conventional fraud in scale, speed, distance, and dependence on data infrastructure. A single stolen credential can be used for thousands of transactions; a single biased decision model can harm a large group; and manipulated logs can erase traces required by investigators. Transactions are also distributed across cloud providers, payment gateways, platforms, analytics vendors, and user devices. Consequently, organizational and evidentiary boundaries become blurred.

Pianoschi and Mierlita (2025) demonstrate that fraud, technology, standards, and stakeholder interests mutually shape one another. This sociomaterial perspective is important: algorithms are not independent moral actors; their design reflects human choices concerning data, risk thresholds, incentives, and accountability. In turn, systems constrain or expand human action. If growth targets pressure teams to disregard alerts, even sophisticated fraud analytics may become ornamental. If administrator access is not logged, personal honesty alone cannot reconstruct evidence.

Digital forensic accounting integrates knowledge of transactions, financial patterns, evidentiary procedures, and technology. Its value extends beyond identifying unusual figures to reconstructing who did what, when, under what authority, through which system, and for whose benefit. Tiron-Tudor et al. (2025) emphasize that the accounting profession must develop analytical and investigative capabilities and collaborate with technology and legal specialists. Ul Hassan et al. (2025) find that governance, information technology techniques, and internal controls are perceived as playing important roles in fraud detection and prevention.

Detection technology must nevertheless be constrained by law and ethics. Collecting all employee data without a clear purpose may infringe privacy and create excessive surveillance. Unexplainable models may generate false allegations. The Personal Data Protection Law

requires a lawful basis and purpose for processing, accuracy, security, and respect for data-subject rights (Republic of Indonesia, 2022). The OECD principles on artificial intelligence likewise emphasize transparency, traceability, safety, human oversight, and accountability throughout the system life cycle (OECD, 2024). Legitimate fraud analytics must therefore be proportionate, documented, tested for bias, and subject to meaningful human accountability.

Table 2. Digital Fraud Risks and Integrative Responses

Risk	Primary Weakness	Governance/Legal Control	Digital Forensic Response	Role of Values
Account takeover	Weak identity and authentication	Multi-factor authentication, restricted access, notifications	Analysis of devices, IP addresses, timestamps, and transaction patterns	Prohibition against abusing trust and identity
Transaction manipulation	Weak segregation of duties and authorization	Dual control, limits, independent reconciliation	Benford/anomaly tests, graph analytics, fund-flow tracing	Trustworthiness and honesty in recordkeeping
Data misuse	Excessive access and unclear purpose	Lawful basis, least privilege, limited retention	Access logs, DLP, preservation, and chain of custody	Respect for dignity and privacy
Vendor/platform collusion	Concealed beneficial ownership	Due diligence, conflict declarations, beneficial-ownership checks	Network analysis and matching of accounts, addresses, and devices	Justice and rejection of conflicts of interest
Algorithm manipulation	Opaque models and biased incentives	Model governance, human oversight, audit trail	Versioning, reproducibility, bias and drift testing	Responsibility for impacts on people

Source: Authors' synthesis based on IESBA (2023, 2025), OECD (2024), Pianoschi and Mierlita (2025), and Tiron-Tudor et al. (2025).

Law as a Boundary, a Safeguard of Rights, and an Accountability Infrastructure

Law performs three functions within the prevention model. First, it defines behavioral boundaries and consequences. Second, it safeguards the rights of data subjects, accused persons, whistleblowers, consumers, and other stakeholders. Third, it provides the evidentiary and authority framework required for investigations. Together, these functions prevent moral values from being applied arbitrarily.

In electronic systems, evidentiary validity depends on process integrity. Organizations must ensure that logs cannot be readily altered, clocks are synchronized, access is recorded, data provenance is traceable, and evidence transfers are documented. The chain of custody must be preserved from identification, preservation, acquisition, and analysis through presentation. If these processes are neglected, analytical findings may support risk management but remain weak in disciplinary or legal proceedings. Legal, information technology, internal audit, cybersecurity, human resources, and forensic accounting functions should therefore establish shared protocols before an incident occurs.

Financial Services Authority Regulation Number 12 of 2024 provides an example of a comprehensive structure through four pillars of anti-fraud strategy: prevention; detection; investigation, reporting, and sanctions; and monitoring, evaluation, and follow-up (OJK, 2024). This structure supports the article's argument that religiosity occupies only part of the

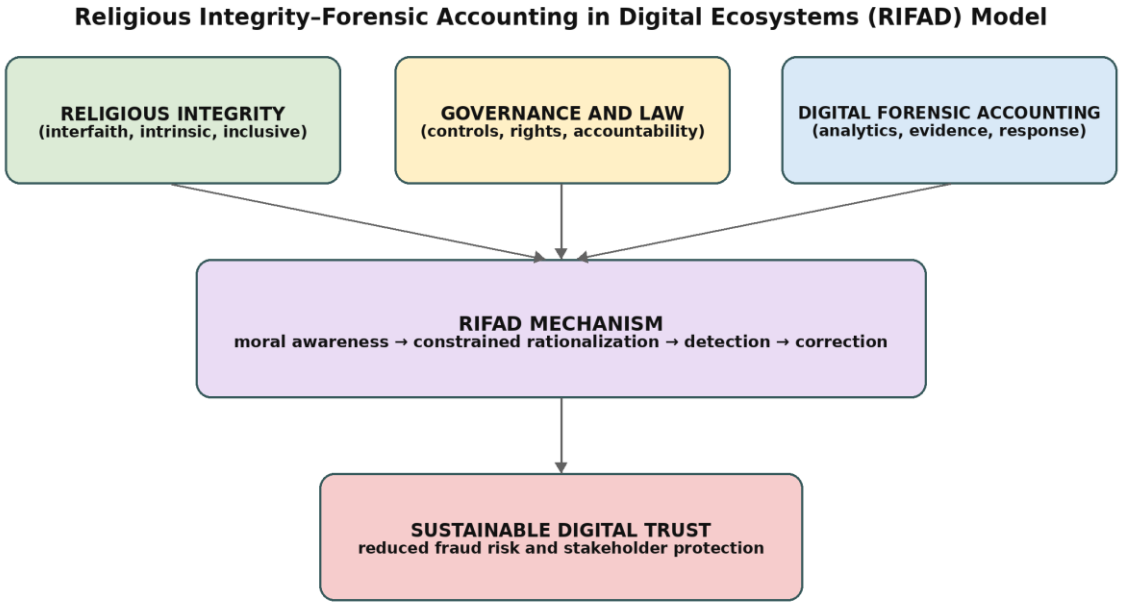
prevention layer. It must be translated into ethical leadership, conflict-of-interest management, and the courage to report, and subsequently reinforced by independent detection and response mechanisms.

The application of interfaith values must comply with the principle of non-discrimination. Integrity training may draw optionally and plurally on religious sources of inspiration, but compliance standards must not depend on declarations of belief, religiosity scores, or religious affiliation. Religious data are socially sensitive personal data and irrelevant to most anti-fraud decisions. Organizations should assess conflicts of interest, access violations, control overrides, documentation quality, and responses to red flags—not the depth of an individual's faith.

The RIFAD Model: Integrating Four Layers of Prevention

Based on the synthesis, this article proposes the Religious Integrity–Forensic Accounting in Digital Ecosystems (RIFAD) Model. The model conceptualizes prevention as four mutually correcting layers. The first is intrinsic and inclusive religious integrity; the second is governance and law; the third is digital forensic accounting; and the fourth is learning and remediation. No single layer is regarded as sufficient.

Religious integrity activates moral awareness and narrows the scope for rationalization. Governance and law reduce opportunity through clear authority, segregation of duties, access controls, transparency, and the protection of rights. Digital forensic accounting increases the likelihood of detection by connecting transactional and electronic evidence. Learning and remediation ensure that findings lead to system redesign, restitution, proportionate sanctions, and cultural improvement. This layered relationship avoids two extremes: morality without evidence and technology without conscience.



Source: Authors' synthesis.

Figure 1. The Religious Integrity–Forensic Accounting in Digital Ecosystems (RIFAD) Model

Table 3. Operational Architecture of the RIFAD Model

Layer	Objective	Core Practices	Auditable Indicators
Inclusive religious integrity	Prevents intent and rationalization	Ethical dilemmas, exemplary conduct, impact reflection, conflict-of-interest commitments	Quality of decision rationales, conflict declarations, override patterns
Governance and law	Constrains opportunity and protects rights	Segregation of duties, least privilege, privacy by design, reporting channels	Access matrix, report SLAs, evidence of anti-retaliation, DPIAs
Digital forensic accounting	Detects and substantiates	Continuous monitoring, anomaly/network analysis, preservation, chain of custody	Data coverage, false-positive rate, detection time, custody completeness
Learning and remediation	Improves systems and remedies harm	Root-cause review, restitution, sanctions, control redesign, governance reporting	Losses recovered, controls improved, recurrence of cases

Source: Authors' synthesis.

At the policy level, organizations can operationalize RIFAD through five steps. First, the board or senior leadership establishes a pluralistic and rights-based integrity statement. Second, risk assessments incorporate scenarios involving the misuse of data, algorithms, accounts, and related-party transactions. Third, preventive and detective controls are mapped to each scenario together with their respective control owners. Fourth, a cross-functional team agrees on evidence-preservation and escalation protocols. Fifth, each case is closed with a root-cause analysis and an assessment of whether target pressure, a culture of silence, or technology design contributed to enabling the fraud.

Training should not be confined to normative lectures. Dilemmas should be drawn from real digital business situations: whether a team may use data beyond the scope of consent to meet targets; when a model-generated alert may be overridden; how to respond to a superior's instruction to delay loss recognition; and whether employees may independently investigate a colleague's account. Participants should identify the victims, rights at risk, conflicts of interest, evidence required, and appropriate escalation route. In this way, religious values intersect with legal and professional competence.

Reporting channels form a critical bridge between values and systems. ACFE (2024) demonstrates the significance of tips in detecting fraud. Yet moral exhortations to report are hollow if whistleblowers face retaliation, their identities are disclosed, or their reports are ignored. Organizations should provide anonymous and confidential channels, ensure independence between channel administrators and reported parties, establish response-time standards, document decisions, and provide appeal mechanisms. Moral courage must be supported by institutional safety.

Fraud analytics should adopt a human-in-the-loop approach. A risk score is not a finding of guilt; it is a trigger for review. Investigators must examine data quality, potential bias, transactional context, and alternative explanations. Data access should be limited to what is necessary, and irrelevant findings should be deleted in accordance with retention policies. This approach aligns professional skepticism with the presumption of innocence, privacy, and procedural fairness.

Four conceptual propositions follow from the model. First, intrinsic religiosity is more strongly associated with fraud prevention than symbolic religiosity because it operates through moral identity and constrains rationalization. Second, the effect of religiosity on fraud prevention becomes stronger when ethical leadership and whistleblower protection are consistently implemented. Third, digital controls and forensic accounting mediate the translation of values into reduced opportunity and enhanced detection. Fourth, rights-based governance moderates the use of analytics so that greater detection effectiveness is not achieved at the expense of privacy and non-discrimination.

These propositions establish an agenda for subsequent empirical research. Religiosity should be measured through internalization and orientation rather than affiliation; fraud risk may be assessed through intentions, experimental behavior, verified incidents, or control effectiveness; and digital forensic maturity may be measured through log quality, detection time, evidence traceability, and investigative capacity. Relevant contextual variables include target pressure, ethical leadership, speak-up climate, model opacity, and dependence on third parties.

Novelty and Implications

The article's novelty lies in repositioning religiosity. First, religiosity is treated neither as a ceremonial variable nor as an autonomous control, but as an internal moral infrastructure that influences problem recognition, rationalization, and the courage to act. Second, the concept is translated into an auditable governance design so that values do not remain declarative. Third, the model treats rights protection, privacy, non-discrimination, and due process as components of anti-fraud effectiveness rather than obstacles to it. Fourth, forensic accounting is incorporated from the prevention and evidence-design stages, rather than only after losses have occurred.

For business leaders, the implication is the need to measure consistency among values, incentives, and actions. Leaders who speak about integrity while imposing unrealistic targets, tolerating overrides, or punishing bearers of bad news create structural rationalization. For accountants and auditors, digital competence must operate alongside objectivity, confidentiality, and professional skepticism in accordance with developments in the IESBA Code and ISA 240 (Revised). For regulators, principles-based approaches should be supplemented by guidance on digital evidence, model accountability, and whistleblower protection.

For higher education, the RIFAD Model can provide a framework for an interdisciplinary curriculum. Ethics and religiosity address the recognition of dilemmas; law addresses rights, obligations, and evidence; digital business addresses platform models and technological risks; and forensic accounting addresses transaction patterns, investigation, and the presentation of evidence. Interdisciplinary case-based learning is more appropriate than treating these four domains as disconnected bodies of knowledge.

The model also provides an important warning: organizations must not infer that fraud perpetrators are less religious or that visibly religious individuals can be trusted without controls. Such conclusions are not only scientifically weak but may also be discriminatory and create blind spots. Sound trust in digital business follows the principle of trust but verify: respecting human dignity while designing fair, transparent, and consistently applied controls.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Religiosity can contribute to preventing fraud in digital business when it takes an intrinsic and inclusive form reflected in judgment and conduct rather than symbols alone. Its principal mechanisms are strengthening moral awareness, constraining rationalization, and encouraging the courage to resist or report abuse. Religiosity, however, cannot eliminate opportunity,

reconstruct evidence, or guarantee procedural justice. Law, governance, digital controls, and forensic accounting are therefore indispensable complements.

The RIFAD Model addresses this need for integration through four layers: inclusive religious integrity; governance and law; digital forensic accounting; and learning and remediation. Its scholarly contribution lies in connecting moral, structural, technological, and corrective dimensions within a testable architecture. Its practical contribution is to provide a basis for organizations to translate values into controls, evidence, rights protection, and system improvement. Sustainable digital trust thus arises neither from morality without oversight nor from technology without conscience, but from the integration of values, rules, competence, and accountability.

Limitations

This article is conceptual and does not test the RIFAD Model in a particular organization or sector. Religiosity literature remains dominated by perception-based measures and by particular religious or national contexts; cross-faith generalization must therefore be undertaken cautiously. Technological and regulatory change is also rapid, while relationships among religiosity, ethical leadership, control quality, and fraud events may be bidirectional. The model should consequently be understood as an analytical framework requiring empirical testing, not as a claim that religiosity invariably reduces fraud.

Recommendations

Organizations are advised to integrate interfaith ethical dilemmas into anti-fraud training while expressing behavioral standards in professional and non-discriminatory language. Risk mapping should connect every digital scenario with a control owner, the lawful basis for data processing, sources of evidence, escalation routes, and victim-remediation mechanisms. Independent reporting channels, anti-retaliation protection, least privilege, continuous monitoring, and chain-of-custody protocols should be prioritized. Future research may test the RIFAD propositions through longitudinal designs, dilemma experiments, multilevel surveys, or comparative case studies across sectors and religious contexts. Such testing should also compare intrinsic and symbolic religiosity and examine the mediating roles of ethical leadership, speak-up climate, analytical maturity, and data-governance quality.

Author Contributions

Robertus Suraji: conceptualization of religiosity and interfaith ethics, and development of the humanities framework. Lintang Putri Estiarto: analysis of digital business ecosystems, platform risks, and technology governance. Istianingsih Sastrodiharjo: conceptualization of forensic accounting, legal and regulatory analysis, model synthesis, and scholarly revision. All authors read and approved the final version of the manuscript.

Acknowledgments

The authors express their gratitude to Universitas Bhayangkara Jakarta Raya and Universitas Terbuka for providing an academic environment that supports interdisciplinary inquiry into religiosity, law, digital business, and forensic accounting. The authors also thank their academic colleagues for facilitating discussions on ethics, integrity, and digital governance. This acknowledgment does not imply institutional involvement in the design, analysis, or publication decision of this article.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Allport, G. W., & Ross, J. M. (1967). Personal religious orientation and prejudice. Journal of Personality and Social Psychology, 5(4), 432–443. https://doi.org/10.1037/h0021212

Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations. ACFE. https://www.acfe.com/en-us/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.

Darsono, D., Ratmono, D., Putri, E. R. P., Cahyonowati, N., & Lee, S. (2024). An empirical analysis of asset misappropriation fraud during the COVID-19 crisis. Problems and Perspectives in Management, 22(3), 314–325. https://doi.org/10.21511/ppm.22(3).2024.25

Financial Services Authority of the Republic of Indonesia. (2024). Financial Services Authority Regulation of the Republic of Indonesia Number 12 of 2024 on the implementation of anti-fraud strategies for financial services institutions [Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 12 Tahun 2024 tentang Penerapan Strategi Anti Fraud bagi Lembaga Jasa Keuangan]. https://www.ojk.go.id/en/regulasi/Pages/12-Tahun-2024-Penerapan-Strategi-Anti-Fraud-bagi-Lembaga-Jasa-Keuangan.aspx

International Auditing and Assurance Standards Board. (2025). ISA 240 (Revised): The auditor's responsibilities relating to fraud in an audit of financial statements. IFAC. https://www.iaasb.org/publications/isa-240-revised-auditor-s-responsibilities-relating-fraud-audit-financial-statements

International Ethics Standards Board for Accountants. (2023). Final pronouncement: Technology-related revisions to the Code. IFAC. https://www.ethicsboard.org/publications/final-pronouncement-technology-related-revisions-code

International Ethics Standards Board for Accountants. (2025). 2025 handbook of the International Code of Ethics for Professional Accountants (including International Independence Standards). IFAC. https://www.ethicsboard.org/publications/2025-handbook-international-code-ethics-professional-accountants

Kontesa, M., Brahmana, R. K., & You, H. W. (2024). National culture, religiosity, and audited financial statements of small-scale MNCs. Pacific Accounting Review, 36(2), 211–233. https://doi.org/10.1108/PAR-10-2022-0162

Koufie, S., Tetteh, L. A., Kwarteng, A., & Fosu, R. A. (2025). The impact of ethical accounting practices on financial reporting quality: The moderating role of religiosity. International Journal of Ethics and Systems, 41(4), 973–1002. https://doi.org/10.1108/IJOES-01-2024-0004

Organisation for Economic Co-operation and Development. (2024). Revised recommendation of the Council on artificial intelligence (OECD/LEGAL/0449). OECD. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Pianoschi, A., & Mierlita, S. (2025). Revising ISA240 in a digital world: The sociomaterial perspective on fraud, technology, and stakeholder influence. Digital Finance, 7, 921–947. https://doi.org/10.1007/s42521-025-00139-2

Republic of Indonesia. (2008). Law Number 11 of 2008 on electronic information and transactions, as most recently amended by Law Number 1 of 2024 [Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024]. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

Republic of Indonesia. (2022). Law Number 27 of 2022 on personal data protection [Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi]. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Tiron-Tudor, A., Faragalla, W. A., & Pianoschi, A. (2025). The role of the accountancy professionals in detecting and preventing fraud, in a digital landscape: A systematic literature review. Digital Finance, 7, 745–786. https://doi.org/10.1007/s42521-025-00138-3

Ul Hassan, S. W., Kiran, S., Gul, S., Khatatbeh, I. N., & Zainab, B. (2025). The perception of accountants/auditors on the role of corporate governance and information technology in fraud detection and prevention. Journal of Financial Reporting and Accounting, 23(1), 5–29. https://doi.org/10.1108/JFRA-05-2023-0235

Weaver, G. R., & Agle, B. R. (2002). Religiosity and ethical behavior in organizations: A symbolic interactionist perspective. Academy of Management Review, 27(1), 77–97. https://doi.org/10.5465/amr.2002.5922390

Wibowo, A. S., Istianah, I., Sari, N. P., Rakhman, F., & Septiari, D. (2026). Does organizational integrity matter in enhancing financial reporting quality? Empirical evidence from local governments in Indonesia. Journal of Accounting & Organizational Change, 22(4), 723–747. https://doi.org/10.1108/JAOC-09-2024-0321

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. The CPA Journal, 74(12), 38–42.