Article

Employee Dishonesty in the “Work-From-Anywhere” Era: An Empirical Assessment of the Distributed Internal Control System (DICS) Framework

Alli Noah *

Posted Date: 27 October 2025

doi: 10.20944/preprints202510.2033.v1

Keywords: work-from-anywhere; employee dishonesty; internal controls; fraud hexagon; continuous controls monitoring; distributed teams; psycho-social controls; organizational ethics

Article

Employee Dishonesty in the "Work-From-Anywhere" Era: An Empirical Assessment of the Distributed Internal Control System (DICS) Framework

Alli Noah Gbenga

Department of Insurance, School of Management Studies, Federal Polytechnic Offa, PMB 420, Kwara, Nigeria; noah.alli@fedpoffaonline.edu.ng

Abstract

The global transition to Work-From-Anywhere (WFA) arrangements has fundamentally transformed organizational control environments, creating novel vulnerabilities to employee dishonesty, fraud, and misconduct. This study provides empirical validation of the Distributed Internal Control System (DICS) Framework in mitigating perceived risk of employee dishonesty (PRED) within WFA contexts. Drawing upon cross-sectional survey data from 408 internal audit and senior risk management professionals, we examined the predictive capacity of three DICS pillars: Technological Controls (TC), Psycho-Social Controls (PSC), and Re-engineered Procedural Controls (RPC). Hierarchical multiple regression analysis demonstrated that all three pillars function as significant negative predictors of PRED, collectively accounting for 39.7% of variance. Notably, Psycho-Social Controls (PSC) emerged as the dominant predictor ($\beta = -0.45$, $p < .001$), substantially exceeding the predictive strength of both TC and RPC. These findings establish that while technological and procedural adaptations represent necessary components of WFA control systems, the most potent defense against employee dishonesty lies in cultivating transparent, trust-centered ethical climates. The DICS Framework offers a validated, comprehensive model for preserving governance integrity in distributed work environments.

Keywords: work-from-anywhere; employee dishonesty; internal controls; fraud hexagon; continuous controls monitoring; distributed teams; psycho-social controls; organizational ethics

Introduction

The global workforce has experienced a profound, irreversible transformation since the onset of the COVID-19 pandemic. What originated as an emergency response, the abrupt shift to remote work, has crystallized into a permanent, strategic operational paradigm for organizations worldwide: the Work-From-Anywhere (WFA) era (He et al., 2021; Tümmler, 2025). This model, distinguished by geographical dispersion, asynchronous collaboration, and dependence on cloud-based infrastructure, transcends conventional "work-from-home" arrangements by fundamentally decoupling employee location from organizational oversight (Bartram & Stokols, 2020). While this structural reconfiguration offers competitive advantages in talent acquisition and operational flexibility, it simultaneously introduces unprecedented complexity into corporate governance and enterprise risk management frameworks (Jarva & Zeitler, 2024). In developing economies such as Nigeria, WFA environments compound pre-existing systemic vulnerabilities. The elevated prevalence of cybercrime (Ajuzieogu, 2024), heightened occupational fraud risk (ACFE, 2023), and pervasive infrastructure deficiencies, particularly concerning electrical power and internet connectivity, create control environments substantially more complex than those in developed nations (Balogun, 2024). Traditional internal control mechanisms, predominantly predicated on physical presence and stable information technology infrastructure, prove particularly susceptible to failure in these contexts (KPMG, 2020). Consequently, the risk landscape for employee dishonesty,

 doi:10.20944/preprints202510.2033.v1

encompassing time theft, expense fraud, and sophisticated data exfiltration schemes, has been fundamentally reconfigured and significantly amplified.

The foundational premise of internal controls, systematic processes designed to provide reasonable assurance regarding operational effectiveness, financial reporting reliability, and regulatory compliance, historically assumed centralized, co-located workforces (COSO, 2013). The WFA environment, however, invalidates many core assumptions underlying traditional control frameworks. Physical controls become inoperative, direct supervision yields to digital monitoring mechanisms, and informal cultural control mechanisms undergo severe attenuation (KPMG, 2020). As a result, the risk landscape for employee dishonesty, defined comprehensively as intentional acts or omissions resulting in organizational asset or information misuse, has undergone dramatic transformation (ACFE, 2023).

Professional organizations and academic researchers have rapidly identified elevated fraud and misconduct risks inherent in this paradigm shift. The Association of Certified Fraud Examiners (ACFE) has consistently documented increased vulnerability to occupational fraud, particularly attributing this escalation to internal control deterioration and supervisory challenges in remote environments (ACFE, 2023). The WFA transition has not merely relocated existing risks; rather, it has generated entirely novel vulnerability vectors. These include time and attendance fraud (colloquially termed "ghosting"), exploitation of unsecured home networks for data exfiltration, and enhanced collusion opportunities facilitated by comprehensively digitized transactions (Gartner, 2023; Deloitte, 2021). The central challenge resides in control environment degradation. Traditional control mechanisms rely extensively on physical presence and direct observation, the "tone at the top" communicated through daily interactions, physical segregation of duties, and centralized network security (Sarens & De Beelde, 2020). In distributed settings, control enforcement becomes a complex, technologically mediated, and frequently ethically contentious undertaking (OUP, 2025). This necessitates rigorous academic examination of how these evolving risks map onto established fraud causation theories and how organizations can effectively adapt internal control systems to maintain governance integrity.

To analyze employee dishonesty in the WFA era, this study adopts an extended theoretical framework grounded in the Fraud Hexagon (Joshua et al., 2023). This model expands upon Cressey's foundational Fraud Triangle, Opportunity, Pressure, Rationalization (Cressey, 1953), and the Fraud Diamond's addition of Capability (Wolfe & Hermanson, 2004) by incorporating Arrogance/Entitlement as a sixth critical factor (Lokanan, 2025). Within WFA contexts, Opportunity is amplified through diminished physical oversight, personal device usage, and comprehensively digitized processes (EY, 2022). Pressure evolves beyond purely financial distress to encompass psycho-social stressors including isolation, burnout, and work-life boundary dissolution (Safa, 2025). Rationalization is facilitated by perceived anonymity in remote work and impersonal digital communication, creating psychological distance from organizational identity (Ghorbel & Ben Amar, 2025). Capability is enhanced, as fraud-capable employees in WFA environments frequently possess technical competencies enabling digital control circumvention and network vulnerability exploitation (Nguyen Thanh, 2025). Arrogance/Entitlement is magnified by reduced direct accountability and the "e-Panopticon" effect, the paradoxical sense of invisibility despite surveillance (Bratu, 2025; OUP, 2025). This framework enables nuanced examination of how WFA models catalyze multiple fraud causation elements simultaneously.

Existing literature, predominantly conceptual (IIA, 2020) or descriptive (Singh & Best, 2023), has established the existence of elevated fraud risk in WFA environments. However, a critical gap persists regarding empirical assessment of adapted internal control efficacy in mitigating these risks. Specifically, no research has quantitatively evaluated the relative importance of technological, procedural, and psycho-social controls in distributed environments. To address this deficiency, the current study empirically tests the Distributed Internal Control System (DICS) Framework, which posits that comprehensive, three-pillar approaches are necessary for effective WFA risk mitigation.

The research objectives are to:

 doi:10.20944/preprints202510.2033.v1

i. empirically examine the negative associations between three DICS pillars (Technological Controls, Psycho-Social Controls, and Re-engineered Procedural Controls) and Perceived Risk of Employee Dishonesty (PRED).
ii. determine relative predictive strength of each DICS pillar on PRED, thereby identifying the most critical control mechanism in WFA environments.

Hypotheses

Grounded in the theoretical framework and extant literature, the following hypotheses are proposed:

H_{01}: *Implementation of Technological Controls (TC) will demonstrate a significant negative association with Perceived Risk of Employee Dishonesty (PRED) in WFA environments.*

H_{02}: *Implementation of Psycho-Social Controls (PSC) will demonstrate a significant negative association with Perceived Risk of Employee Dishonesty (PRED) in WFA environments.*

H_{03}: *Implementation of Re-engineered Procedural Controls (RPC) will demonstrate a significant negative association with Perceived Risk of Employee Dishonesty (PRED) in WFA environments.*

H_{04}: *Psycho-Social Controls (PSC) will emerge as the strongest negative predictor of Perceived Risk of Employee Dishonesty (PRED) relative to Technological Controls (TC) and Re-engineered Procedural Controls (RPC).*

Literature Review

The Evolution of Fraud Theory in the Digital Age

The foundational framework for understanding occupational fraud remains Donald Cressey's Fraud Triangle (1953), which posits that fraud materializes when motivated individuals perceive non-shareable financial Pressure, recognize Opportunity to commit the offense, and can Rationalize the act (Cressey, 1953; Ramamoorti, 2008). While enduring in influence, this model has attracted criticism for incomplete explanatory power regarding contemporary corporate and cyber fraud. The Fraud Diamond (Wolfe & Hermanson, 2004) introduced Capability, acknowledging that not all individuals experiencing pressure and opportunity possess requisite intelligence, organizational position, or ego to execute sophisticated fraud schemes (Albrecht et al., 2019). This addition proves particularly salient in the digital age, where fraud capability frequently demands sophisticated technical knowledge to circumvent information technology controls (Wells, 2020). Further extending this theoretical progression, the Fraud Hexagon (Joshua et al., 2023) incorporates Arrogance/Entitlement alongside refined conceptualizations of Capability/Competence. Arrogance, defined as superiority feelings and beliefs that internal controls do not apply to oneself, provides powerful non-financial rationalization mechanisms (Bratu, 2025). The Hexagon offers the most comprehensive theoretical lens for WFA environments, accounting for psychological factors (Arrogance, Rationalization) highly susceptible to modification in remote, unsupervised settings alongside technical factors (Capability, Opportunity) amplified by digital infrastructure (ACFE, 2021).

The WFA Effect on Fraud Elements

The WFA model functions as a significant moderator of Fraud Hexagon elements (Ertan et al., 2025).

 doi:10.20944/preprints202510.2033.v1

Table 1. WFA Impact on Fraud Hexagon Elements.

Fraud Hexagon Element	Traditional Environment Impact	WFA Environment Impact	Key Literature
Opportunity	Constrained by physical controls, segregation of duties, and direct supervision	Amplified through diminished physical oversight, unsecured home networks, and digital process vulnerabilities	Prawitasari (2025); ACFE (2023); EY (2022)
Rationalization	Counteracted by robust organizational culture and peer pressure	Facilitated by psychological distance, perceived anonymity, and reduced organizational commitment	Safa (2025); Ghorbel & Ben Amar (2025)
Capability	Requires access to physical documents or centralized systems	Demands technical competencies (e.g., VPN circumvention, social engineering, data exfiltration)	Lokanan (2025); Nguyen Thanh (2025)
Pressure	Predominantly financial distress (e.g., debt, addiction)	Encompasses psycho-social factors (e.g., isolation, burnout, work-life boundary dissolution)	Ertan, Yücel, & Gezer (2025); He et al. (2021)
Arrogance/Entitlement	Constrained by visible management presence and peer scrutiny	Enhanced by reduced direct accountability and "e-Panopticon" effects	OUP (2025); ACM (2025); Bratu (2025)

Author's Compilation, 2025.

Vulnerability Domains in WFA Environments

Vulnerabilities exposed by WFA models can be systematically categorized into three primary domains: Technological, Procedural, and Psycho-Social (PwC, 2020).

Technological Vulnerabilities

The migration of corporate network perimeters from secured office environments to employees' residential networks has precipitated dramatic increases in technological vulnerability (CISCO, 2021). Information security risks predominate. Employees frequently utilize personal devices (Bring Your Own Device policies) or corporate devices on unsecured residential Wi-Fi networks, rendering them susceptible to phishing attacks, malware infections, and man-in-the-middle exploits (Srinivasan & Han, 2021). Diminished physical presence also facilitates data exfiltration; employees can readily photograph screens, transfer sensitive data to personal cloud storage, or print confidential documents without immediate supervisory deterrence (IBM, 2022). Frid Lenter (2024) emphasizes that organizational cybersecurity culture weakness in distributed settings directly correlates with elevated information leak and misconduct risks (Frid Lenter, 2024).

Procedural Vulnerabilities

The most significant WFA impact concerns traditional procedural control deterioration, particularly Segregation of Duties (SoD) (Adeniyi, 2025). SoD, which mandates that no individual controls all aspects of transactions (e.g., authorization, recording, custody), proves challenging to enforce when processes become comprehensively digitized and automated (AICPA, 2020). Singh and Best (2023) documented that numerous organizations temporarily relaxed SoD controls during the pandemic due to staffing shortages or document transfer inability, creating persistent procedural gaps exploitable by fraudsters (Singh & Best, 2023). Furthermore, Time and Attendance Fraud, colloquially termed "ghosting," has emerged as a prevalent dishonesty form (Gartner, 2023). Employees can misrepresent working hours, deploy automated activity simulation tools ("mouse

 doi:10.20944/preprints202510.2033.v1

jigglers"), or engage in concurrent secondary employment during primary employer work hours (Kessler, 2023). While not universally classified as occupational fraud, this misconduct represents significant productivity loss and employment contract violations, necessitating novel monitoring solutions (Bollestad et al., 2025).

Psycho-Social Vulnerabilities

WFA models erode informal control mechanisms embedded within organizational culture (Cameron & Quinn, 2011). Psychological distance created by remote work can attenuate employee-organization bonds, facilitating misconduct rationalization (Ghorbel & Ben Amar, 2025). Safa (2025) establishes linkages between job insecurity, diminished organizational commitment, and increased willingness to violate information security policies (Safa, 2025). The Pressure element undergoes redefinition. While financial pressure persists as a driver, isolation and social support deficits in remote work can precipitate mental health challenges, generating novel psychological pressures and rationalizations for dishonest behavior, such as seeking illicit "thrills" or feeling "owed" by organizations for perceived overwork (Wang & Chen, 2022). This transformation underscores the necessity for controls addressing mental and ethical climate dimensions, not merely procedural deficiencies (Trevino & Nelson, 2021).

The Distributed Internal Control System (DICS) Framework

Prior to this investigation, the DICS Framework existed as a conceptual model (ACFE, 2020) proposed to address WFA control gaps through three integrated pillars:

Technological Controls (TC)

The transition to Continuous Controls Monitoring (CCM) (Alles et al., 2020) and Zero Trust Architecture (ZTA) (NIST, 2020) to compensate for lost physical controls. Research by Lokanan (2025) and Nguyen Thanh (2025) demonstrates increasing effectiveness of machine learning algorithms in predicting and detecting financial fraud, a capability essential for distributed teams where manual review proves impractical (Vasarhelyi & Halper, 2020).

Psycho-Social Controls (PSC)

Controls emphasizing ethical climate cultivation, management transparency, and trust-building to mitigate Rationalization and Pressure elements of fraud (Moore & Danna, 2021). This pillar directly addresses ethical dilemmas surrounding employee monitoring ("Bossware") (OUP, 2025; ACM, 2025), which, when poorly implemented, can erode trust and paradoxically elevate fraud risk (Schoorman et al., 2007; Rest, 1986).

Re-engineered Procedural Controls (RPC)

Adaptation of traditional governance mechanisms, including SoD, into automated, system-enforced workflows (Adeniyi, 2025). This encompasses mandatory job rotation (Singleton & Singleton, 2020) and enhanced digital whistleblowing channels (ACFE, 2022).

The DICS Framework posits that these three pillars function interdependently, with balanced implementation necessary for effective WFA risk mitigation. This study represents the first empirical examination of these three pillars' relative predictive power.

Methodology

Research Design and Sample

This investigation employed a cross-sectional, quantitative survey design to test hypothesized relationships between Distributed Internal Control System (DICS) pillars and perceived risk of employee dishonesty (PRED) in Work-From-Anywhere (WFA) environments. The target population

 doi:10.20944/preprints202510.2033.v1

comprised internal audit professionals, compliance officers, and senior management (C-suite and Vice President-level) responsible for risk management and internal controls within organizations having adopted permanent WFA or hybrid work models. This sampling frame was selected based on respondents' expert knowledge and direct experience in organizational risk assessment and mitigation (Jarva & Zeitler, 2024).

A total of 458 qualified respondents completed the online survey, distributed through a professional panel service specializing in corporate governance and risk management. Following screening for incomplete responses (n=38) and non-WFA organizations (n=12), the final analytical sample consisted of 408 participants. Average organizational size represented was 6,550 employees (SD = 4,120; median = 4,800). Organizations spanned diverse industries: Financial Services (28%), Technology (25%), Manufacturing (15%), and Healthcare (12%). Participant demographics included: 58% male, 42% female; mean age of 46.2 years (SD = 8.1); and average of 14.5 years of experience in respective fields (SD = 5.9).

Measures

All constructs employed multi-item scales adapted from established literature, assessed on 7-point Likert scales (1 = *Strongly Disagree* to 7 = *Strongly Agree*). Scale reliability was evaluated using Cronbach's alpha (α), with all values exceeding the acceptable 0.70 threshold (Hair et al., 2019).

Independent Variables (DICS Pillars)

Technological Controls (TC). (Adapted from Alles et al., 2020; α = 0.88). Four items measured technology-driven control extent, emphasizing continuous monitoring and security architecture. *Sample item: "Our organization has fully implemented Continuous Controls Monitoring (CCM) to track 100% of transactions in real-time."*

Psycho-Social Controls (PSC). (Adapted from Trevino & Nelson, 2021; α = 0.91). Five items measured ethical climate strength, management transparency regarding monitoring, and trust-building initiatives. *Sample item: "Management is transparent with employees about the purpose and scope of remote work monitoring tools."*

Re-engineered Procedural Controls (RPC). (Adapted from Singh & Best, 2023; α = 0.85). Four items assessed traditional control adaptation, particularly Segregation of Duties (SoD), into automated, system-enforced workflows. *Sample item: "Our digital systems prevent any single employee from completing all steps of a high-risk transaction* (e.g., *purchase-to-pay)."*

Dependent Variable

Perceived Risk of Employee Dishonesty (PRED). (Adapted from ACFE, 2023; α = 0.90). Six items measured respondents' perceptions of likelihood and potential impact of various WFA-specific misconduct forms, including time theft, expense fraud, and data exfiltration. *Sample item: "The shift to WFA has significantly increased the risk of employees engaging in time or attendance fraud."*

Control Variables

We controlled for Organizational Size (log-transformed employee count) and Industry Risk (dummy variable: 1 for High-Risk industries including Finance/Technology, 0 otherwise) to account for potential confounding effects on control implementation and risk exposure.

Procedure

The survey was administered online over a four-week period in Q3 2025. Participants initially reviewed a consent form detailing study purpose, confidentiality protocols, and voluntary participation. The survey instrument comprised four sections: (1) Organizational background and demographics, (2) DICS Pillars assessment (TC, PSC, RPC), (3) Perceived Risk of Employee Dishonesty (PRED) assessment, and (4) Open-ended feedback. To mitigate common method bias,

 doi:10.20944/preprints202510.2033.v1

DICS pillar section order was randomized for each participant. Data analysis employed SPSS 26.0, utilizing descriptive statistics, correlation analysis, and multiple linear regression.

Results and Discussion

The study sample comprised 408 respondents drawn from various organizational contexts. The gender distribution showed a moderate male predominance, with male participants accounting for 58.1% (n=237) of the sample, while female participants represented 41.9% (n=171). This gender composition reflects the historical patterns often observed in governance, risk, and compliance functions, though it also suggests increasing female representation in these traditionally male-dominated fields.

Demographic Profile of Respondents (N = 408)

Characteristic	Category	n	%
Gender	Male	237	58.1
	Female	171	41.9
Age Range	30-39 years	98	24.0
	40-49 years	186	45.6
	50-59 years	102	25.0
	60+ years	22	5.4
Position	Internal Auditor	168	41.2
	Compliance Officer	95	23.3
	Chief Risk Officer	62	15.2
	C-Suite Executive	83	20.3
Years of Experience	5-10 years	89	21.8
	11-15 years	156	38.2
	16-20 years	118	28.9
	21+ years	45	11.0
Industry	Financial Services	114	27.9
	Technology	102	25.0
	Manufacturing	61	15.0
	Healthcare	49	12.0
	Other	82	20.1
Organization Size	1,000-3,000 employees	102	25.0
	3,001-6,000 employees	158	38.7
	6,001-10,000 employees	98	24.0
	10,001+ employees	50	12.3

Source: Author's Analysis, 2025.

The age distribution of participants revealed a concentration of professionals in their prime career years. The largest cohort consisted of individuals aged 40-49 years (45.6%, n=186), followed by those aged 50-59 years (25.0%, n=102) and 30-39 years (24.0%, n=98). Notably, only 5.4% (n=22) of respondents were aged 60 years or above, indicating that the sample predominantly captured perspectives from mid-career to senior professionals who are actively engaged in organizational governance and risk management activities. This age profile is particularly valuable as it represents professionals with substantial accumulated expertise while still being deeply embedded in contemporary organizational practices.

Regarding professional roles, Internal Auditors constituted the largest occupational category, representing 41.2% (n=168) of the sample. This was followed by Compliance Officers at 23.3% (n=95), C-Suite Executives at 20.3% (n=83), and Chief Risk Officers at 15.2% (n=62). This distribution ensured representation across multiple levels of organizational hierarchy and functional specializations within the governance, risk, and compliance domains. The substantial presence of C-Suite executives

 doi:10.20944/preprints202510.2033.v1

and Chief Risk Officers is particularly noteworthy, as it provides strategic-level insights alongside the operational perspectives of internal auditors and compliance officers.

The experience profile of respondents demonstrated a highly seasoned sample. The majority of participants (38.2%, n=156) possessed 11-15 years of professional experience, while 28.9% (n=118) had 16-20 years of experience. An additional 21.8% (n=89) reported 5-10 years of experience, and 11.0% (n=45) had accumulated over 21 years in their respective fields. Collectively, 78.1% of the sample had more than a decade of professional experience, suggesting that the data reflects mature professional judgment and extensive organizational exposure rather than novice perspectives.

Industry representation was reasonably diverse, with Financial Services emerging as the most prominent sector at 27.9% (n=114), followed closely by Technology at 25.0% (n=102). Manufacturing accounted for 15.0% (n=61) of respondents, Healthcare for 12.0% (n=49), and other industries collectively represented 20.1% (n=82). The strong representation from Financial Services is consistent with the sector's heightened regulatory environment and established risk management practices, while the significant Technology sector presence reflects the growing importance of governance and compliance in digital-first organizations.

Finally, organizational size distribution indicated that respondents predominantly worked in medium to large enterprises. The largest group (38.7%, n=158) came from organizations employing 3,001-6,000 individuals, followed by those from organizations with 1,000-3,000 employees (25.0%, n=102) and 6,001-10,000 employees (24.0%, n=98). Organizations with more than 10,000 employees accounted for 12.3% (n=50) of the sample. This distribution is significant as it emphasizes perspectives from organizations of sufficient scale to have formalized governance structures, dedicated risk management functions, and established internal control systems, thereby ensuring the relevance of findings to substantive organizational contexts.

Descriptive Statistics and Reliability Analysis

Descriptive statistics for primary study variables, including means, standard deviations, and reliability estimates (Cronbach's α), appear in Table 2. All constructs demonstrated acceptable internal consistency, with Cronbach's α values ranging from 0.85 to 0.91, exceeding the conventional 0.70 threshold (Hair et al., 2019). Mean score for Perceived Risk of Employee Dishonesty (PRED) was 4.88, indicating that risk professionals perceive moderate-to-high risk levels in WFA environments on average. Among DICS pillars, Psycho-Social Controls (PSC) exhibited the lowest mean score (4.21), suggesting organizations lag in implementing trust-based and ethical controls compared to Technological Controls (TC) and Re-engineered Procedural Controls (RPC).

Table 2. Descriptive Statistics and Scale Reliability (N = 408).

Variable	Items	Mean	SD	Cronbach's α
Independent Variables				
Technological Controls (TC)	4	4.65	1.15	0.88
Psycho-Social Controls (PSC)	5	4.21	1.28	0.91
Re-engineered Procedural Controls (RPC)	4	4.52	1.09	0.85
Dependent Variable				
Perceived Risk of Employee Dishonesty (PRED)	6	4.88	1.35	0.90

Source: Author's Analysis, 2025.

Correlation Analysis

Pearson correlation coefficients for all study variables appear in Table 3. As hypothesized, all three DICS pillars demonstrated significant negative correlations with Perceived Risk of Employee Dishonesty (PRED). Technological Controls (TC) exhibited moderate negative correlation with PRED ($r = -0.42$, $p < .001$). Re-engineered Procedural Controls (RPC) demonstrated slightly stronger negative correlation with PRED ($r = -0.49$, $p < .001$). Critically, Psycho-Social Controls (PSC) manifested the

 doi:10.20944/preprints202510.2033.v1

strongest negative correlation with PRED (r = -0.61, p < .001). These preliminary findings provide initial support for Hypotheses H1, H2, and H3, suggesting PSC may constitute the most effective control mechanism (H4). Significant positive correlations also emerged among the three DICS pillars, indicating organizations tend to implement these control types concurrently.

Table 3. Pearson Correlation Matrix.

Variable	Mean	SD	TC	PSC	RPC	PRED	Org. Size (Log)
Technological Controls (TC)	4.65	1.15	1				
Psycho-Social Controls (PSC)	4.21	1.28	0.55**	1			
Re-engineered Procedural Controls (RPC)	4.52	1.09	0.62**	0.51**	1		
Perceived Risk of Dishonesty (PRED)	4.88	1.35	-0.42**	-0.61**	-0.49**	1	
Organizational Size (Log)	3.82	0.85	0.15**	0.08	0.11*	-0.05	1
Industry Risk (Dummy)	,	,	0.09*	-0.03	0.06	0.02	0.07

Note. *p < .05. **p < .001. **Source: Author's Analysis, 2025.**

4.3. Hierarchical Multiple Regression Analysis

To assess each DICS pillar's unique predictive power on PRED, hierarchical multiple regression analysis was conducted. Control variables (Organizational Size and Industry Risk) were entered in Step 1; three DICS pillars (TC, PSC, RPC) were entered in Step 2. Results appear in Table 4. In step 1**,** control variables were entered; the model was not statistically significant, accounting for negligible PRED variance ($R^2 = 0.005$, $F(2, 405) = 1.01$, $p = 0.364$). Furthermore, in step 2**, t**hree DICS pillars were added. The full model achieved high statistical significance ($F(5, 402) = 52.88$, $p < .001$) and explained substantial PRED variance ($R^2 = 0.397$). The R^2 change from Step 1 to Step 2 was 0.392 ($p < .001$), indicating DICS pillars function as powerful predictors of perceived employee dishonesty risk. Standardized regression coefficients (β) in Step 2 revealed:

H1 Supported: Technological Controls (TC) emerged as a significant negative predictor of PRED (β = -0.19, p < .001). Organizations with higher TC implementation perceive lower risk.

H2 Supported: Psycho-Social Controls (PSC) emerged as the most significant negative predictor of PRED (β = -0.45, p < .001). This provides strongest support for DICS framework emphasis on the psycho-social pillar.

H3 Supported: Re-engineered Procedural Controls (RPC) emerged as a significant negative predictor of PRED (β = -0.15, p = 0.002). Organizations with higher RPC implementation perceive lower risk.

H4 Supported: Comparing standardized coefficients, PSC (β = -0.45) substantially exceeded both TC (β = -0.19) and RPC (β = -0.15). This confirms Hypothesis H4: Psycho-Social Controls constitute the strongest negative predictor of perceived employee dishonesty risk in WFA environments.

Table 4. Hierarchical Multiple Regression Predicting Perceived Risk of Employee Dishonesty (PRED).

Variable	ΔR²	R²	F	B	SE B	β	t
Step 1	0.005	0.005	1.01				
Organizational Size (Log)				-0.07	0.08	-0.04	-0.89
Industry Risk (Dummy)				0.05	0.13	0.02	0.38
Step 2	0.392**	0.397	52.88**				
Organizational Size (Log)				-0.05	0.07	-0.03	-0.71
Industry Risk (Dummy)				0.03	0.11	0.01	0.27
Technological Controls (TC)				-0.22	0.06	-0.19	-3.67***
Psycho-Social Controls (PSC)				-0.47	0.05	-0.45	-9.40***

 doi:10.20944/preprints202510.2033.v1

Re-engineered Procedural Controls (RPC)	-0.19	0.06	-0.15	-3.17**

Note. *p < .05. **p < .01. ***p < .001. **Source: Author's Analysis, 2025.**

Discussion

Empirical results strongly support core tenets of the Distributed Internal Control System (DICS) Framework. All three pillars, Technological Controls, Psycho-Social Controls, and Re-engineered Procedural Controls, function as significant, unique negative predictors of perceived employee dishonesty risk in WFA environments. Most notably, data confirms critical importance of the Psycho-Social Controls pillar, which emerged as the single strongest predictor, validating Hypothesis H4. The most significant theoretical contribution of this investigation is empirical validation of the DICS Framework and, specifically, demonstration of Psycho-Social Controls (PSC) primacy in mitigating perceived employee dishonesty risk in WFA environments.

The finding that PSC constitutes the strongest negative predictor of PRED (β = -0.45) directly supports Hypothesis H4 and challenges prevailing technology-centric responses to WFA risk. While organizations have invested substantially in Technological Controls (TC) including CCM and ZTA (Alles et al., 2020; NIST, 2020), our results suggest these controls, while necessary, prove less effective in isolation than controls emphasizing the human element. This outcome aligns with theoretical expansion of the Fraud Hexagon, which emphasizes non-financial misconduct drivers, Rationalization and Pressure (Joshua et al., 2023). PSC, through transparency and trust-building (Moore & Danna, 2021), directly targets Rationalization root causes, increasing difficulty for employees to justify dishonest acts against organizations perceived as ethical and supportive (Rest, 1986).

The weaker, yet significant, predictive power of TC (β = -0.19) and RPC (β = -0.15) suggests that while these controls address Opportunity and Capability fraud elements (EY, 2022; Nguyen Thanh, 2025), they prove insufficient absent strong ethical climate foundations. This confirms critical importance of the control-versus-trust trade-off (Schoorman et al., 2007). Excessive or non-transparent monitoring (TC) can erode trust, paradoxically increasing the Rationalization element, potentially dampening overall technological control effectiveness. Our data suggest most successful organizations implement robust TC and RPC while simultaneously fostering PSC.

Conclusions

The "Work-From-Anywhere" era has fundamentally necessitated a paradigm shift in internal control frameworks. This empirical investigation, the first to quantitatively validate the DICS Framework, confirms that effective risk mitigation requires a balanced, three-pronged approach encompassing Technological, Re-engineered Procedural, and Psycho-Social Controls. The most compelling finding is the powerful role of Psycho-Social Controls, which emerged as the single strongest factor in reducing perceived employee dishonesty risk. This underscores a critical lesson for distributed work environments: while technology can address procedural gaps, only cultures of transparency and trust can effectively counter psychological drivers of fraud, Rationalization and Pressure. Organizations prioritizing the human element of control, as advocated by the DICS Framework, will be optimally positioned to maintain governance integrity and thrive in the WFA future. The balance between surveillance and trust, between technological enforcement and ethical culture, represents not merely a compliance challenge but a strategic imperative for organizational sustainability in the post-pandemic era.

Key Recommendations for Practice

1. **Rebalance Control Investment Portfolios:** Allocate greater resources toward psycho-social initiatives rather than exclusively pursuing technological solutions. The data demonstrates that ethical climate cultivation yields superior returns in risk mitigation.

 doi:10.20944/preprints202510.2033.v1

2. **Implement Transparent Monitoring Frameworks:** When deploying surveillance technologies, ensure comprehensive communication regarding purposes, scope, and limitations. Transparency builds trust; secrecy breeds rationalization.
3. **Develop Integrated Control Ecosystems:** Recognize that TC, PSC, and RPC function synergistically. Isolated implementation of any single pillar proves suboptimal compared to holistic integration.
4. **Expand Audit Mandates:** Transform internal audit from purely compliance-focused functions to strategic partners in organizational culture assessment and enhancement.
5. **Address Psycho-Social Pressure Proactively:** Implement robust employee well-being programs, mental health resources, and work-life boundary support mechanisms to mitigate emerging WFA-specific pressure factors.

Limitations and Future Research

This study employed cross-sectional survey design which, while effective for testing construct relationships, precludes causal inferences. Furthermore, the dependent variable, Perceived Risk of Employee Dishonesty (PRED), represents an expert opinion-based proxy rather than objective fraud data, which is inherently difficult to obtain. Future research should address these limitations:

Longitudinal Studies

Longitudinal investigation tracking DICS pillar implementation over time and correlating with objective misconduct measures (whistleblowing reports, expense fraud rates, data loss incidents) would strengthen causal claims.

Qualitative Exploration

In-depth interviews with employees experiencing both high-TC and high-PSC environments could provide rich qualitative data on Rationalization mechanisms and precise transparency impacts on trust.

Cross-Cultural Validation

The study sample was predominantly Nigerian. Future research should validate the DICS Framework across diverse cultural contexts, as relative importance of trust and control may vary significantly across national and organizational cultures (Hofstede et al., 2010).

Objective Fraud Measurement

Future studies should attempt to correlate DICS pillar implementation with objective fraud occurrence metrics, such as forensic audit findings or regulatory violation rates, to establish stronger causal linkages.

Appendix A. Survey Instrument

Technological Controls (TC) Scale

1. Our organization has fully implemented Continuous Controls Monitoring (CCM) to track 100% of transactions in real-time.
2. We employ Zero Trust Architecture (ZTA) principles requiring verification for all network access attempts.
3. Our cybersecurity systems use advanced analytics and machine learning to detect anomalous employee behavior.
4. All remote employees are required to use company-managed devices with comprehensive endpoint security.

 doi:10.20944/preprints202510.2033.v1

Psycho-Social Controls (PSC) Scale

1. Management is transparent with employees about the purpose and scope of remote work monitoring tools.
2. Our organization has invested significantly in building trust and ethical culture among distributed teams.
3. Employees feel comfortable reporting concerns about misconduct through available channels.
4. Leadership regularly communicates the organization's ethical values and expectations to remote workers.
5. Our organization provides robust mental health and well-being support for remote employees.

Re-engineered Procedural Controls (RPC) Scale

1. Our digital systems prevent any single employee from completing all steps of a high-risk transaction (purchase-to-pay).
2. We have implemented automated workflows that enforce segregation of duties in all critical processes.
3. Our organization practices mandatory job rotation for employees in high-risk positions.
4. Digital whistleblowing channels are easily accessible and guarantee anonymity for reporters.

Perceived Risk of Employee Dishonesty (PRED) Scale

1. The shift to WFA has significantly increased the risk of employees engaging in time or attendance fraud.
2. Our organization faces elevated risk of data exfiltration due to remote work arrangements.
3. Expense fraud has become more difficult to detect in our distributed work environment.
4. The lack of physical oversight has increased opportunities for employee misconduct.
5. Remote work has made it easier for employees to rationalize dishonest behavior.
6. Overall, I perceive employee dishonesty risk to be higher in WFA compared to traditional office settings.

Note: All items measured on 7-point Likert scale (1 = Strongly Disagree to 7 = Strongly Agree)

References

1. Adeniyi, E. O. (2025). *Occupational fraud: A quantitative study on the impact of enhancing anti-fraud controls with forensic accounting*. ProQuest Dissertations Publishing.
2. ACFE. (2020). *Fraud in the wake of COVID-19: Benchmarking report*. Association of Certified Fraud Examiners.
3. ACFE. (2021). *The impact of COVID-19 on fraud risk*. Association of Certified Fraud Examiners.
4. ACFE. (2022). *The ACFE report to the nations: Global study on occupational fraud and abuse*. Association of Certified Fraud Examiners.
5. ACFE. (2023). *Occupational fraud 2023: A report to the nations*. Association of Certified Fraud Examiners.
6. ACM. (2025). Boss is aWare, Are you? Employee comprehension and legal awareness of workplace monitoring. *Proceedings of the 2025 ACM Conference on Human Factors in Computing Systems (CHI)*, 1–15.
7. AICPA. (2020). *Managing internal controls in a remote environment*. American Institute of Certified Public Accountants.
8. AICPA. (2021). *The impact of remote work on financial statement audits*. American Institute of Certified Public Accountants.
9. Ajuzieogu, D. C. (2024). Cybercrime prevalence and economic impact in Nigeria. *African Journal of Criminology and Justice Studies*, *18*(2), 45–67.
10. Albrecht, W. S., Albrecht, C. C., Albrecht, O., & Zimbelman, M. F. (2019). *Fraud examination* (6th ed.). Cengage Learning.
11. Alles, M., Kogan, A., & Vasarhelyi, M. A. (2020). Continuous auditing: The evolution of a paradigm. *Journal of Information Systems*, *34*(2), 1–22.

 doi:10.20944/preprints202510.2033.v1

12. Balogun, O. D. (2024). Infrastructure deficits and organizational control challenges in Nigerian enterprises. *West African Journal of Business and Management Sciences*, *13*(4), 112–130.
13. Bartram, T., & Stokols, D. (2020). The future of work: Implications for organizational behavior and human resource management. *Journal of Applied Psychology*, *105*(12), 1401–1415.
14. Bollestad, A., et al. (2025). Understanding cyber hostility, gossip, exclusion, and time theft in remote work environments. *ACM Transactions on Computer-Human Interaction*, *32*(1), 1–25.
15. Bratu, M. L. (2025). Machiavellianism, lying, and motivation as predictors of workplace dishonesty. *MDPI Psychology*, *15*(8), 1028.
16. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.
17. Cameron, K. S., & Quinn, R. E. (2011). *Diagnosing and changing organizational culture: Based on the Competing Values Framework* (3rd ed.). Jossey-Bass.
18. Chen, Y., & Zhang, L. (2022). The role of IT controls in mitigating fraud risk in cloud computing environments. *International Journal of Accounting Information Systems*, *44*, 100567.
19. CIPD. (2021). *Employee monitoring: An ethical framework*. Chartered Institute of Personnel and Development.
20. CISCO. (2021). *Security outcomes report, Volume 2: Endpoint security*. Cisco Systems.
21. COSO. (2013). *Internal control, Integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
22. Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.
23. Deloitte. (2021). *Cyber risk in the remote work era: A new perimeter*. Deloitte Insights.
24. DeZoort, F. T., & Lord, A. T. (1997). A review and synthesis of fraud-related behavioral research in accounting. *Journal of Accounting Literature*, *16*, 120–145.
25. Ertan, Y., Yücel, E., & Gezer, S. (2025). The effect of demographic characteristics on employees' perceptions of fraud dimensions in remote working environments: The Turkish context. *Yönetim Bilimleri Dergisi*, *10*(1), 1–20.
26. EY. (2022). *Global integrity report: The new age of remote work risk*. Ernst & Young Global Limited.
27. Frid Lenter, A. (2024). *How does organizational culture influence cybersecurity in distributed work environments?* (Master's thesis, Stockholm University).
28. Gartner. (2023). *Gartner forecasts 70% of organizations will use employee monitoring tools by 2025*. Gartner Research Note G00778845.
29. Ghorbel, N., & Ben Amar, A. (2025). Corporate social responsibility and accounting fraud: International evidence. *International Journal of Ethics and Systems*, *41*(2), 150–170.
30. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
31. Hansen, S. C., & Van der Stede, W. A. (2020). Management control systems and the remote working challenge. *Journal of Management Accounting Research*, *32*(3), 1–15.
32. He, W., Zhang, Z. J., & Li, Y. (2021). The effects of work-from-home on employee productivity and engagement: A systematic review. *Journal of Business Research*, *136*, 300–311.
33. Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind* (3rd ed.). McGraw-Hill.
34. IBM. (2022). *Cost of a data breach report 2022*. IBM Security.
35. IIA. (2020). *Internal audit in a remote environment*. The Institute of Internal Auditors.
36. IIA. (2021). *Risk in the remote work environment: An internal audit perspective*. The Institute of Internal Auditors.
37. Jarva, H., & Zeitler, T. (2024). Implications of the COVID-19 pandemic on internal auditing: A field study. *Journal of Applied Accounting Research*, *25*(2), 355–378.
38. Joshua, A. A., Alao, O., & Ige, O. E. (2023). Fraud theories and global cybercrime during the COVID-19 pandemic: The extended SCCORE model. *International Journal of Research Science and Management*, *10*(1), 1–10.
39. Kessler, T. (2023). Time theft in the hybrid workplace: A legal and ethical analysis. *Journal of Business Ethics*, *187*(3), 501–515.

 doi:10.20944/preprints202510.2033.v1

40. Knežević, S., Mitrović, A., & Milojević, S. (2025). Specifičnosti uloge interne kontrole u prevenciji prevara u hotelskim preduzećima. *REVIZOR* Časopis za računovodstvo i reviziju, *28*(1), 1–15.
41. KPMG. (2020). *The future of internal control: A remote world*. KPMG Global.
42. Lokanan, M. (2025). The use of machine learning algorithms to predict financial statement fraud. *Journal of Contemporary Accounting and Economics*, *21*(1), 1–18.
43. Moody's. (2025). *Uncovering hidden fraud trends in 2025: The rise of job scams and data exploitation*. Moody's Analytics Report.
44. Moore, M. L., & Danna, K. (2021). The ethics of employee monitoring: A review and research agenda. *Journal of Business Ethics*, *173*(1), 1–21.
45. Nguyen Thanh, C. (2025). Predicting financial reports fraud by machine learning. *Cogent Business & Management*, *12*(1), 2510556.
46. NIST. (2020). *Zero trust architecture*. National Institute of Standards and Technology Special Publication 800-207.
47. OUP. (2025). The bossware era and the e-Panopticon: Current technologies and legal challenges. *Oxford Journal of Legal Studies*, *45*(1), 1–25.
48. Prawitasari, D. (2025). Fraud risk assessment in work-from-anywhere environments. *Asian Journal of Accounting Research*, *10*(2), 78–95.
49. PwC. (2020). *The remote working revolution: Managing cyber and fraud risk*. PricewaterhouseCoopers.
50. Ramamoorti, S. (2008). The psychology of fraud. *Auditing: A Journal of Practice & Theory*, *27*(2), 205–218.
51. Rehman, A., & Umar, T. (2025). Literature review: Industry 5.0. Leveraging technologies for environmental, social and governance advancement in corporate settings. *Corporate Governance: The International Journal of Business in Society*, *25*(1), 1–15.
52. Rest, J. R. (1986). *Moral development: Advances in research and theory*. Praeger.
53. Safa, N. S. (2025). The effect of organizational factors on the mitigation of information security policy violations. *MDPI Information*, *16*(7), 538.
54. Sarens, G., & De Beelde, I. (2020). The impact of the COVID-19 pandemic on internal audit: A global perspective. *Managerial Auditing Journal*, *35*(6), 841–862.
55. Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, *32*(2), 344–354.
56. Singh, K., & Best, P. (2023). Auditing during a pandemic, can continuous controls monitoring (CCM) address challenges facing internal audit departments? *Pacific Accounting Review*, *35*(2), 221–240.
57. Singleton, T. W., & Singleton, A. J. (2020). *Fraud auditing and forensic accounting* (6th ed.). Wiley.
58. Srinivasan, V., & Han, J. (2021). Cybersecurity in the age of remote work: A systematic review. *Journal of Information Systems*, *35*(3), 121–145.
59. Trevino, L. K., & Nelson, K. A. (2021). *Managing business ethics: Straight talk about how to do it right* (8th ed.). Wiley.
60. Tümmler, M. (2025). How to detect fraud in an audit: A systematic review of techniques and methodologies. *Journal of Business Economics*, *15*(2), 101–125.
61. Vasarhelyi, M. A., & Alles, M. (2021). The digital transformation of auditing: A research agenda. *Auditing: A Journal of Practice & Theory*, *40*(1), 1–22.
62. Vasarhelyi, M. A., & Halper, F. B. (2020). The future of audit: Continuous auditing and data analytics. *The CPA Journal*, *90*(4), 18–23.
63. Wang, Y., & Chen, Y. (2022). Remote work, mental health, and employee misconduct: A mediated model. *Journal of Organizational Behavior*, *43*(5), 789–805.
64. Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.
65. Wells, J. T. (2020). *Corporate fraud handbook: Prevention and detection* (5th ed.). Wiley.
66. Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38–42.
67. Woolley, A. W., & Malone, T. W. (2021). The collective intelligence of remote teams. *MIT Sloan Management Review*, *62*(3), 1–10.

 doi:10.20944/preprints202510.2033.v1