

From Compliance to Culture: Organizational Communication as a Tool to Foster Effective Fraud Risk Management in Insurance Industry

Ruchi Agarwal

Assistant Professor, Department of Strategic Management, MDI, Gurgaon (India)

Email id: ruchi.agarwal@mdi.ac.in

ORCID ID: <https://orcid.org/0000-0002-9836-5045>

Abstract

Fraud continues to pose a systemic challenge to the insurance industry, undermining regulatory compliance, consumer trust, and financial stability. Traditional explanations of fraud have relied on psychological frameworks such as the Fraud Triangle, Diamond, and Pentagon, which identify pressures, opportunities, rationalization, capability, and arrogance as central drivers of misconduct. Yet limited attention has been given to how organizational communication can intervene in these dynamics and operationalize legal and regulatory requirements within Enterprise Risk Management (ERM). This article presents findings from a longitudinal case study (2014–2024) of a leading Indian insurance company. Drawing on archival documents, internal communication records, and semi-structured interviews, the study traces how communication practices evolved across three phases of fraud risk management. In the compliance phase, communication served primarily as a legal tool to satisfy regulatory mandates, but it did little to reduce underlying opportunities or rationalizations. In the process phase, middle managers acted as sensegivers, reframing fraud detection through narratives, visualizations, and financial performance metrics, thereby linking regulatory compliance to operational value and enhancing organizational capability. In the transformation phase, communication shifted toward participatory dialogue and co-created digital tools, addressing arrogance and competence concerns and embedding fraud prevention into organizational identity. The findings demonstrate that communication functions as more than a compliance mechanism: it operates as a psychological and cultural bridge that translates abstract legal mandates into shared organizational practices. By linking communication strategies with established fraud theories, the study offers insights for regulators, insurers, and policymakers on how fraud risk management can be strengthened. It argues that effective communication not only supports regulatory alignment but also fosters a resilient risk culture, thereby reinforcing the legal and institutional integrity of the insurance sector.

Keywords: Insurance fraud, organizational communication, Enterprise Risk Management, regulatory compliance, risk culture, fraud psychology

1. Introduction

Fraud has long been treated as a form of unlawful conduct, positioned within the domain of criminology and regulatory sanction. In the insurance industry, fraud manifests not only in deliberate misrepresentation at the proposal stage or exaggerated claims but also in subtler manipulations that fall short of criminal thresholds yet undermine trust, fairness, and contractual obligations (Rawlings & Lowry, 2017). These include opportunistic exaggerations, reckless omissions, and third-party collusion, which may evade strict evidentiary proof yet erode the

388

Citation: Agarwal, R. (2025). From Compliance to Culture: Organizational Communication as a Tool to Foster Effective Fraud Risk Management in Insurance Industry. *International Insurance Law Review*, 33 (S4), 388-402.

principle of indemnity central to insurance law. The expanding notion of fraud has therefore shifted scholarly and regulatory attention from purely punitive enforcement toward systemic mechanisms of prevention, detection, and control. While legal instruments such as the fraudulent claims rule remain central, they cannot alone address the behavioural drivers—pressures, opportunities, rationalizations, and arrogance—that underlie fraudulent acts, nor the organizational practices that enable or constrain them.

Against this backdrop, communication emerges as a pivotal but underexplored dimension of fraud risk management. Existing scholarship on risk culture highlights governance structures, leadership tone, and audit mechanisms (Law, 2011; Roeschmann, 2014; Sheedy & Griffin, 2018), but often treats communication as secondary. Yet in practice, communication constitutes the channel through which regulatory requirements, ethical expectations, and organizational practices are translated into shared meaning. In the context of fraud risk, the absence of effective communication can reduce compliance to a transactional exercise, reinforcing symbolic legitimacy without materially addressing misconduct. Conversely, when communication operates as a strategic process—shaping narratives, fostering trust, and enabling participatory dialogue—it functions as a cultural bridge that embeds fraud prevention into Enterprise Risk Management (ERM). This article addresses the question of how communication practices evolve from compliance-driven directives to participatory and identity-shaping mechanisms, and how this evolution strengthens both legal compliance and organizational resilience in fraud risk management.

Building on prior research in developed economies that emphasizes governance structures, leadership tone, and audit mechanisms for fraud prevention (Law, 2011; Roeschmann, 2014; Sheedy & Griffin, 2018), and extending communication theory through Johansson and Heide's (2008) modes and Elving's, (2005) functional model, this study contributes to the literature by demonstrating how communication serves as the foundation of risk culture. First, it advances theory by showing that communication evolves from compliance-oriented directives, to participatory sensemaking, and finally to identity-shaping practices that embed fraud prevention within Enterprise Risk Management (ERM). Second, it addresses the conceptual gap in prior research that underplayed the *purpose* of communication—clarifying how informative communication reduces definitional ambiguity while community-building communication fosters trust, psychological safety, and ownership. Finally, the study provides practical insights for risk managers, regulators, and insurers by illustrating how differentiated communication strategies—ranging from top-down clarity to middle manager sensegiving and frontline trust-building—can shift fraud management from symbolic compliance toward an integrated, value-creating organizational culture.

The remainder of this paper is organized as follows: I first review the relevant literature on risk culture, organizational communication, and fraud risk management. I then present the theoretical framework and research methodology adopted in this study. Next, I provide the findings from the case analysis, illustrating how communication evolved from compliance to sensemaking and cultural integration. Finally, I discuss the implications of these findings for theory and practice, and conclude with recommendations for future research on the role of communication in strengthening risk culture and embedding fraud prevention within Enterprise Risk Management (ERM).

2. Literature Review

Understanding fraud through a psychological lens offers critical insights into how individuals' motivations and cognitive processes, shaped by organizational culture and communication, influence fraudulent behavior. Three predominant frameworks—the Fraud Triangle, Fraud Diamond, and Fraud Pentagon—inform ongoing psychological debates about the drivers of fraud. Cressey, 1950, 1953) Fraud Triangle posits that fraud emerges from three interconnected conditions: pressure, opportunity, and rationalization. Pressure may be financial, social, or identity-based, reflecting deeper psychological strains. Rationalization functions as a cognitive mechanism to reduce dissonance, allowing individuals to preserve a positive self-image while engaging in unethical behavior. Opportunity speaks not only to gaps in control systems but also to the perceived likelihood of detection, which is influenced by cultural norms and communication practices (Wallang & Taylor, 2012). Critics argue that this model is static and individual-centric, failing to account for collective dynamics and evolving narratives within organizations (Duffield and Justice, 2001).

Wolfe and Hermanson's (2004) Fraud Diamond extends the Triangle by adding capability, referring to individuals' ability to exploit opportunities. From a psychological standpoint, capability encompasses self-efficacy, confidence in one's technical skills, and resilience under pressure. Personality traits such as Machiavellianism or elevated risk tolerance have been linked to higher predisposition toward fraud, emphasizing the role of dispositional factors in fraud (Yang & Chen, 2023). However, some argue that capability may overlap with opportunity and question whether it should stand as a distinct dimension.

However, the Fraud Pentagon (Free & Murphy, 2015; Hidayah & Saptarini, 2019) introduces two further psychological constructs: arrogance and competence. Arrogance refers to excessive self-assurance and entitlement, prevalent among individuals in positions of relative power. Competence denotes deep expertise or insider knowledge facilitating concealment and manipulation. These aspects resonate with social psychological theories of moral disengagement and power dynamics. However, the addition of these traits raises concerns about redundancy and overemphasis on dispositional factors, potentially overlooking cultural and communicative influences.

Existing models, though informative, tend to prioritize individual decision-making over nuanced organizational contexts. Psychological research underscores the importance of communication—how fraud is narrated, framed, and discussed—in shaping rationalization pathways and reporting behavior. Models of fraud must evolve to incorporate dynamic sensemaking, where risk culture co-constructs perceptions and actions over time through dialogue which underscores the influence of trust, authenticity, and legitimacy in organizational contexts. For example, how trust cues are perceived can shape interpersonal behavior, and authenticity may provoke varied employee responses depending on relational dynamics (Tang et al., 2022). Meanwhile, research reflects concerns about the replicability and trustworthiness of IO psychology findings (Keener et al., 2023), underscoring the importance of rigorous psychological inquiry into fraud-related behaviors.

2.1 State of the Art in ERM, Fraud Risk, and Risk Culture

Enterprise Risk Management (ERM) has become a cornerstone of corporate governance, providing organizations with an integrated framework to identify, assess, and manage risks (Committee of Sponsoring organisations of the Treadway Commission, COSO, 2004; Venter, 2007). Within the ERM framework, fraud control occupies a strategic position, as fraud erodes between 5%–7% of an organization's annual revenue globally (Ramamoorti, 2008). Regulatory bodies and governance codes increasingly emphasize the embedding of fraud risk into ERM processes to safeguard financial stability and reputational capital (PwC, 2020). Risk culture is now recognized as a central determinant of ERM's success (Roeschmann, 2014), shaping how formal risk frameworks are internalized into daily practice. Following Schein (1996), culture is expressed through artifacts, shared values, and underlying assumptions, which together influence how employees perceive and act on fraud risks. Perspectives on risk culture range from integrated (unified and cohesive) to differentiated (subcultures with varying priorities) and fragmented (ambiguous and inconsistent), each carrying implications for how fraud risks are addressed (Dellaportas et al., 2007; Martin, 2002).

However, much of the ERM and fraud risk literature privileges structural and regulatory mechanisms over the lived experiences of organizational actors. Studies emphasize governance tools such as audit committees, internal controls, and regulatory compliance (H. Hassink et al., 2010; Hassink et al., 2009; Law, 2011), but provide limited insights into how these systems are understood and enacted across organizational levels. Power (2013) argues that fraud risk management often functions as a “ritual of verification,” where compliance reporting creates a façade of control without addressing underlying cultural weaknesses. This gap is particularly pronounced in emerging markets, where regulatory frameworks may mandate FRM units and reporting templates, but organizations still struggle with fragmented interpretations of fraud, weak employee buy-in, and limited integration with broader ERM systems (Agarwal & Kallapur, 2018). Thus, while ERM provides a formal scaffolding for fraud control, its effectiveness ultimately depends on how risk culture is cultivated and sustained through everyday practices.

2.2. Role of Communication in Improving Risk Culture

Despite advances in ERM theory, communication remains underexplored as a driver of risk culture. Hooks, Kaplan, and Schultz (1994) positioned communication indirectly through whistleblowing systems, where reporting channels act as deterrents and detection mechanisms. More recently, George et al. (2018) highlighted how communication media and cultural context shape the accuracy of deception detection¹, underscoring the need to tailor risk communication across both technological and cultural boundaries.

Yet, communication in practice is often constrained by institutional pressures and legitimacy concerns. Organizations frequently adopt standardized reporting formats and regulatory templates to satisfy external expectations (Beasley et al., 2015; Greenwood & Hinings, 1996), but these uniform systems risk entrenching rigidity, discouraging adaptation when fraud patterns evolve. Suddaby (2010) warns that communication strategies designed primarily for legitimacy may privilege symbolic compliance over material effectiveness. This creates a paradox: while

¹ George et al. (2018) define deception detection as the ability of individuals to distinguish between truthful and deceptive communication across different media and cultural contexts.

communication is necessary to build trust, clarify roles, and motivate employees, it is often reduced to procedural announcements that fail to engage meaningfully with frontline realities.

2.3 Issues Faced by Middle Managers in Risk Communication

Middle managers play a crucial role in shaping and sustaining risk communication within organizational risk culture, yet the literature consistently highlights significant challenges that undermine their effectiveness. In integrated cultures, where shared values and behaviours are intended to function as the “glue” of the organization (Schultz, 1994), middle managers are expected to reinforce a cohesive risk management narrative. However, the first issue they face is unclear messaging about what exactly they are supposed to do in Fraud Risk Management (FRM). While research often emphasizes the tone at the top (Law, 2011; Sheedy & Griffin, 2018), it fails to adequately address how strategic policies and risk objectives are translated into clear, actionable instructions for middle managers. In differentiated or fragmented cultures, where subcultures coexist or even conflict (Dellaportas et al., 2007; Martin, 2002), this ambiguity is magnified, leaving middle managers to interpret and align disparate departmental practices with organizational objectives under Traditional Risk Management (TRM), which tends to be siloed and compliance-oriented.

The second issue involves the lack of motivation and information regarding how fraud can be controlled, which prevents middle managers from effectively acting as “sensemakers” and “sensegivers” (Lüscher & Lewis, 2008). In fragmented cultures or under TRM, risk policies are often confined to documents and dashboards, lacking interactive communication channels that can foster understanding. This deficiency results in low psychological safety, underreporting of potential fraud indicators, and unchallenged rationalizations, echoing the fraud risk factors outlined in the Fraud Triangle, Diamond, and Pentagon (Cressey, 1953; Free, 2015; Free & Murphy, 2015; Wolfe & Hermanson, 2004). Studies also indicate that without motivational mechanisms and localized communication, middle managers may become disengaged from fraud monitoring efforts, relying solely on automated tools or auditors who themselves face role ambiguity (Hillison et al., 1999; Vinten et al., 2005).

The third issue is the lack of commitment and purpose in fraud, as middle managers often perceive fraud control as a box-ticking exercise rather than a meaningful component of strategic risk governance. In differentiated cultures, performance pressures within sub-units lead to prioritization of short-term results over cross-functional fraud risk objectives (Ghazali et al., 2014). This problem is exacerbated by the fourth issue: the weak embeddedness of fraud control within Enterprise Risk Management (ERM) frameworks. Literature highlights that ERM supports the development of cognitive risk culture, where risk awareness, learning, and feedback loops are institutionalized across the organization (Agarwal & Kallapur, 2018; Roeschmann, 2014). Without this integration, middle managers operate with fragmented or delayed information, fail to communicate lessons learned across units, and are unable to bridge formal fraud frameworks with daily practices.

Beyond these, three additional challenges emerge. First, role conflict and overload often hinder middle managers’ ability to prioritize fraud communication, as they juggle competing demands from senior management and frontline staff (Sims, 2003). Second, limited training and capability gaps constrain their effectiveness, since most fraud risk training emphasizes technical

compliance rather than communication and sensegiving skills (Watkins, 2003)(Watkins, 2003). Third, geographical dispersion and digital barriers in large organizations weaken the consistency of fraud communication, as localized interpretations and technological limitations prevent uniform engagement across branches (Hess & Cottrell Jr, 2016).

Collectively, these issues—unclear messaging, lack of motivation and information, weak commitment, poor ERM integration, role conflict, capability gaps, and geographical barriers—demonstrate that while middle managers are pivotal in fostering effective risk communication, they remain under-supported. Unless addressed, these challenges leave organizations vulnerable to fragmented fraud control, low employee engagement, and the persistence of compliance-oriented rather than learning-oriented cultures.

3. Methodology

This study employed a longitudinal single-case design to investigate how organizational communication shapes psychological aspects of fraud control and its integration into Enterprise Risk Management (ERM). A longitudinal approach was appropriate as it enabled the capture of evolving communication practices over time, tracing the shift from compliance-driven approaches to participatory and identity-based practices (Langley, 1999). The case study methodology allowed for an in-depth exploration of communication processes within their organizational context, particularly how middle managers acted as sensegivers and how communication strategies adapted to institutional pressures and cultural barriers (Yin, 2011). A revelatory case study approach was selected due to the rarity of access to fraud risk communication practices in emerging markets and the scarcity of empirical evidence linking communication frameworks with FRM-ERM integration. The chosen organization was a leading Indian insurance firm with revenues exceeding USD 1.5 billion and extensive regulatory exposure. Its transformation from regulatory compliance toward embedded cultural practices supported by digital tools made it an exemplary case, and access to multi-level communication processes in a highly regulated and confidential domain of fraud risk management further reinforced its revelatory nature (McCutcheon & Meredith, 1993).

Data were collected over a ten-year period (2014–2024) using semi-structured interviews, field notes, and organizational documents such as policy guidelines, regulatory submissions, presentations, and campaign materials. In total, fifteen interviews were conducted with senior leaders and operational managers, including the Group CRO, CRO, CFO, Head of Fraud, vice presidents, and members of the FRM department. Interviews ranged from 30 to 60 minutes and were conducted in person at the company's Indian head office and German headquarters as well as online via Zoom. Supplementary field notes were prepared during internal workshops, review meetings, and fraud prevention campaigns, while archival materials such as fraud reporting templates and analytics dashboards were reviewed to enhance data triangulation. Data collection followed three phases corresponding to the company's evolving communication practices: as a tool (2014–2016), as a process (2017–2020), and as social transformation (2021–2024).

The analysis followed a processual and iterative approach (Langley, 1999). All interviews were transcribed and, along with field notes, subjected to open coding (Strauss & Corbin, 1990). Codes were grouped into broader themes such as compliance framing, narrative reframing, trust-building, and ERM integration. These themes were then mapped against Johansson and Heide's

(2008) communication approaches—Tool, Process, and Social Transformation—and Elving's (2005) distinction between informative and community-building functions. This enabled a comparative analysis of how organizational communication evolved from transactional compliance to participatory sensemaking and cultural embedding. To strengthen the credibility of findings and minimize researcher bias, member-checking sessions were conducted with company stakeholders, ensuring contextual alignment and validation of interpretations.

All research activities were conducted in accordance with established ethical guidelines for psychological and organizational research. Informed consent was obtained from all participants, and confidentiality and anonymity were strictly maintained by removing identifiable information from transcripts and organizational records. Participation was entirely voluntary, and participants retained the right to withdraw at any time without penalty. As the study involved interviews with professionals discussing organizational practices and did not include vulnerable groups, medical procedures, or personal clinical data, it did not require approval from a formal Institutional Review Board (IRB). Instead, the research adhered to the APA Ethical Principles of Psychologists and Code of Conduct (2017) and the Declaration of Helsinki (2013) as a guiding framework, ensuring that participants' rights, dignity, and welfare were fully respected.

4. Theoretical Framework

The psychology of fraud highlights that fraudulent behavior cannot be explained solely by structural or regulatory failures; it is also driven by individual cognition, motivation, and cultural context. The Fraud Triangle (Cressey, 1950) identifies opportunity, pressure, and rationalization as key enablers of unethical behavior, while the Fraud Diamond Wolfe and Hermanson (2004) adds capability as a fourth factor. More recently, the Fraud Pentagon (Hidayah & Saptarini, 2019) has emphasized arrogance as an additional psychological driver. Together, these frameworks underscore that fraud risk communication must address both organizational structures and the psychological mechanisms through which individuals justify or pursue misconduct.

From an institutional perspective, organizations often imitate others when designing fraud risk communication systems, adopting tools such as risk registers or Control Self-Assessments (CSA) to signal legitimacy (DiMaggio & Powell, 1983; Elshandidy et al., 2018). While such imitation can safeguard reputation, it frequently leads to standardized reporting formats that may be poorly aligned with contextual realities (Beasley et al., 2015; Greenwood & Hinings, 1996). This tendency illustrates the psychological mechanism of rationalization in the Fraud Triangle, where compliance with external templates provides a façade of control, reducing the felt need for deeper cultural engagement.

Rigid adherence to standardized communication can create blind spots, as managers may resist revising fraud messages even when emerging risks demand flexibility (Suddaby, 2010). Some organizations attempt to move beyond symbolic compliance by using narratives (Avraamidou & Osborne, 2009; Suddaby, 2010), visual tools (Garcia-Retamero et al., 2012), or incentive-based strategies (Dobler, 2008). These efforts recognize that fraud communication is not merely technical but also psychological, shaping how employees interpret pressures, rationalizations, and opportunities. For example, capability misuse (Fraud Diamond) and arrogance (Fraud Pentagon) can only be countered when communication fosters trust, vigilance, and shared responsibility rather than passive adherence.

To conceptualize these dynamics, Johansson and Heide's (2008) framework offers three perspectives on communication: as a Tool, as a Process, and as Social Transformation. Communication as a "Tool" emphasizes top-down directives and compliance reporting. This approach is effective for standardization but limited in psychological impact, as employees often follow rules mechanically without internalizing fraud awareness. Communication as a "Process," by contrast, emphasizes sensemaking, enabling employees—particularly middle managers—to contextualize fraud risks through dialogue, stories, and visual cues. This corresponds to reducing rationalization (Fraud Triangle) and limiting capability misuse (Fraud Diamond) by fostering adaptive learning. Finally, communication as "Social Transformation" positions fraud prevention as a cultural and ethical practice, embedding vigilance within organizational identity. Storytelling, whistleblower protections, and symbolic recognition are key here, directly addressing the psychological roots of arrogance and entitlement emphasized in the Fraud Pentagon.

Despite its usefulness, Johansson and Heide's, (2008) (2008) framework does not fully explain why fraud communication matters for psychological engagement. (Elving, 2005) dual perspective of informative and community-building functions fills this gap. The informative function clarifies fraud definitions, thresholds, and reporting protocols, reducing ambiguity and preventing rationalization. The community-building function fosters trust, ownership, and moral commitment, thereby addressing deeper psychological enablers of fraud such as pressure, capability, and arrogance.

In sum, this theoretical framework integrates institutional theory, communication approaches, and psychological models of fraud to explain why organizations must move beyond symbolic compliance. Fraud risk communication becomes effective not merely when it informs but when it transforms—by engaging with the psychological drivers of fraud and embedding cultural practices that align with the Fraud Triangle, Diamond, and Pentagon.

5. Findings

Between 2014 and 2024, Company A's approach to fraud risk management (FRM) communication evolved in three distinct phases—compliance, process, and transformation. Each phase reflected not only regulatory alignment but also shifts in how employees psychologically engaged with fraud risk, moving from transactional reporting to cultural integration.

5.1 Phase I: Compliance (2014–2016) – Communication as Legal Clarity

In the early years, communication functioned primarily as a top-down compliance tool, aimed at clarifying definitions and satisfying reporting obligations. Employees were required to follow structured formats aligned with Insurance Regulatory and Development Authority of India (IRDAI, 2013) guidelines and the Companies Act (2013), but definitional inconsistencies created operational confusion. As one executive explained:

"They are not able to prove a claim to be fraudulent due to lack of evidence... [so] the company could not take any action against insured on the ground of 'intention to commit fraud'." (Head of Fraud)

To address this, the firm introduced "Name and Shame" guidelines to codify the distinction between fraud and abuse, a move described by the Vice-President of Legal Risk as necessary for consistency:

“Fraud is wilful and deliberate... Abuse generally fails to meet one or more of these criteria... repeated instances of abuse... should be termed as fraud beyond a certain threshold.”

While these measures enhanced compliance clarity, they did little to motivate employees or address the psychological drivers of fraud (opportunity and rationalization). Communication remained instrumental rather than engaging, and employees perceived FRM as “more of a disturbance” compared to existing audit and regulatory functions (Chief Risk Officer).

However, early signs of sensemaking emerged. A branch manager, during an internal review, used narrative and visual metaphors to reframe fraud risk as a “leaking bucket,” linking prevention directly to business outcomes. By showing how avoiding a single fraudulent motor claim funded two new outreach events, he demonstrated how communication could bridge compliance mandates and employee motivation.

5.2 Phase II: Process (2017–2020) – Communication as Sensemaking and Value Alignment

During the second phase, communication shifted from regulatory compliance toward sensegiving by middle managers, who began reframing fraud control as integral to business performance. Communication was no longer limited to directives; instead, managers employed narratives, visualizations, and financial metrics to connect fraud risk to everyday operations.

For instance, regional heads introduced monthly “fraud performance dashboards” that highlighted cost savings from fraud detection alongside policy sales figures. One senior manager explained:

“When we showed employees that each fraudulent cheque we stopped saved enough to fund new marketing campaigns, the conversation changed. Fraud control was no longer just about rules—it was about protecting growth.”

This approach linked fraud management to the Fraud Diamond’s competence dimension, emphasizing organizational capability rather than mere compliance. Employees began to see fraud reporting as an opportunity to contribute to efficiency rather than a burdensome regulatory exercise.

Still, tensions persisted. Some employees resisted additional documentation, perceiving it as “extra paperwork.” Yet, where managers employed narratives and outcome-oriented communication, employees reported higher ownership and reduced hesitation in reporting. In this phase, communication thus served as a process of translation—bridging legal requirements with operational priorities and helping employees rationalize fraud control as part of their own performance contribution.

5.3 Phase III: Transformation (2021–2024) – Communication as Cultural Integration

In the most recent phase, communication evolved into a participatory and transformative practice that directly addressed psychological drivers such as arrogance and rationalization, as emphasized in the Fraud Pentagon. Communication became multidirectional, emphasizing dialogue, trust-building, and co-creation of tools that embedded fraud control into organizational identity.

The launch of digital tools such as DigiSwasth, i-Inspect, Sarathi, and Motor OTS was accompanied by collaborative workshops where frontline staff helped design reporting formats and test usability. This participatory design process gave employees a sense of ownership, making fraud

management part of their professional identity rather than an imposed responsibility. As one employee noted: “Earlier fraud reporting felt like compliance. Now it feels like teamwork—when we design the tool together, we also design how we protect the company.”

Moreover, communication emphasized trust and psychological safety. Leaders encouraged open dialogue in town halls, sharing both successes and failures of fraud investigations. By normalizing discussion of errors and near misses, the company reduced fear of reprisal and fostered collective vigilance.

In this phase, communication transcended compliance and performance alignment, becoming a cultural practice that reinforced fraud prevention as “how we do things here.” Employees increasingly associated fraud control with organizational pride and ethical responsibility, while the company reported measurable improvements in claim savings and fraud reporting rates.

5.4 Communication as Social Transformation

The integration phase marked the transition from departmental adoption of FRM to its embedding as part of the organization’s cultural identity. The purpose of communication expanded beyond motivation and commitment to full integration within Enterprise Risk Management (ERM). At this stage, the challenge was not disengagement but autonomy concerns—departments perceived fraud checks as intrusive oversight: “Sometimes, it feels like we are being audited every day... FRM needs to trust that we also aim for the company’s good.” (Underwriting Head)

To resolve this tension, middle managers framed FRM as a mutual safeguard: “We’re not here to question your judgment; we’re here to co-develop safeguards. If the same customer cheats underwriting and later hits claims, it affects us all.” (LM Manager)

Digital innovations—such as DigiSwasth, i-Inspect, i-Inspect OTS, and Sarathi—were positioned as communicative anchors. Rather than being viewed as control tools, they were reframed as enablers of efficiency, transparency, and trust (see Table 1). This reframing illustrates how communication aligned identity, power, and discourse, turning FRM from a regulatory imposition into a collective responsibility and cultural norm.

Table 1: Examples of Reframed Meaning Through Tech

App	Communicative Reframing
<i>DigiSwasth</i>	From “medical tests as delays” → to “trust-building enabler for policyholders and underwriters”
<i>i-Inspect</i>	From “surveyor inefficiency” → to “customer empowerment and cost transparency”
<i>i-Inspect OTS</i>	From “repair shop overcharges” → to “objective claim valuation through AI”
<i>Sarathi</i>	From “agent onboarding burden” → to “smart governance of agent credibility”

Source: Created by authors

The analysis shows that communication acted as the central driver in advancing fraud risk management (FRM) through successive phases of compliance, readiness, commitment, and integration. In the compliance phase, communication was transactional, focused on regulatory alignment and top-down directives. While tools such as the “Name and Shame Guidelines”

reduced interpretive variance, unclear definitions of fraud across IRDAI and Company Law created operational ambiguity, limiting deeper engagement. The readiness phase marked a turning point, where middle managers reframed FRM from fault-finding into a business enabler using narratives, visual tools, and financial storytelling. This shift translated compliance into business relevance, as reflected in cost savings and declining cheque dishonour rates, though psychological safety concerns continued to limit active whistleblowing.

As the process matured, communication moved toward building trust, ownership, and cultural integration. The commitment phase addressed motivational gaps through initiatives like town halls, role-reversal workshops, and the “Loss Prevention Ambassador” campaign, which incentivized fraud reporting and normalized participation. In the final integration phase, communication resolved autonomy concerns by fostering co-creation and cross-functional innovation, embedding FRM within the broader ERM framework. Digital tools such as DigiSwasth, i-Inspect, and Sarathi became communicative anchors of efficiency and ethics, reinforcing FRM as a collective responsibility. Overall, communication evolved from compliance-driven messaging to sensegiving and collaborative meaning-making, transforming FRM into a resilient organizational capability and part of the company’s cultural identity.

6. Discussion: From Compliance to Cultural Integration

This study demonstrates how communication in fraud risk management (FRM) evolved from a compliance-oriented function into a transformative organizational practice that shaped motivation, trust, and identity. Rather than being a neutral tool, communication emerged as a psychologically grounded process that mediated the relationship between regulatory expectations, managerial framing, and employee engagement.

In the early compliance phase (2014–2016), communication served primarily as a legitimacy mechanism. Standardized templates and “Name and Shame” guidelines clarified definitions and fulfilled regulatory obligations, reflecting institutional theory’s argument that organizations initially adopt practices symbolically to meet external expectations (DiMaggio & Powell, 1983; Suddaby, 2010). However, the lack of definitional clarity between IRDAI and Company Law created interpretive gaps, weakening sensemaking and reinforcing the perception of FRM as externally imposed. Psychologically, employees complied without engagement, viewing fraud reporting as disruptive rather than meaningful.

The process phase (2017–2020) marked a shift toward sensemaking and value alignment. Middle managers reframed communication using narratives, dashboards, and financial storytelling to connect fraud control with business outcomes. This reflects Johansson and Heide’s (2008) framing of communication as sensegiving, where meaning is actively constructed to align employee cognition with organizational goals. Employees began to recognize fraud control as a contributor to growth, not just surveillance. Campaigns such as the *Loss Prevention Ambassador* demonstrated how communication that integrates incentives with ethical framing can enhance psychological safety, transforming whistleblowing into an act of prosocial contribution. This aligns with motivational psychology, where extrinsic and intrinsic drivers combine to foster sustained behavioral change.

Finally, in the transformation phase (2021–2024), communication became a cultural practice. By embedding FRM into the broader ERM framework, organizations redefined fraud prevention as

a shared identity and collective responsibility. Participatory workshops, town halls, and co-designed digital tools (e.g., DigiSwasth, i-Inspect, Sarathi) acted as communicative anchors, reframing fraud checks as enablers of trust and efficiency rather than control mechanisms. This resonates with discursive perspectives on communication (Johansson & Heide, 2008), where meaning is negotiated and institutionalized into “how we do things here.” Psychologically, this stage reflected internalization: employees no longer needed extrinsic monitoring but instead engaged in fraud control as an expression of organizational pride and ethical responsibility. Taken together, the findings highlight a psychological trajectory of communication—from compliance (external regulation), to process (sensemaking and salience), to transformation (identity and internalization). This complements existing frameworks by demonstrating how communication functions simultaneously as tool, process, and discourse (Johansson & Heide, 2008) while fulfilling both informative and community-building roles (Elving, 2005).

7. Conclusion

This study shows that fraud risk management (FRM) in the insurance industry cannot be understood only as a matter of regulatory compliance or technical control. Instead, FRM communication operates as a psychological and cultural mechanism that shapes how employees perceive, rationalize, and act upon fraud. By examining Company A’s decade-long trajectory, the findings demonstrate a progression across three phases: compliance, process, and transformation.

In the compliance phase, communication served as a legal tool to enforce definitions and reporting standards, but its symbolic and top-down nature produced only limited ownership. In the process phase, communication evolved into sensemaking, where middle managers used narratives, visualization, and financial storytelling to make fraud risk both cognitively salient and commercially relevant. The transformation phase marked a cultural shift: communication was embedded into identity and organizational practice through dialogue, psychological safety, and co-creation of digital tools. Together, these phases show how FRM communication advanced from regulatory alignment to cultural integration, aligning fraud vigilance with organizational identity and ethical responsibility.

From a theoretical standpoint, the study confirms that communication frameworks (Elving, 2005; Johansson & Heide, 2008) are essential for understanding how regulatory practices translate into lived organizational norms. It also contributes to law-and-management scholarship by illustrating how regulatory ambiguities—such as divergent definitions of fraud under IRDAI guidelines and Company Law—can create operational confusion unless mediated by communicative practices that foster sensemaking and shared meaning.

For managers and insurers, the study underscores that fraud risk communication must evolve beyond transactional compliance. Narrative-based training, financial storytelling, and participatory workshops can make fraud vigilance more meaningful, helping employees perceive reporting not as punitive but as a value-creating activity. Institutionalizing psychological safety is equally critical: employees must be assured that whistleblowing will not result in reprisals but will instead be recognized as a contribution to collective goals. In addition, embedding digital tools such as dashboards and reporting apps into daily workflows can serve as communicative anchors, making vigilance both visible and normalized across the organization.

For policymakers, the findings highlight the need to recognize that compliance, while essential, is insufficient in isolation. Effective fraud management requires regulatory frameworks that encourage insurers to integrate communication strategies linking fraud control to organizational culture and ethical identity. Policy initiatives could require insurers not only to demonstrate compliance metrics but also to provide evidence of employee engagement, participation, and cultural embedding of fraud risk management practices. Moreover, harmonizing legal definitions of fraud and abuse across statutes would reduce operational ambiguity and enhance legal certainty, ensuring that employees and organizations alike can act with clarity and consistency. For regulators in the insurance industry, particularly IRDAI, the study suggests the importance of shifting from checklist-based supervision toward evaluating the communicative and cultural dimensions of fraud risk management. Regulators could mandate periodic communication audits—through surveys, training evaluations, and whistleblowing metrics—to provide early warning signals of weak vigilance. Digital fraud management innovations such as DigiSwasth, i-Inspect, and Sarathi should also be promoted not merely as control mechanisms but as instruments of transparency and trust, strengthening relationships between insurers, policyholders, and regulators. Taken together, these steps emphasize that sustaining fraud resilience in the insurance sector requires legal precision, organizational engagement, and regulatory foresight in equal measure.

References

- Ruchi Agarwal & Sanjay Kallapur, *Cognitive Risk Culture and Advanced Roles of Actors in Risk Governance: A Case Study*, 19 J. Risk Fin. 4 (2018), <https://doi.org/10.1108/JRF-11-2017-0189>.
- Lucy Avraamidou & Jonathan Osborne, *The Role of Narrative in Communicating Science*, 31 Int'l J. Sci. Educ. 1683 (2009), <https://doi.org/10.1080/09500690802380695>.
- Mark Beasley, Bruce Branson & Don Pagach, *An Analysis of the Maturity and Strategic Impact of Investments in ERM*, 34 J. Acct. & Pub. Pol'y 219 (2015).
- Comm. of Sponsoring Orgs. of the Treadway Comm'n, *Enterprise Risk Management—Integrated Framework: Executive Summary* (2004).
- Donald R. Cressey, *The Criminal Violation of Financial Trust*, 15 Am. Soc. Rev. 738 (1950).
- Donald R. Cressey, *Other People's Money: A Study of the Social Psychology of Embezzlement* (1953).
- Steven Dellaportas, Barry J. Cooper & Philomena Braica, *Leadership, Culture and Employee Deceit: The Case of the National Australia Bank*, 15 Corp. Governance: Int'l Rev. 1442 (2007), <https://doi.org/10.1111/j.1467-8683.2007.00597.x>.
- Paul DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Collective Rationality and Institutional Isomorphism in Organizational Fields*, 48 Am. Soc. Rev. 147 (1983).
- Michael Dobler, *Incentives for Risk Reporting—A Discretionary Disclosure and Cheap Talk Approach*, 43 Int'l J. Acct. 184 (2008).
- Graeme Duffield & Peter Grabosky, *The Psychology of Fraud*, Trends & Issues in Crime & Crim. Just., no. 199 (2001), <https://www.aic.gov.au/sites/default/files/2020-05/tandi199.pdf>.
- Tamer Elshandidy, Philip J. Shrivess, Mary Bamber & Solomon Abraham, *Risk Reporting: A Review of the Literature and Implications for Future Research*, 40 J. Acct. Literature 54 (2018).

- Wouter J.L. Elving, *The Role of Communication in Organisational Change*, Corp. Commc'ns: Int'l J. (2005).
- Christopher Free, *Looking Through the Fraud Triangle: A Review and Call for New Directions*, 23 *Meditari Acct. Rsch.* 175 (2015), <https://doi.org/10.1108/MEDAR-02-2015-0009/full/html>.
- Christopher Free & Patrick R. Murphy, *The Ties That Bind: The Decision to Co-Offend in Fraud*, 32 *Contemp. Acct. Rsch.* 18 (2015), <https://doi.org/10.1111/1911-3846.12063>.
- Rocio Garcia-Retamero, Yasmina Okan & Edward T. Cokely, *Using Visual Aids to Improve Communication of Risks About Health: A Review*, JNCI Monographs, no. 25, at 149 (2012), <https://doi.org/10.1100/2012/562637>.
- Mohd Zulkifli Ghazali, Mohd S. Rahim, Azian Ali & Siti A. Abidin, *A Preliminary Study on Fraud Prevention and Detection at the State and Local Government Entities in Malaysia*, 164 *Procedia Soc. & Behav. Sci.* 437 (2014).
- Royston Greenwood & C.R. Hinings, *Understanding Radical Organizational Change: Bringing Together the Old and the New Institutionalism*, 21 *Acad. Mgmt. Rev.* 1022 (1996).
- H.F.D. Hassink, L.H. Bollen, R.H.G. Meuwissen & M.J. de Vries, *Corporate Fraud and the Audit Expectations Gap: A Study Among Business Managers*, 18 *J. Int'l Acct., Auditing & Tax'n* 85 (2009).
- Henk Hassink, Ruud Meuwissen & Laurens Bollen, *Fraud Detection, Redress and Reporting by Auditors*, 25 *Managerial Auditing J.* 861 (2010).
- Mark F. Hess & James H. Cottrell Jr., *Fraud Risk Management: A Small Business Perspective*, 59 *Bus. Horizons* 13 (2016).
- Eka Hidayah & Gita D. Saptarini, *Pentagon Fraud Analysis in Detecting Potential Financial Statement Fraud of Banking Companies in Indonesia*, Proc. UII-ICABE, 89 (2019), <https://journal.uui.ac.id/icabe/article/view/14697>.
- William Hillison, Carl Pacini & David Sinason, *The Internal Auditor as Fraud-Buster*, 14 *Managerial Auditing J.* 351 (1999).
- Christian Johansson & Mats Heide, *Speaking of Change: Three Communication Approaches in Studies of Organizational Change*, 13 *Corp. Commc'ns: Int'l J.* 288 (2008), <https://doi.org/10.1108/13563280810893661/full/html>.
- Skyler Keener, Szilvia Kepes & Anke Torke, *The Trustworthiness of the Cumulative Knowledge in Industrial/Organizational Psychology: The Current State of Affairs and a Path Forward*, 239 *Acta Psychologica* 04005 (2023), <https://www.sciencedirect.com/science/article/pii/S0001691823001816>.
- Ann Langley, *Strategies for Theorizing from Process Data*, 24 *Acad. Mgmt. Rev.* 691 (1999), <https://doi.org/10.5465/amr.1999.2553248>.
- Philip Law, *Corporate Governance and No Fraud Occurrence in Organizations: Hong Kong Evidence*, 26 *Managerial Auditing J.* 501 (2011).
- Lotte S. Lüscher & Marianne W. Lewis, *Organizational Change and Managerial Sensemaking: Working Through Paradox*, 51 *Acad. Mgmt. J.* 221 (2008).
- Joanne Martin, *Organizational Culture: Mapping the Terrain* (2002).

- David M. McCutcheon & Jack R. Meredith, *Conducting Case Study Research in Operations Management*, 11 J. Operations Mgmt. 239 (1993), [https://doi.org/10.1016/0272-6963\(93\)90002-7](https://doi.org/10.1016/0272-6963(93)90002-7).
- Michael Power, *The Apparatus of Fraud Risk*, 38 Acct., Orgs. & Soc'y 525 (2013).
- PwC, *Fighting Fraud: A Never Ending Battle* (2020).
- Sridhar Ramamoorti, *The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component into Fraud and Forensic Accounting Curricula*, 23 Issues in Acct. Educ. (2008), <http://jthomasniu.org/class/781/Readings/psychoffraud.pdf>.
- Philip Rawlings & John P. Lowry, *Insurance Fraud and the Role of the Civil Law*, 80 Mod. L. Rev. 510 (2017), <https://doi.org/10.1111/1468-2230.12269>.
- Andrea Zeller Roeschmann, *Risk Culture: What It Is and How It Affects an Insurer's Risk Management*, 17 Risk Mgmt. & Ins. Rev. 277 (2014).
- Edgar H. Schein, *Three Cultures of Management: The Key to Organizational Learning*, Sloan Mgmt. Rev., Fall 1996, at 9.
- Majken Schultz, *On Studying Organisational Cultures* (1994).
- Elizabeth Sheedy & Barbara Griffin, *Risk Governance, Structures, Culture, and Behavior: A View from the Inside*, 26 Corp. Governance: Int'l Rev. 4 (2018).
- David Sims, *Between the Millstones: A Narrative Account of the Vulnerability of Middle Managers' Storying*, 56 Hum. Relations 1195 (2003).
- Anselm Strauss & Juliet M. Corbin, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques* (1990).
- Roy Suddaby, *Challenges for Institutional Theory*, 19 J. Mgmt. Inquiry 14 (2010), <https://doi.org/10.1177/1056492609347564>.
- Yiqun Tang, Ruixue Jia, Lili Long, Zhen Ren & Xinhui Pu, *The Double-Edged Sword of Employee Authenticity in Coworker Interactions: The Moderating Role of Relationship Duration*, 54 Acta Psychologica Sinica 529 (2022), <https://doi.org/10.3724/SP.J.1041.2022.00529>.
- A.C. Venter, *A Procurement Fraud Risk Management Model*, 15 Meditari Acct. Rsch. 77 (2007), <https://doi.org/10.1108/10222529200700012/full/html>.
- George Vinten, Philip Alleyne & Michael Howard, *An Exploratory Study of Auditors' Responsibility for Fraud Detection in Barbados*, Managerial Auditing J. (2005).
- Philip Wallang & Robin Taylor, *Psychiatric and Psychological Aspects of Fraud Offending*, 18 Advances in Psychiatric Treatment 183 (2012), <https://doi.org/10.1192/apt.bp.111.008946>.
- Sherron Watkins, *Former Enron Vice President Sherron Watkins on the Enron Collapse*, 17 Acad. Mgmt. Persp. 119 (2003).
- David T. Wolfe & Dana R. Hermanson, *The Fraud Diamond: Considering the Four Elements of Fraud* (2004).
- Meng Yang & Yiyuan Chen, *Cognitive Rationalization in Occupational Fraud: Structure Exploration and Scale Development*, 14 Frontiers in Psych. 1112127 (2023), <https://doi.org/10.3389/fpsyg.2023.1112127/full>.
- Robert K. Yin, *Applications of Case Study Research* (2011), <https://books.google.com/books?id=LM5yAwAAQBAJ>

Received: 07 Sep 2025 Accepted: 16 Sep 2025 Published: 23 Sep 2025
--