

THE RISK MANAGEMENT FORUM

TRMF Working Paper Series

WP-2026-005

ISSN: Applied for

JEL Classification: M14, D73, J24, K42, M12

COHESION OR COMPLICITY:

Organisational Culture as a Risk Transmission Environment

Dr André Du Venage, DBA, CSMP, CCTP

Strategic Risk Architect | Co-Founder and Chief Executive Officer
The Risk Management Forum (TRMF)

Published: May 2026

ABSTRACT

This working paper examines the structural and behavioural differences between organisations governed by rule of law principles and those operating within cultures of embedded corruption and personal gain. Drawing on research in organisational behaviour, institutional economics, compliance science, and criminology, the paper argues that the critical distinction between these two environments lies not in the presence or absence of cohesion, but in the *basis* of that cohesion: whether it is anchored in shared institutional norms or consolidated through mutual complicity. The paper identifies four diagnostic domains across which the two environments diverge, and derives a tiered set of early warning indicators applicable to any organisational context. The analysis is situated within the Corporate Strategic Risk Architecture Integrated (C-SRA-I) framework developed by The Risk Management Forum (TRMF), with particular reference to the insider risk transmission model established in WP-2026-004. The Individual Risk Layer (IRL) and Individual Motivation Assessment (IMA) are presented as diagnostic instruments for identifying individual-level transmission pathways. The paper concludes that effective governance intervention must distinguish between surface indicators of stability and the underlying normative logic driving organisational behaviour.

Keywords: *organisational culture, rule of law, corruption transmission, staff cohesion, insider risk, early warning indicators, C-SRA-I, IRL, IMA, compliance, corporate governance*

1. INTRODUCTION

Organisations do not fail because risk exists. They fail because the internal architecture meant to contain risk has been compromised, often before any external measurement confirms it. The most dangerous form of this compromise is cultural: a slow, incremental normalisation of conduct that gradually replaces

institutional norms with informal loyalty networks, and accountability with impunity.

The question of how staff cohesion differs between a rule of law corporate environment and one characterised by embedded malfeasance is not merely academic. For practitioners in governance, risk management, and compliance, it carries direct operational implications. High cohesion has traditionally been regarded as a signal of organisational health. The research base reviewed in this paper challenges that assumption and demonstrates that cohesion itself is diagnostically neutral. What matters is the normative substrate on which cohesion rests.

This paper develops that argument in four stages. Section 2 establishes the definitional and theoretical frame. Section 3 identifies the distinguishing factors across four diagnostic domains. Section 4 derives a tiered framework of early warning indicators. Section 5 situates the analysis within the C-SRA-I framework and identifies the role of the IRL and IMA as diagnostic instruments. Section 6 presents applied implications for governance practitioners and Section 7 concludes.

2. THEORETICAL AND DEFINITIONAL FRAMEWORK

2.1 Defining the Two Environments

For the purposes of this paper, a **rule of law corporate environment** is defined as one in which organisational conduct is governed by codified standards, enforced accountability mechanisms, and a normative culture in which institutional rules are understood to apply consistently regardless of seniority or relationship proximity.

A **corrupt organisational environment** is defined, following Anand, Ashforth and Joshi (2004) and Pinto, Leana and Pil (2008), as one in which organisational power, position, or authority is systematically misused for personal or collective gain, and in which this misuse constitutes a sustained deviation from formal standards and norms. Critically, the literature distinguishes between *organisations of corrupt individuals* and *corrupt organisations*, where the latter implies systemic embedding of corruption in structures, incentives, and cultural norms (Pinto et al., 2008).

The distinction is operationally significant. An organisation of corrupt individuals may be remediated through personnel action. A corrupt organisation requires architectural intervention.

2.2 Corruption as Systemic Deviation

Ashforth, Gioia, Robinson and Trevino (2008) establish that organisational corruption is better understood as a system-level phenomenon than as an aggregation of individual misconduct. Their taxonomy identifies four typologies of corrupt behaviour corresponding to different organisational environments: system malfeasance, procedural malfeasance, categorical malfeasance, and structural malfeasance (Cambridge Core, 2015). This typology maps directly onto the C-SRA-I pillar architecture, which similarly distinguishes between individual, process, structural, and systemic risk transmission channels.

Vardi and Weiner (1996) note that most individuals engage in some form of corrupt acts and misbehaviours at work, and that corrupt behaviours plague all types of work organisations involving non-supervisory and staff personnel alike (ProQuest, 2021). This finding is important because it cautions against the assumption that rule of law environments are simply those in which corrupt individuals are absent. They are environments in which the system itself constrains and penalises corruption, regardless of individual inclination.

2.3 Cohesion: A Diagnostic Ambiguity

Team cohesion is generally understood as the degree to which team members are attracted to the team and motivated to remain part of it (Edmondson, 1999). It is positively correlated with communication, learning, and performance in ethically stable environments. However, Pearsall and Ellis (2011) demonstrated what they termed the *thick as thieves* effect: teams with high utilitarian ethical orientation operating under conditions of psychological safety were significantly more likely to engage in collective unethical behaviour. The shared safety enabled the shared transgression. Cohesion, in a corrupt environment, is bonded by mutual exposure rather than by mutual purpose.

This finding is central to the argument developed in this paper. Governance practitioners who rely on observed cohesion as a health indicator are, in corrupt environments, reading the strength of the informal network rather than the integrity of the institution.

2.4 The Broken Windows Transmission Mechanism

Wilson and Kelling's (1982) broken windows theory, applied to organisational behaviour by subsequent researchers, provides the transmission mechanism linking individual deviation to systemic cultural corruption. Minor rule failures, if unremediated, signal that external controls have degraded, leading to increasingly serious deviant behaviours (Frontiers in Psychology, 2020). The critical organisational implication is that corruption rarely arrives fully formed. It is grown incrementally through the normalisation of progressively larger deviations, each of which recalibrates what is understood to be permissible.

This mechanism is directly relevant to the C-SRA-I Early Warning System (EWS), which identifies structural degradation signals before systemic failure manifests in measurable performance outcomes.

3. DISTINGUISHING FACTORS: FOUR DIAGNOSTIC DOMAINS

The research base identifies four primary domains across which rule of law and corrupt environments diverge. These domains are not mutually exclusive; they interact and reinforce one another. They are presented here as a diagnostic matrix for the purpose of analytical clarity.

3.1 Leadership Architecture and Accountability

In a rule of law environment, leadership is accountable to the institution. Decision authority is exercised within defined parameters, and deviation carries consistent

consequences. This consistency is the institutional signal that rules apply uniformly.

In a corrupt environment, Taylor (2019) observes that leadership is complacent and hierarchical, hoarding information and constructing plausible deniability. Highly hierarchical authority systems host cultures of fear in which employees are reluctant to express concerns (NYU Compliance and Enforcement, 2019). The leadership architecture is designed not to govern conduct but to insulate power.

The Corporate Executive Board's research identifies organisational justice as the single most significant factor in maintaining ethical conduct across an organisation (Sigurdson Post, 2019). Where leadership is visibly exempted from accountability, the normative message to all other staff is that rules are instruments of power, not principles of governance.

3.2 Information Architecture and Knowledge Behaviour

In a rule of law environment, information flows are open, documented, and accessible across functions. Psychological safety, as defined by Edmondson (1999) and extensively validated in subsequent literature, enables individuals to surface concerns, share knowledge, and escalate risk signals without fear of retribution. Ethical leadership is negatively correlated with knowledge hiding, with psychological safety mediating this relationship (ScienceDirect, 2024).

In a corrupt environment, information is a strategic resource. Knowledge hoarding protects individual position. Opacity is structural rather than incidental. Taylor (2019) identifies the deliberate isolation of high-revenue teams from conventional compliance oversight as a characteristic feature of corrupt organisational cultures, noting that such teams evade attention precisely because they command power.

This produces a diagnostic observable: compliance silence. Areas of the organisation that generate no escalations, no whistleblower reports, and no flagged concerns are not necessarily well-governed. They may represent zones of enforced silence.

3.3 Incentive Structures and Normative Reference Points

In a rule of law environment, incentives are designed to reward conduct aligned with institutional norms. Performance targets are bounded by behavioural standards. Misconduct carries a cost that offsets the benefit of the transgression.

In a corrupt environment, incentive misalignment is both a symptom and a cause. Volkov (2026) identifies pressure to 'make the numbers', reluctance to escalate concerns, inconsistent accountability, and tolerance of misconduct as warning signs visible in culture before they appear in financial statements or regulatory actions. When revenue generation is rewarded irrespective of the conduct through which it was achieved, the implicit message recalibrates the normative reference point for all staff.

Ganintegrity (2023) notes that when organisations do not hold offenders accountable for misconduct, it is a body blow to employees' trust, from which it is a short jump to employees making their own judgements about permissible

conduct. The corruption of the normative reference point is how systemic rule deviation begins.

3.4 The Cohesion Differential

This is the domain most frequently misread by governance practitioners and the one most directly relevant to early warning indicator development.

In a rule of law environment, cohesion is centripetal: it draws members toward a shared institutional standard. Disagreement is permissible because it is safe. Escalation is an act of loyalty to the institution. Individuals cohere around norms that exist independently of any particular person.

In a corrupt environment, cohesion is centrifugal in its outward presentation but consolidating in its internal logic. It is built on shared risk. Complicity creates dependency, and dependency creates loyalty. The informal network is held together by the mutual knowledge that exposure of one member exposes all. Taylor (2019) observes that the behavioural dynamics of such teams are unlikely to be detected by conventional compliance processes, and are often the root of ethical and corruption problems precisely because they evade attention.

The diagnostic implication is that high cohesion in a corrupt environment is a lagging indicator, not a leading one. By the time cohesion is observable, the informal network has already consolidated.

Diagnostic Domain	Rule of Law Environment	Corrupt Environment
Leadership	Accountable to institution; consistent standards; transparent decisions	Complacent; hierarchical; information hoarding; plausible deniability
Information Flow	Open; cross-functional; psychological safety enables escalation	Controlled; compartmentalised; silence enforced; knowledge weaponised
Incentive Structures	Conduct and performance co-rewarded; misconduct carries consistent cost	Revenue rewarded irrespective of conduct; accountability selectively applied
Basis of Cohesion	Anchored in shared norms; safe to dissent; escalation is loyalty	Anchored in mutual complicity; dissent is betrayal; exposure is the bond
Normative Reference Point	Institutional rules; codified standards; uniform application	Informal hierarchy; personal gain; rules as instruments of power

Table 1: Diagnostic Domain Comparison — Rule of Law vs Corrupt Environment

4. EARLY WARNING INDICATOR FRAMEWORK

Early warning indicators in the context of organisational corruption are observable signals that precede measurable performance failure, regulatory action, or public exposure. The research base, and the C-SRA-I EWS architecture,

both support a tiered approach in which indicators are classified by proximity to systemic risk crystallisation.

The following framework is structured across three tiers, corresponding to precursor, structural, and active risk stages. These tiers are not sequential in all cases; indicators across tiers can manifest simultaneously.

4.1 Tier One: Cultural Precursors

These are low-signal, high-importance indicators. They are often dismissed as morale issues or management style concerns. Their significance lies in what they signal about the normative trajectory of the organisation.

- Pervasive staff cynicism about stated values. Where employees hold cynical attitudes about management's objectives or ethical commitments, they begin to form independent judgements about permissible conduct (Ganintegrity, 2023). This is the earliest observable precursor of normative drift.
- Visible disconnect between stated policy and observed behaviour. The Volkov (2026) research identifies actions not aligning with words as a primary cultural warning sign. This is particularly significant when the disconnect is most visible at senior levels.
- Compliance investment treated as reputational expenditure. Ganintegrity (2023) identifies the reduction of compliance budgets following regulatory settlements as a clear signal that governance is performative rather than substantive.
- Loss of voluntary ethical reporting. Where staff cease to raise concerns informally, before formal mechanisms are engaged, it signals that the psychological safety required for escalation has been eroded.

4.2 Tier Two: Structural Signals

These indicators suggest that informal networks have consolidated and are actively insulating themselves from oversight.

- Pockets of compliance silence. Taylor (NYU, 2019) identifies areas of the organisation that use whistleblowing lines considerably less than the organisational average, or that produce no reports of concern about leadership whatsoever, as potential zones of enforced silence rather than evidence of good governance.
- Concentration of authority in relationship networks. Where decision-making consistently flows through informal personal relationships rather than through documented governance structures, the formal architecture has been bypassed.
- Selective accountability. Misconduct at senior levels that is addressed less rigorously than equivalent misconduct at junior levels signals that accountability is a function of power rather than of principle.
- Cross-functional isolation of high-revenue units. Taylor (2019) identifies the deliberate distancing of powerful, revenue-generating teams from standard compliance oversight as a structural enabler of embedded corruption.
- Incentive misalignment without remediation. Where performance incentives that reward outcomes irrespective of conduct are identified but not corrected, it signals institutional tolerance of the misalignment.

4.3 Tier Three: Active Risk Crystallisation

These are high-signal indicators that suggest systemic corruption is active and the informal network has achieved sufficient consolidation to resist conventional oversight mechanisms.

- Coordinated resistance to external review or audit. Where teams or units respond to oversight with coordinated information management rather than transparent disclosure, informal network protection is active.
- Ritualised loyalty signalling. Expectations that staff demonstrate alignment through participation in informal rule-bending, however minor, represent the classic onboarding mechanism for complicity networks.
- Formal loyalty structuring around individuals rather than functions. Where staff coalitions form in defence of individuals under investigation or review, rather than in defence of process integrity, the network has crystallised.
- Repeated tolerance of misconduct by high-performing individuals. Whistleblowers Security (2023) identifies failure to penalise individuals involved in ethically or legally questionable behaviour as directly supportive of perpetuation and the development of a culture of impunity.
- Unexplained attrition of ethical staff. Where individuals with strong ethical orientation exit the organisation in concentrated patterns, it indicates that the normative environment has become hostile to rule-consistent behaviour.

Tier	Indicator Category	Observable Signal	Risk Stage
Tier 1	Cultural Precursors	Staff cynicism; policy disconnect; compliance underinvestment	<i>Normative drift / Pre-structural</i>
Tier 2	Structural Signals	Compliance silence; selective accountability; incentive misalignment	<i>Network consolidation / Active insulation</i>
Tier 3	Active Risk Crystallisation	Audit resistance; loyalty rituals; ethical staff attrition	<i>Systemic corruption / Oversight resistance</i>

Table 2: Early Warning Indicator Tier Framework

5. C-SRA-I FRAMEWORK INTEGRATION

5.1 Positioning within the C-SRA-I Architecture

The Corporate Strategic Risk Architecture Integrated (C-SRA-I) framework, developed by The Risk Management Forum (TRMF), provides a five-pillar diagnostic architecture for organisational risk: Governance Architecture and Decision Integrity (P1), Capital Strength and Financial Stability (P2), Organisational Cohesion and Execution Alignment (P3), Operational Risk and Threat Landscape (P4), and Strategic Resilience and Adaptive Capacity (P5). The fifth pillar functions as the central systemic corporate stabiliser into which pressure from the surrounding four pillars ultimately transmits. The analysis presented in this paper is primarily anchored in Organisational Cohesion and Execution Alignment (P3) and Governance Architecture and Decision Integrity (P1), with the individual behavioural dimension captured through the Behavioural

Governance Intelligence layer (IRL and IMA) and transmission implications extending across all five pillars.

The insider risk transmission model established in WP-2026-004, which applied the C-SRA-I architecture to the 1995 Barings Bank collapse, demonstrated how individual behavioural risk transmits through organisational structure to produce systemic failure. The present paper extends that model by identifying the cultural environment as a precondition for transmission: corrupt cultures do not merely tolerate risk transmission; they create the conditions in which it becomes structurally inevitable.

5.2 The Individual Risk Layer and Individual Motivation Assessment

The Individual Risk Layer (IRL) maps individual behavioural orientations across two primary typologies: the Activator and the Disruptor, assessed across seniority tiers and positioned against C-SRA-I pillars. The Individual Motivation Assessment (IMA) draws on Self-Determination Theory (Deci and Ryan, 1985), McClelland's Need Theory (1961), and the Fraud Triangle (Cressey, 1953) to profile the motivational architecture underlying individual conduct.

The research synthesised in this paper confirms a critical implication for both instruments: corrupt environments do not simply recruit Disruptor profiles. They transform Activator profiles over time through normalisation, social proof, and complicity bonding. The broken windows transmission mechanism operates at the individual level as well as the structural level. An individual who enters a corrupt environment as an Activator may, absent effective countermeasures, migrate to Disruptor behavioural patterns as the normative recalibration process advances.

This has direct diagnostic implications. Early warning indicators at Tier One (cultural precursors) are the intervention window within which IRL and IMA diagnostics can identify individuals at risk of normative migration before the migration consolidates. By Tier Three, the informal network has sufficient cohesive strength to resist individual-level intervention.

5.3 Cohesion as a Composite Resilience Index Variable

The C-SRA-I Composite Resilience Index (CRI) synthesises pillar diagnostic scores into a single organisational resilience measure. The analysis in this paper recommends that CRI assessments incorporate a cohesion quality variable: a measure not simply of the degree of cohesion but of its normative basis. An organisation with high cohesion anchored in mutual complicity may score well on surface indicators of engagement and retention while carrying significant systemic risk. The CRI should be stress-tested against the early warning indicators in Section 4 to distinguish genuine resilience from consolidated informal network strength.

6. APPLIED IMPLICATIONS FOR GOVERNANCE PRACTITIONERS

The practical implications of this analysis for governance, risk, and compliance professionals are significant and directly actionable.

Do not read cohesion as a health indicator without qualifying its basis.

High staff cohesion, low attrition, and strong team solidarity are not self-evidently signs of organisational health. Governance practitioners should assess the normative substrate of cohesion: whether it is oriented toward institutional standards or toward informal loyalty networks.

Treat compliance silence as a risk signal.

Areas of the organisation that produce no escalations, no concerns, and no reports should be subjected to enhanced review rather than treated as well-governed. The absence of signal in a high-complexity, high-stakes environment is unlikely to reflect genuine risk absence.

Anchor incentive design in conduct, not only in outcomes.

Incentive structures that reward revenue generation irrespective of the conduct through which it was achieved are not merely an ethics problem. They are a risk architecture problem, because they systematically recalibrate the normative reference point across the entire workforce.

Intervene at Tier One.

The research base consistently demonstrates that by Tier Three, the informal network has achieved sufficient consolidation to resist conventional compliance and governance mechanisms. The early warning indicators at Tier One are the primary intervention opportunity. Organisations that wait for financial statement anomalies or regulatory action have already allowed the informal architecture to harden.

Apply the IRL and IMA diagnostics within the EWS architecture.

Individual-level diagnostics have greatest utility as early-stage tools. The IRL and IMA should be deployed as part of a structured organisational health assessment at Tier One indicator activation, rather than in response to confirmed misconduct.

7. CONCLUSION

This paper has argued that the fundamental distinction between rule of law and corrupt organisational environments is not the presence or absence of cohesion, but the normative basis on which cohesion rests. Where cohesion is anchored in institutional standards, it is an organisational asset. Where it is anchored in mutual complicity, it is an organisational risk multiplier.

The four diagnostic domains identified in Section 3, and the tiered early warning indicator framework in Section 4, provide governance practitioners with a structured analytical lens for distinguishing surface signals of stability from the underlying normative logic that drives organisational behaviour. The C-SRA-I framework, and specifically the IRL and IMA instruments, provide the diagnostic architecture through which these signals can be translated into actionable risk assessments.

The foundational argument unifying all TRMF framework work applies directly here: systems fail from within, and the gap between structural appearance and

operational reality is measurable. The measurement of that gap, in the domain of organisational culture, is the central contribution of this paper.

Future research directions include the development of a validated quantitative scoring instrument for the Tier One to Tier Three indicator framework, and the application of the cohesion quality variable within the C-SRA-I Composite Resilience Index across sector-specific case studies.

REFERENCES

Anand, V., Ashforth, B.E. and Joshi, M. (2004) 'Business as usual: The acceptance and perpetuation of corruption in organizations', *Academy of Management Executive*, 18(2), pp. 39-53.

Ashforth, B.E., Gioia, D.A., Robinson, S.L. and Trevino, L.K. (2008) 'Re-viewing organizational corruption', *Academy of Management Review*, 33(3), pp. 670-684.

Becker, G.S. and Stigler, G.J. (1974) 'Law enforcement, malfeasance, and the compensation of enforcers', *Journal of Legal Studies*, 3(1), pp. 1-19.

Cressey, D.R. (1953) *Other People's Money: A Study in the Social Psychology of Embezzlement*. Glencoe: Free Press.

Deci, E.L. and Ryan, R.M. (1985) *Intrinsic Motivation and Self-Determination in Human Behavior*. New York: Plenum Press.

Du Venage, A. (2026) 'The Insider Within: Applying the Corporate Strategic Risk Architecture Integrated Transmission Model to the Collapse of Barings Bank', TRMF Working Paper WP-2026-004. Johannesburg: The Risk Management Forum.

Du Venage, A. (2026) 'Corporate Strategic Risk Architecture Integrated (C-SRA-I): A Framework for Organisational Risk Governance', TRMF Working Paper WP-2026-003. Johannesburg: The Risk Management Forum.

Edmondson, A.C. (1999) 'Psychological safety and learning behavior in work teams', *Administrative Science Quarterly*, 44(2), pp. 350-383.

Kaufmann, D., Kraay, A. and Mastruzzi, M. (2010) 'The Worldwide Governance Indicators: Methodology and Analytical Issues', World Bank Policy Research Working Paper No. 5430. Washington: World Bank.

McClelland, D.C. (1961) *The Achieving Society*. Princeton: Van Nostrand.

Meadows, D.H. (2008) *Thinking in Systems: A Primer*. White River Junction: Chelsea Green Publishing.

Pearsall, M.J. and Ellis, A.P. (2011) 'Thick as thieves: The effects of ethical orientation and psychological safety on unethical team behavior', *Journal of Applied Psychology*, 96(2), pp. 401-411.

Pinto, J., Leana, C.R. and Pil, F.K. (2008) 'Corrupt organizations or organizations of corrupt individuals? Two types of organization-level corruption', *Academy of Management Review*, 33(3), pp. 685-709.

Senge, P.M. (1990) *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York: Doubleday.

Taleb, N.N. (2012) *Antifragile: Things That Gain from Disorder*. New York: Random House.

Taylor, A. (2019) 'Organizational Culture in Corrupt Companies', *Corporate Compliance Insights*. Available at: <https://www.corporatecomplianceinsights.com/organizational-culture-corrupt-companies/> [Accessed: May 2026].

Transparency International (2023) *Corruption Perceptions Index 2023*. Berlin: Transparency International.

Vardi, Y. and Weiner, Y. (1996) 'Misbehavior in organizations: A motivational framework', *Organization Science*, 7(2), pp. 151-165.

Volkov, M. (2026) 'Culture as Strategy: Why Ethics and Integrity Drive Long-Term Financial Performance', *Corruption, Crime and Compliance*. Available at: <https://blog.volkovlaw.com> [Accessed: May 2026].

Wilson, J.Q. and Kelling, G.L. (1982) 'Broken windows: The police and neighbourhood safety', *The Atlantic Monthly*, March, pp. 29-38.

Intellectual Property and Framework Declaration

The Corporate Strategic Risk Architecture Integrated (C-SRA-I), the Individual Risk Layer (IRL), the Individual Motivation Assessment (IMA), and the C-SRA-I Early Warning System (EWS) are proprietary frameworks originated and authored by Dr André Du Venage, in whom all intellectual property rights are reserved personally. The Risk Management Forum (TRMF) acts as the publishing vehicle for this work and is not the rights holder. © 2026 Dr André Du Venage, DBA, CSMP, CCTP. All rights reserved. No part of this paper or the frameworks described within it may be reproduced, adapted, or applied commercially without the prior written consent of Dr André Du Venage.

Contact: andre@trmf.org.za | www.trmf.org.za | +27 83 463 2047

About the Author

Dr André Du Venage (DBA, CSMP, CCTP) is Co-Founder and Chief Executive Officer of The Risk Management Forum (TRMF) and Managing Director of Secure Logistics (Pty) Ltd. He is the originator and Strategic Risk Architect of the SRA-I, C-SRA-I, Government Delivery Probability Index (GDPI), Individual Motivation Assessment (IMA), and Individual Risk Layer (IRL) frameworks. With over 21 years of experience in risk management and security consulting, Dr Du Venage holds TAPA EMEA Regional Lead status for South Africa. His research focuses on systemic risk, institutional fragility, and the measurable gap between governance architecture and operational delivery.