

Insider Threats Are Governance Failures, Not Human Failures

Insider threats emerge from weak structure, not weak ethics.

A critical misconception in security thinking is the assumption that insider threats are primarily driven by malicious individuals. In reality, most insider incidents are **structural in nature**, not intentional. They arise from organizational designs that concentrate power, grant excessive access, and operate with insufficient oversight.

The TPSRSR model surfaces a fundamental insight: insider risk is rarely about *who* a person is, but about *what the structure allows*. When transparency is limited, duties are not separated, supervision is absent, and reviews are infrequent, even well-intentioned individuals can cause significant harm—often unintentionally.

This perspective reframes insider threat management away from surveillance, suspicion, and mistrust, and toward **governance, role design, and control structures**. Effective mitigation focuses on principles such as separation of duties, access proportionality, supervisory controls, and continuous review.

Most insider incidents are enabled by **concentration of power**, not bad actors. Technology alone cannot correct these conditions; only thoughtful organizational structure can.

“Trust without governance is risk by design.”

