Risk Culture and Governance

Risk Culture and Governance

1. **Definition of Risk Culture**
    - The shared values, attitudes, and behaviors within an organization that shape how risk is understood and managed at every level.
2. **Tone at the Top**
    - Leadership's visible commitment to risk management strongly influences whether risk culture is taken seriously throughout the organization.
3. **Risk Governance Structure**
    - Typically includes a board risk committee, a Chief Risk Officer (CRO), and clearly defined risk ownership across business units.
4. **Three Lines of Defense Model**
    - **First line**: operational management owns and manages risk day-to-day.
    - **Second line**: risk management and compliance functions provide oversight and challenge.
    - **Third line**: internal audit provides independent assurance.
5. **Signs of a Weak Risk Culture**
    - Risks being hidden or downplayed, lack of accountability, and risk management seen as a "box-ticking" exercise rather than integral to decision-making.
6. **Why It Matters**
    - Even the best ERM framework fails without a genuine risk-aware culture - governance structures and processes only work if people actually follow their spirit, not just their letter.