2025/01/28

THE PLAYBOOK: UNDERSTANDING CGRC IN THE REAL WORLD

In the business environment, the acronym "GRC" is everywhere yet it often feels like corporate jargon, abstract and complex. At its core, GRC (Governance, Risk, and Compliance) is the consolidated structure that allows an organisation to operate effectively.

Cyclopedic Consulting incorporates Conduct Risk as a fundamental component to the GRC function, aligning an organisation's strategy with its most important asset, the people.

A. Governance: The Driver

Governance is the foundation, that is the framework of rules, practices, and processes that direct and control an organisation. It answers the questions: Where are we going, who decides and how do we get there?

Key components include:

- Policies & Procedures: The organisational "rulebook."
- Organisational Structure: Who reports to whom.
- Leadership & Board: The captains that set the journey.
- Ethical Standards: The moral compass.
- Performance Metrics: The scorecards and tracking progress.

Governance ensures everyone knows the play, their position, and the goal.

B. Risk Management: The Weather Forecast & Wind Shield Wipers

Risk Management is the proactive process of identifying, assessing, and controlling threats to an organisation's capital, earnings, and operations. Its purpose is not to eliminate the risk, which is often impossible, but to managing it intelligently.

It involves:

- Risk Identification: Spotting potential storms on the horizon.
- Risk Assessment: Determining how severe those storms could be.
- Risk Avoidance/Mitigation: Staying indoors or functional windscreen wipers.
- Risk Monitoring: Eyes on the road, puddles hide potholes.

Risk Management answers: What could go wrong, How to handle it? Be prepared, not scared.

C. Compliance: The Rulebook and Enforcer

Compliance ensures an organisation adheres to external laws, regulations, and internal policies. It's the confirmation that you're playing by the rules.

Key functions include:

- Regulatory Tracking: Knowing all the applicable rules.
- Monitoring & Testing: Continuously checking for adherence.
- Reporting & Documentation: Proving you followed the rules.
- Remediation: Fixing rule violation issues when they arise.

Compliance is doing what you are permitted or required to do by following the rules, highlighting and correcting deviations.

How They Work Together:

- Governance is the driver, the map, and the destination. You decide where to go (strategy), choose the route (policies), and control the steering wheel (decision-making).
- Risk Management is your awareness of road conditions and weather. You check reports (risk assessment), slow down in the rain (risk mitigation), and wear a seatbelt (control).

- Compliance is traffic laws and vehicle regulations. You obey speed limits, pass regular inspections, and have a valid license. The police (auditors) ensure you're following the rules.

All three must work in unison for a safe, efficient, and successful journey.

Great governance sets the right destination, risk management navigates the terrain, and compliance ensures you have the legal right to drive.

The Bottom Line

- Governance = WHERE we're going and WHO decides.
- Risk = WHAT could go wrong and HOW we prepare.
- Compliance = RULES we must follow and PROOF we did.

When integrated deliberately, GRC provides clarity, certainty, and competence. It's the difference between a smooth, strategic journey and one riddled with preventable accidents, costly fines, and dead ends.

D. Conduct Risk in the GRC cycle

Conduct risk is a vital and evolving concept that doesn't fit neatly into just one letter of the GRC triad; it is woven through all three, acting as both a specific risk category and a cultural outcome of the entire framework.

1. As a Specific Category of RISK

At its core, conduct risk is the risk that individual or collective human behaviours within an organisation will cause harm to customers, market integrity, or the organisation itself.

In the Risk Register: It is a discrete risk category (like operational, credit, or market risk) that must be identified, assessed, mitigated, and monitored.

- Examples: Mis-selling products, market manipulation, abusive sales practices, conflicts of interest, unethical decision-making, or fostering a toxic organisational culture that drives instability or misconduct.

Conduct risk is a specific type of "storm" that originates inside the car (the organisation) due to human actions, rather than an external "weather" event.

2. As an Outcome and Test of Governance

Governance sets the tone from the top, which is the single most important factor in managing conduct risk.

- Culture & Ethical Standards: Governance is responsible for establishing the ethical framework and culture that either encourages or suppresses poor conduct. A weak governance framework that prioritises short-term profits over TCF is a direct enabler of conduct risk.
- Incentive Structures (Performance Metrics): Perhaps the most direct link. If governance sets sales targets and compensation schemes (the "scorecards") that are excessively aggressive without proper controls, it actively creates conduct risk. Governance must design incentives that reward the right behaviour, not just the bottom-line outcomes.
- Accountability: Strong governance ensures clear accountability for conduct at all levels, especially in senior leadership.

3. As a Primary Driver of Compliance obligations

In many industries (especially financial services), conduct risk has become a major focus for regulators, transforming it from an internal concern into a heavy compliance burden.

- New Rulebooks: Legislation like Conduct of Financial Institutions COFI Act (Bill), is essentially a compliance framework built to mitigate conduct risk.
- Monitoring & Reporting: Compliance functions must now implement specific controls to monitor for conduct and report on conduct metrics to regulators.
- Regulators are less interested in only whether you have a license (a static compliance check) and intensely interested in how your organisational culture could lead to e.g. conflicts of interest (conduct risk). They audit for both rules and behaviour.

Integrated GRC Cycle with Conduct Risk

Using the Car Analogy, Conduct Risk is:

- A GOVERNANCE failure if the driver (leadership) encourages speeding or ignores reckless behaviour in the car.
- A key RISK that the passengers (employees) might act recklessly, causing an accident.
- A COMPLIANCE focus; traffic laws (regulations) specifically penalise "aggressive driving" (poor conduct) and hold the driver accountable for the passengers' actions.

Conduct risk is the human element of GRC, it is in every aspect.

- It is a Risk to be managed.
- It is a direct product of Governance (culture and incentives).
- It is a primary subject of Compliance and regulation.

A mature GRC framework recognises that conduct risk cannot be controlled by rules (compliance) alone. It requires the right culture (governance) to be actively managed (risk).

Conduct, Governance, Risk, Compliance (CGRC) with conduct being both an input and output of the entire system.

By **Adv. Sannah Pooe** 2026/01/28