The Institute of Internal Auditors Australia

Factsheet: GRC

What is GRC?

GRC is an acronym for Governance Risk Compliance. Research published in 2007 by Scott L Mitchell defined GRC as:

> *The integrated collection of capabilities that enable an organisation to reliably achieve objectives, address uncertainty and act with integrity.*

GRC relates to integrating activities designed for organisations to be well-governed with an effective assurance environment and compliance focus.

What are GRC Components?

Each of the three GRC components has its own definition:

> *Governance – The combination of processes and structures implemented by the board to inform, direct, manage and monitor the activities of the organisation toward achievement of objectives.*

> *Risk – Anticipating and managing the uncertainties that affect organisation performance.*

> *Compliance – Fulfillment of an obligation, while non-compliance is non-fulfilment of an obligation – obligations may be externally imposed or may be aspirational and a voluntary undertaking.*

What does GRC Look Like?

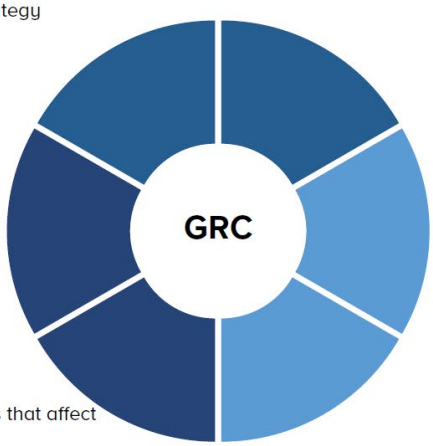
Though GRC is a widely discussed concept, there is not a lot of reference material that directly relates to it. Neither is there much in the way of descriptive models to diagrammatically show how GRC might be structured.

The IIA-Australia designed the following diagram to demonstrate what a GRC model might look like, though every organisation would need to consider its own circumstances when considering an appropriate GRC model.

Governance

The combination of processes and structures implemented by the board to inform, direct, manage and monitor the activities of the organisation toward achievement of objectives

- Board of directors (governing authority)
- Mission, vision, values, objectives, strategy
- Corporate governance framework
- Board sub-committees
- Management committees
- Learning, development
- Integrated assurance
- Feedback, improvement
- Internal audit



Compliance

Fulfillment of an obligation, while non-compliance is non-fulfilment of an obligation – obligations may be externally imposed or may be aspirational and a voluntary undertaking

- Compliance framework – laws, regulations, policy
- Health, safety, environment
- Project management office
- Corporate social responsibility
- Annual report and performance reporting
- Management systems

Risk

Anticipating and managing the uncertainties that affect organisation performance

- Strategic risk management, risk appetite, risk culture
- Operational risk management
- Cybersecurity, ICT governance, ICT security
- Information security
- Culture, ethics, code of conduct
- Anti-fraud and corruption
- Resilience program – business continuity, crisis management, emergency response, disaster recovery
- Monitoring and review of the organisation's environment and performance

What is 'Principled Performance'?

Scott L Mitchell described GRC as 'principled performance' which the OCEG (Open Compliance and Ethics Group) website says is:

> *Principled performance translates corporate goals into individual, team, department and divisional goals. It helps to clarify corporate goals. It is a continuous and evolutionary process in which performance improves over time.*

The OCEG describes the '3 pillars of principled performance' as needing to 'be strong enough to hold up your organisation'.

The 3 Pillars of Principled Performance

Principled Purpose

A principled purpose is perhaps the most basic starting point for principled performance. Defining your highest purpose via mission, vision and values guide everything the organisation does.

Principled People

Leadership, the workforce and extended enterprise must comprise principled people who have strong character and who consistently direct their energies toward a principled purpose.

Principled Pathway

Break down silos and leverage common capabilities in every key system that keeps an organisation on track including governance, strategic management, performance management, risk management, compliance management and audit management systems.

10 Universal Outcomes of Principled Performance

Achieve business objectives	Ensure that all parts of the organisation work together toward the achievement of enterprise objectives.
Ensure risk aware setting of objectives and strategic planning	Provide timely, reliable and useful information about risks, rewards and responsibilities to the governing authority, strategic planners and business managers responsible for execution at all levels.
Enhance organisational culture	Inspire and promote a culture of performance, accountability, integrity, trust and communication.
Increase stakeholder confidence	Grow stakeholder trust in the organisation.
Prepare and protect the organisation	Prepare the organisation to address risks and requirements while protecting the organisation from adversity and surprise and enabling it to grasp opportunities.
Prevent, detect, and reduce adversity and weaknesses	Establish actions and controls to prevent negative outcomes, reduce impact, detect potential problems and address issues as they arise.
Motivate and inspire desired conduct	Provide incentives and rewards for desirable conduct, especially in the face of challenging circumstances.
Stay ahead of the game	Learn information necessary to support quick changes in strategic and tactical direction while avoiding obstacles and pitfalls.
Improve responsiveness and efficiency	Establish capabilities that make the organisation as a whole more responsive and efficient so that it has a competitive advantage.
Optimise economic return and values	Allocate human and financial resources in a way that maximises the economic return generated for the organisation while maximising its values.

Why Focus on GRC?

GRC comprises non-core business activities that represent a necessary cost to organisations. As such, it is important to ensure there is sufficient GRC coverage that is fit-for-purpose and also cost-effective. This means organisations should:

- Maintain effective GRC reporting and oversight.
- Synchronise governance reach and information.
- Align GRC endeavours with the organisation's vision, mission, values and strategies.
- Share information across governance, risk and compliance activities, and with the internal audit function.
- Assess governance coverage and effectiveness against key organisation strategies, risks, business drivers and assurance requirements.
- Ensure there is a comprehensive risk and assurance process.
- Minimise duplication of effort.
- Identify governance gaps and take steps to close them.
- Minimise governance and assurance cost, while optimising efficient, effective and ethical compliance coverage.
- Provide comfort to stakeholders about the quality of governance and assurance.
- Help to understand where overall governance and assurance roles and accountabilities reside.
- Identify skills required to deliver appropriate governance and assurance, as a guide to resourcing.

Where should GRC Live?

To be effective and maintain a measure of independence, GRC should ideally be separate from business operations and located in an area where few audit and assurance activities are performed.

For that reason, it would generally be positioned as a separate governance entity under the leadership of a governance director, chief legal officer or company secretary.

It should also be remembered that GRC is a framework, meaning all elements do not necessarily need to be positioned under one discrete entity. For example, compliance may be a separate entity which is now being seen by organisations as requiring independence similar to internal audit with functional reporting to the audit committee and administrative reporting to the chief executive officer.

Are there GRC Systems?

These days there is a variety of automated GRC software products available on the market that may incorporate such things as:

- Corporate governance.
- Enterprise risk management, risk analysis, risk registers.
- Legal compliance.
- Policy management and compliance.
- Business continuity management.
- Incident management.
- Health and safety management.
- Environmental management.
- Audit management.
- Records management.
- Claims management.
- Training.
- Feedback surveys.
- Monitoring and follow-up of non-conformances and audit recommendations.
- Standards compliance such as:
  - ISO 9001 Quality management systems.
  - ISO 10002 Complaint handling.
  - ISO 14001 Environmental management.
  - ISO 22301 Business continuity.
  - ISO 27001 Information security.
  - ISO 37301 Compliance.
  - ISO 45001 Health and safety.

Other Ideas

A series of compliance-related White Papers authored by Nigel Dalton-Brown and published by the IIA-Australia suggests GRC could be supplemented by O for Obligations to form a GORC model. The author suggests there is an issue with the usual GRC approach – it excludes obligations and introduces a risk-centric bias. Risk management is concerned with managing uncertainties whereas obligations are already known.

A model offered by the OCEG is GRACE–IT:

GRACE-IT					
G	**R**	**A**	**C**	**E**	**IT**
Governance and strategy	Risk Management	Internal Audit	Compliance Management	Ethics and Culture	Information and Security

Useful References

Mitchell, S. L., 2007. GRC360: A framework to help organisations drive principled performance. International Journal of Disclosure and Governance, Oct, 4(4), pp. 279-296.

OCEG, n.d. Ultimate Resource for Governance Risk and Compliance (GRC). [Online]
Available at: oceg.org

The Institute of Internal Auditors - Australia, 2019. The 20 Critical Questions Series: What Directors should ask of Assurance. [Online]
Available at: https://iia.org.au/sf_docs/default-source/technical-resources/20-critical-questions/20-questions-directors-should-ask-of-assurance.pdf

The Institute of Internal Auditors - Australia, 2019. The 20 Critical Questions Series: What Directors should ask of Corporate Governance. [Online]
Available at: https://iia.org.au/sf_docs/default-source/technical-resources/20-critical-questions/20-questions-directors-should-ask-of-corporate-governance.pdf

The Institute of Internal Auditors - Australia, 2020. Factsheet: Corporate Governance. [Online]
Available at: https://iia.org.au/sf_docs/default-source/technical-resources/2018-fact-sheets/corporate-governance.pdf

The Institute of Internal Auditors - Australia, 2020. Factsheet: Corporate Governance Responsibility Matrix. [Online]
Available at: https://iia.org.au/technical-resources/knowledgeitem.aspx?ID=345

The Institute of Internal Auditors Inc, 2017. International Professional Practices Framework. Lake Mary, FL, USA: Internal Audit Research Foundation.