Factsheet: The relationship between Assurance and GORC in plain English

What is GRC?

The acronym GORC stands for:

- Governance.
- Obligational awareness.
- Risk management.
- Compliance administration.

It is a shorthand for the discipline inherent in establishing formal compliance management processes in an organisation. These formal processes are an important part of the assurance that a board of directors[1] needs from its organisation.

What is Governance?

Governance refers to the way in which an organisation is controlled – the organisation may be a company, a division or department (part of an organisation) or even a contract. Governance involves determination of priorities, objectives, strategies and accountability within the context in which an organisation is established. In any organisation, many constraints are inherited from the context in which it operates – divisions or departments of organisations inherit much of their context from the overall parent organisation.

The Institute of Internal Auditors (IIA) has defined governance as

> *The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organisation toward the achievement of its objectives. (International Internal Auditing Standards Board, 2016)*

Other definitions, used in different contexts, are materially consistent with this definition[2].

What are Obligations?

ISO 37301:2021 'Compliance management systems – Requirements with guidance for use' defines obligations as:

> *Requirements that an organisation mandatorily has to comply with as well as those that an organisation voluntarily chooses to comply with.*

Obligations relate very closely to objectives – they are concrete expressions of things an organisation is to achieve. For example, getting certified to ISO 9001:2015 'Quality management systems – Requirements' while not being a legal requirement, is a voluntary business practice that an organisation can strive to achieve.

What is Risk Management?

AS ISO 31000:2018 'Risk management – Guidelines' defines risk management as:

> *Coordinated activities to direct and control an organisation with regard to risk.*
>
> where risk is:
>
> *effect of uncertainty on objectives.*

Risk management uses tools like scenario planning, risk matrices, hierarchy of controls and bowtie diagrams to identify and analyse risk so appropriate controls (plans, processes, procedures) can be put in place to manage risks. For example, a business continuity plan is a control put in place to manage the consequences of a loss of critical services.

Organisations develop controls, for example plans / processes / procedures to manage uncertainties associated with meeting obligations.

What is Compliance?

Compliance is the process of making sure an organisation and its members fulfill an organisation's obligations. If there is a robust system of compliance administration in place, the level of compliance can be measured.

How does Compliance Administration fit into this?

Compliance administration is the collection of documentary evidence showing that the controls defined by good governance, mandatory and voluntary obligations and risk management are being followed. In addition, good compliance management calculates the level of compliance and reports back to management and the board.

[1] The term 'board' is used in the IIA's International Standards for the Professional Practice of Internal Auditing to represent the individual or group ultimately responsible for the performance of an organisation. Other sources refer to 'those charged with governance'. It may be a board of directors or in other contexts a group of trustees or an individual accountable authority.

[2] See Definitions of 'Governance' at end of this Factsheet

Assurance

One dictionary definition of assurance is:

> *A positive declaration intended to give confidence.*

It might also be regarded as a process designed to achieve and to confirm achievement of particular objectives.

In business terms:

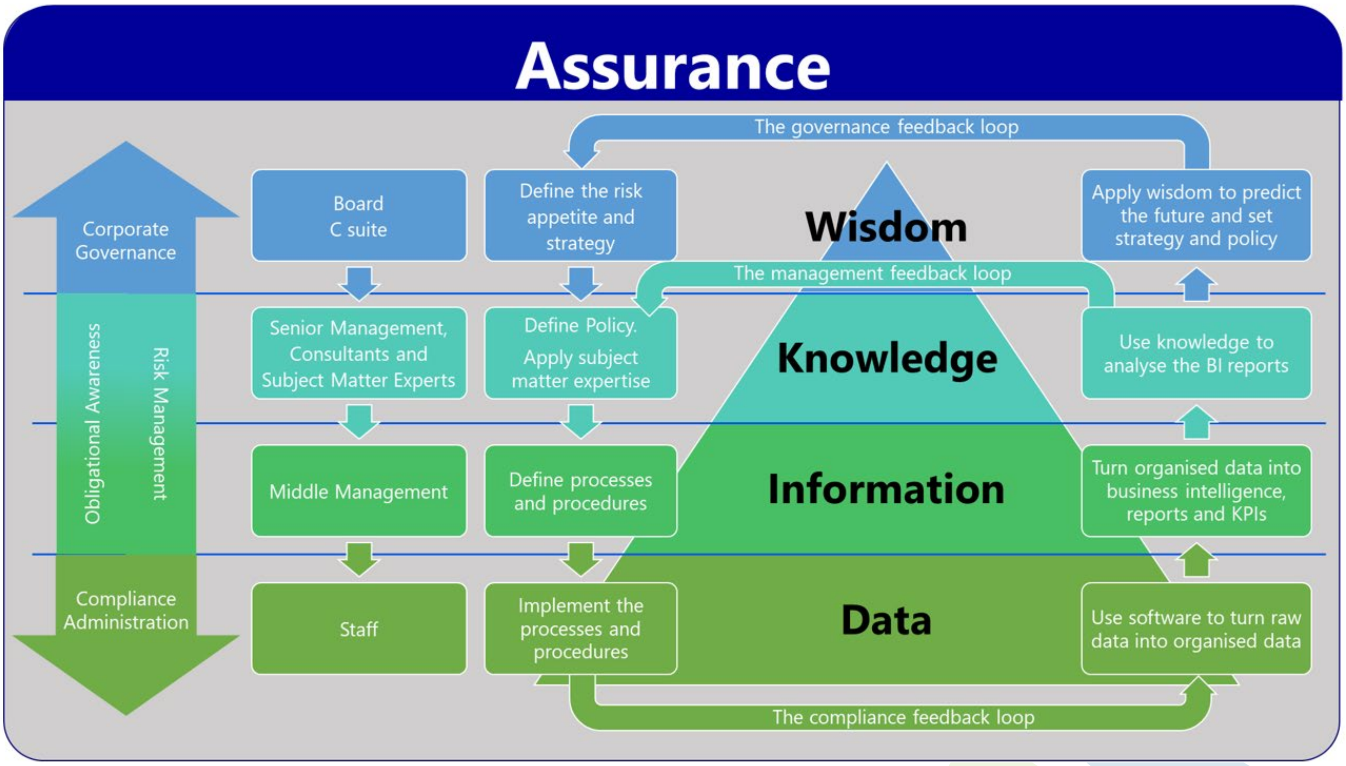
- Directors seek assurance the business is not insolvent and is meeting all its obligations.
- Shareholders seek assurance the business is solvent and meeting its strategic objectives.
- Employees seek assurance they will still be alive at the end of their working day and their work environment will be clean and safe.
- The community seeks assurance the local environment will not be damaged.
- Society seeks assurance the organisation behaves ethically.
- All levels of government seek assurance all relevant laws are being upheld.
- Creditors seeks assurance they will be paid.
- Customers seek assurance goods will be delivered and are of the right quality.

So, how do organisations provide this assurance or promise? They provide it through:

- a system of good **governance** that is aware of all the organisation's mandatory and voluntary **obligations** and
- the ability to manage **risks** and
- an effective **compliance** administration system that confirms the controls imposed above are being met.

How to explain Assurance and GORC?

In simple terms, 'good' and effective GORC provides stakeholders with **assurance** that all of an organisation's obligations are being met.


Assurance
The governance feedback loop
Corporate Governance
Obligational Awareness
Risk Management
Compliance Administration
Board C suite
Define the risk appetite and strategy
Wisdom
Apply wisdom to predict the future and set strategy and policy
The management feedback loop
Senior Management, Consultants and Subject Matter Experts
Define Policy. Apply subject matter expertise
Knowledge
Use knowledge to analyse the BI reports
Middle Management
Define processes and procedures
Information
Turn organised data into business intelligence, reports and KPIs
Staff
Implement the processes and procedures
Data
Use software to turn raw data into organised data
The compliance feedback loop

Assurance is the outcome of good GORC.

Alternative Definitions for Governance

The International Organization for Standardisation (ISO) defines governance as *the system of directing and controlling* or *principles, policies and framework by which an organisation is directed and controlled.*

The Organisation for Economic Co-operation and Development (OECD) defines corporate governance as *a set of relationships between a company's management, its board, its shareholders and other stakeholders........provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.*

The Australian Stock Exchange (ASX) defines corporate governance as *the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations – it encompasses the mechanisms by which companies, and those in control, are held to account.*

The Australian Institute of Company Directors (AICD) defines corporate governance as *the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations.*

The Governance Institute of Australia (GIA) definition of governance *encompasses the system by which an organisation is controlled and operates, and the mechanisms by which it, and its people, are held to account and whole-of-organisation governance as a principles-based approach to good governance from the board through management to the whole organisation in order to achieve strategic objectives.*

All these definitions are materially similar and reflect the responsibility of the governing body and all levels within an organisation.

Useful References

Dalton-Brown, N., 2021. *White paper: GORC – the new and improved GRC, with added O.* [Online] Available at: https://iia.org.au/sf_docs/default-source/technical-resources/2018-whitepapers/iia-whitepaper_gorc-the-new-and-improved-grc-with-added-o.pdf

International Internal Auditing Standards Board, 2016. *International Standards for the Professional Practice of Internal Auditing*, Lake Mary, FL, USA: Internal Audit Foundation.

International Organization for Standardization, 2018. *ISO 31000:2018 Risk managment - Guidelines*, Geneva: International Organization for Standardization.

International Organization for Standardization, 2021. *ISO 37000:2021 Governance of organizations - Guidance*, Geneva: International Organization for Standardization.

International Organization for Standardization, 2021. *ISO 37301:2021 Compliance management systems — Requirements with guidance for use*, Geneva: International Organization for Standardization.