Operational GRC: Naming a dangerous, many headed beast

by **NIGEL DALTON-BROWN FGIA** *Founder and CEO, Strytex*

- Operational GRC is often overlooked but it is just as important as financial GRC and potentially carries more risk.
- Operational GRC is accountable to a wide range of local and national regulators, making compliance complicated and challenging.
- There is no standardised position or team within an organisation to oversee operational GRC and take ownership of operational compliance.

Board members, directors, managers and persons conducting a business or undertaking (PCBUs) are all coming under increasing threat of legal action from non-financial legislation covering areas such as: corporate manslaughter, chain of responsibility (CoR), workplace health and safety (WHS) and so on. These non-financial events have the potential to attract legal action and cause severe brand damage, so why is so little attention being paid to them? The purpose of this article is to raise awareness of non-financial risks by coining the term 'operational [governance, risk and compliance] GRC' (OpGRC) to elevate it to the same level of awareness and attention as financial GRC.

Too long, didn't read

Financial GRC is easy; it's well understood. There are only a handful of regulations and regulators and they are all national. Tertiary qualifications are well recognised, and accountants and bookkeepers are

readily-available. It's so well organised and understood that every size of business uses a single financial software package and there is always a single person or department dedicated to finance.

OpGRC is completely different. There are thousands of standards and multiple regulators across all levels of government. OpGRC does not have the same level of academic maturity as FinGRC. There is no homogenous OpGRC tertiary qualification and no homogenous group of skilled, trained OpGRC professionals. There definitely isn't a single piece of software and no single position or department that encompasses the entirety of OpGRC.

GRC has become a shorthand for financial governance, risk and compliance and this focus is exposing organisations, board members, executives, managers and PCBUs to very real personal risks of fines and jail sentences. The first step is to recognise and name the problem, which is why this article proposes splitting GRC into FinGRC and OpGRC, so that organisations can use a completely different set of subject matter experts for OpGRC.

We recommend organisations structure their GRC teams in the same way that the core of the C-suite consists of a chief executive officer (CEO), a chief financial officer (CFO) and a chief operating officer (COO). The GRC team needs to be led by a senior GRC manager supported by a financial GRC manager and an operational GRC manager. (Figure 3)

> When the [board] discussion turns to operational issues... most executives are unaware of the potential risks and have little idea of the organisation's governance and risk prevention controls

What is OpGRC?

The conversation about GRC at board or C-suite level invariably begins by focussing on financial and sustainability issues. When the discussion turns to operational issues like property, suppliers or food safety, most executives are unaware of the potential risks and have little idea of the organisation's governance and risk prevention controls in these areas.

One board member said that the only time they want to discuss operational risk is when something has happened, or when there is a lot of press attention on a subject: 'I just want to know what happened and what's been put in place to stop it from happening again'. Imagine if we applied this approach to financial reporting.

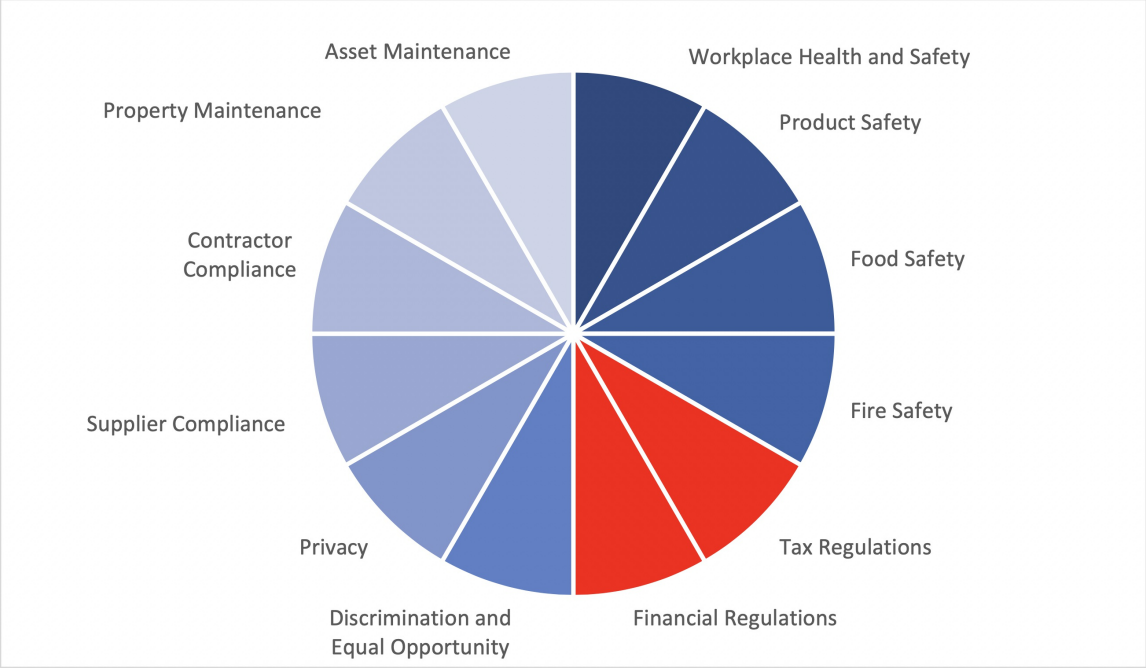
OpGRC is a vast topic that covers non-financial GRC issues like:

- WHS
- property assurance
- fire safety
- asset maintenance
- food safety
- product safety
- supply chain
- data privacy.

Many of these issues, like WHS and duty of care, are themselves deeply complicated. OpGRC also includes associated topics, like:

- asset maintenance to ensure a safe environment and that equipment is safe-to-use
- fire safety across the property portfolio to ensure that, in the event of a fire, everyone survives
- safety of foods provided by the organisation and consumed by staff, visitors and contractors, including the kitchenette in the office
- test and tag to ensure the equipment used by staff, visitors and contractors is safe-to-use
- anti-bullying and anti-discrimination policies, to ensure a safe working environment.

Figure 1: OpGRC issues far outweigh FinGRC issues:



What are the key differences between OpGRC and FinGRC?

Most organisations view OpGRC either as a mythological beast that won't affect them, or as a dangerous beast that's too difficult to tame. The bad news is that OpGRC is real and needs to be tamed. To get to grips with this huge untamed beast, we first need to understand it. The best way to do this is to compare it to FinGRC, a mature and well-tamed beast.

OpGRC has hundreds of regulators

FinGRC has a handful of national regulators, as follows:

- Australian Securities and Investments Commission (ASIC)
- Australian Competition and Consumer Commission (ACCC)
- Australian Prudential Regulatory Authority
- Australian Taxation Office
- Australian Securities Exchange
- Australian Transaction Reports and Analysis Centre.

OpGRC has a few national regulators and hundreds of state and local government regulators. The national regulators are as follows:

- Office of the Australian Information Commissioner
- *Food Standards Australia NewZealand*
- Therapeutic Goods Administration
- ACCC (for product safety)
- IP Australia
- Australian Skills Quality Authority
- Aged Care Quality and Safety Commission.

The state regulators, or areas that are regulated at a state level, include the following:

- WorkSafe/Safework
- Working with Children
- plumbers' licences
- electrical licences
- liquor licences
- painting licences (in New South Wales painting is a trade and is licensed)
- food safety (meat and seafood)
- food safety (dairy)
- building regulations
- locksmiths
- environmental protection
- plant item design and registration.

In addition, local government can require multiple certificates of registration and that an organisation holds certain permits, as well as carrying out audits at random.

There are thousands of acts, regulations and standards relevant to OpGRC, compared to relatively few for FinGRC, as well as a plethora of state regulators.

OpGRC has thousands of acts, regulations and standards

There are thousands of acts, regulations and standards relevant to OpGRC, compared to relatively few for FinGRC, as well as a plethora of state regulators. Consider the organisation where you work: you probably work in an office building. Do you know which acts, regulations and standards apply to your workplace, let alone the WHS ramifications? The Facility Management Association of Australia has compiled a list of over 369 design and maintenance standards. When asked for a list of the mandatory documents required for any building, one facility management expert joked that they would tackle world hunger first, as that would be a lot easier!

If you operate nationally, you have to be aware of the minor differences between the states. In New South Wales the annual fire safety statement can only be signed off by an accredited and competent person. In other states, like Victoria, the annual regulatory statement can be signed off by the building owner. To make things even more complicated, some states do not even require an annual statement.

The situation is so bad that according to Deloitte:

> *Not even the federal government knows how many rules you are meant to obey. In fact, we don't even know how many government bodies currently have the ability to set rules in the first place, let alone the number of rules those agencies have laid down.* [1]

Acts, regulations and standards are only 40 per cent of the problem

In the report referenced above, Deloitte noted that over 60 per cent of the rules governing OpGRC are rules that the private sector has inflicted on itself: public sector regulations are only 40 per cent of the problem. Almost every industry has non-statutory 'accepted practices' and every organisation has multiple procedures and processes that should be followed, and forms that should be completed.

For example, liability insurance is not a statutory requirement, however most organisations, to reduce their risk, require all suppliers to have public and professional, or product liability insurance. To comply, suppliers must submit proof, that is, a certificate of currency, with every invoice, or on an annual basis.

OpGRC has a bewildering range of document expiry periods

The vast majority of FinGRC documents are filed as a one-off, or on a monthly or annual basis. For example, monthly financial reports or annual reports. In contrast, not only does OpGRC have to cope with documents expiring every few hours to every 30 years, it also has to cope with multiple expiry periods for individual assets. For example, food safety requires that food temperatures are recorded at least three times a day: at breakfast, lunch and dinner. The temperature of fridges and freezers must be recorded at least twice a day, the temperature of food deliveries must be checked on a random basis and cleaning schedules must be completed daily.

Under AS1851-2012, fire extinguishers must be checked every six months, every year and every five years. If there are hundreds of fire extinguishers across an entity's properties, it's relatively easy to track the six-monthly and yearly maintenance requirements. It gets a lot harder for the five-yearly checks, because all the fire extinguishers were installed or replaced at various times of the year and in different years. AS1851 – Routine service of fire protection systems and equipment is another statutory obligation, which includes a wide range of maintenance periods, shown in Figure 2.

Figure 2: AS1851 maintenance periods:

2012 (latest version)	2005 (still valid)
Monthly	Weekly
Three-monthly	Monthly
Six-monthly	Three-monthly
Yearly	Six-monthly

2012 (latest version)	2005 (still valid)
Every five years	Yearly
Every ten years	Every three years
Every 25 years	Every five years
Every 30 years	Every 12 years
	Every 24 years

Thousands of qualifications, accreditations, certificates, licences and permits

FinGRC has a small number of clearly defined and nationally recognised qualifications, accreditations and job titles. Accountants are Chartered Accountants, Certified Practising Accountants or Public Accountants and have to be accredited by either Chartered Accountants Australia and New Zealand, CPA Australia or the Institute of Public Accountants respectively. In order to become accredited by one of these bodies, an accountant must have a recognised tertiary qualification, either a diploma or a university degree. Even bookkeepers require a qualification, such as a Diploma in Accounting or a Certificate IV Accounting and Bookkeeping. If they provide BAS services, they must be registered with the Tax Practitioners Board.

OpGRC has no such consistent structure in place. There are few bachelors or masters degrees in governance, risk or compliance and even when there is a module within a law, commerce or business degree, the focus is on FinGRC. Anyone can become a facility manager, and most small-to-medium-enterprise (SME) business managers get tasked with the responsibilities of the role and have to learn on the job. If they are lucky, their employer pays for a course at a registered training organisation (RTO). To fill this gap, many professional bodies are setting themselves up as RTOs and developing their own courses. The worrying part about this is that these business managers are unwittingly exposing themselves to the threat of prosecution when something goes wrong. For example, in your organisation, which qualifications does your de facto facility manager hold? Are they fully aware of all the regulations and polices that must be followed to provide a safe environment for your staff, visitors and contractors?

Often those holding this position are unclear about what they should be doing.

OpGRC has no clear, recognised C-suite representation or organisational structure

In almost every organisation there is a chief financial officer (CFO), who manages a financial department staffed with financial controllers/management accountants, internal auditors, cost accountants, staff accountants and bookkeepers. Financial services firms may also include forensic accountants, tax accountants, auditors and so on.

OpGRC rarely has a centralised department or a responsible C-suite executive or senior manager. There are more chief risk officers and chief compliance officers at large corporates, but their focus and responsibility is still mainly financial, with WHS and cyber risk, including privacy, beginning to be included.

Finance uses a single software platform; OpGRC is fragmented

Every organisation in the world standardises its finances on a single financial management software system. Corporates and large organisations use solutions like SAP, Oracle or Microsoft and SMEs generally use Xero, Freshbooks, Quicken, Zoho and so on. Multinationals often standardise their global financial reporting on a single platform.

There aren't any similar software programs that can manage every type of OpGRC requirement. Organisations, if they have any, generally have separate platforms for risk management, contract management, contractor management, supplier management, WHS, facility management and so on, none of which talk to each other, so data is duplicated, and no one knows which information is the latest.

OpGRC has a lack of hierarchy, which leads to a skills mismatch

There is often a large skills mismatch in OpGRC. Large organisations do not task the CFO, corporate or company accountants with the data entry of receipts or invoices of purchase orders, yet senior procurement managers and senior contract managers are often tasked with chasing suppliers for compliance certificates.

Because there is little to no visibility of OpGRC, there is no clear hierarchy. In the finance department, from the top down, the CFO and senior management set the strategy and policy; middle management develop the procedures required by the policies and the clerks and bookkeepers implement the procedures, ensuring they are followed. From the bottom up, the clerks and bookkeepers enter the data, middle management use their knowledge to produce the relevant reports and the CFO and senior management apply their wisdom to analyse the reports. This system all works because everyone from the CFO to the bookkeeper is trained in finance.

In OpGRC, we find that data collection (paper-chasing) is handled in one of the following ways:

- managed by the senior manager, who has been hired for their wisdom and knowledge, not for their administrative skills
- delegated to the most junior person possible who has no real understanding of the potential risk of non-compliance. This means that certificates are not kept up-to-date and audits are difficult
- unsuccessfully delegated, so that nothing is kept up-to-date, meaning that when the auditor visits, the business is shut down.

Penalties and prosecutions

Under the new ASIC regime, the maximum civil penalties for non-compliance relating to OpGRC are a$1.05 million fine for individuals and up to 15 years in jail and a $10.5 million fine for entities, or 10 per cent of the entity's turnover. Under the latest industrial manslaughter legislation, the maximum penalties for non-compliance are up to 20 years in jail for a PCBU or officer or a fine of up to $10 million for an entity. Under WHS legislation the penalties for non-compliance are: a $600,000 fine or five years in jail for officers; a $300,000 fine or five years in jail for workers and a $3 million fine for entities. There are also multiple fines for breaches of WHS, food safety regulations and so on, up to and including closing the business.

In terms of the number of prosecutions, Professor Michael A Adams says that:

Since 2000 to 2018, the ASIC annual reports have shown that 336 corporate officers (mostly directors) have been sentenced to imprisonment and the average jail time has increased from two years to nearly four years.[2]

According to Action OHS consulting,[3] since 2015 there have been 575 WHS prosecutions across New South Wales and Victoria alone, with an average fine value of around $70,000.

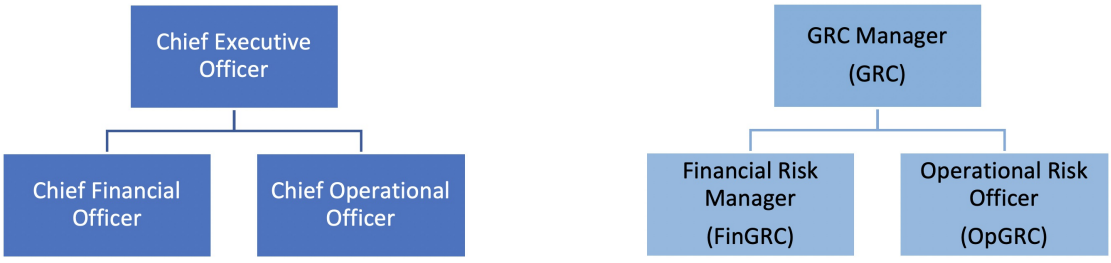
Recommendation: Naming the beast

As yet, there is no umbrella term for operational risks and events, even though they have the capacity to injure and kill. It is these catastrophic operational events that have a far higher potential for attracting legal action and causing severe brand damage.

The objective of this article is to raise awareness of non-financial risks by coining the term OpGRC (operational governance, risk and compliance) in order to elevate it to the same level of awareness and attention as financial GRC.

We recommend organisations structure their GRC teams in the same way that the core of the C-suite consists of a chief executive officer (CEO), a chief financial officer (CFO) and a chief operating officer (COO). The GRC team needs to be led by a senior GRC manager supported by a financial GRC manager and an operational GRC manager. (Figure 3)

Figure 3: Applying the core of the C-suite to FinGRC and OpGRC:



OpGRC has a completely different set of regulations, expertise and knowledge to FinGRC. This segmentation is the first step in highlighting and raising awareness of the different governance requirements, different potential risks and different compliance requirements associated with OpGRC.

Notes

[1] Deloitte, November 2014, *Get out of your own way: Unleashing productivity.*

[2] Adams A, 2019, 'Significant changes in financial disclosure and greater penalties in corporate law', Vol 71 No 7, *Governance Directions.*

[3] Action OHS Consulting, *Prosecutions: 2018 Summary for NSW and Victoria*, www.actionohs.com.au/prosecutions-2018-summary-for-nsw-victoria [3 September 2019].

Nigel Dalton-Brown can be contacted on 0403 958 156 or by email at nigeldb@strytex.com

---