CORPORATER

EMPHASIZING THE **P** IN **GRC**

Owe Lie-Bjelland
Director - Program Management GPRC

ARTICLE

GRC (Governance, Risk & Compliance) is a widely known concept. However, new acronyms, such as, DRM (Digital Risk Management)[i] and IRM (Integrated Risk Management)[ii] are being introduced.

GARTNER'S IRM CONCEPT

The IRM concept was introduced in 2017 by Gartner to meet the increasingly complex needs related to digitalization, cyber security, and risk management affecting most businesses across its operational domains. Gartner brings a slightly new concept to the market reiterating the inherent positive aspects of GRC under a new name, focusing more on the operational approach of GRC.

MEANWHILE, WHAT DID FORRESTER SAY?

Forrester states in its GRC vision 2017-2022[iii] that “GRC efforts have evolved slowly over the past 15 years. However, in the next five years, unprecedented changes in business and technology will demand much more sophisticated, strategic, and proactive GRC capabilities.”

But, why did Gartner see a need for redefining GRC?

Why so many companies perceive GRC as a negative initiative could have several explanations.

1 LACK OF VALUE AND BROKEN PROMISES

One observation is that although GRC is a paramount discipline in running a successful business, few and poor technologies have been around to support it properly.

Excel, and even Word and Power Point, have in fact been some of the most used software technologies to support the business' need for risk management, compliance management, and governance. The capabilities required for enabling a sustainable, efficient, and effective GRC program aligned with strategy and performance is simply not present in such tools and will eventually lead to lack of value and broken promises. This leaves GRC with a negative reputation among top management.

2 CHECK-BOX COMPLIANCE AND A NECESSARY EVIL

A second observation is the consumer focus on companies' shortcomings to good governance. This is driving a new trend referred to as "business integrity." Regulators have been failing short in this domain and thus have not been broadly included in an immature business' GRC program. Executives experience they are failing in this regard, even though they have been running GRC for years. It is worth mentioning that traditional GRC is often associated with check-box compliance and is a necessary evil that makes a company focus solely on the absolute minimum requirements for regulatory compliance – simply to pass a possible audit.

3 THE MISSING P IN GRC

A third observation and my key point is the missing P in GRC. OCEG.org, the inventor of GRC, states that "the successful attainment of Principled Performance[iv] requires coordinated capabilities that address performance against objectives, risk arising from uncertainties, and compliance with both mandatory and voluntary requirements – each with consideration of the other."

A company's objective should be to govern their common capabilities to achieve business value through effective and efficient performance, risk and compliance management – aligned with strategy.

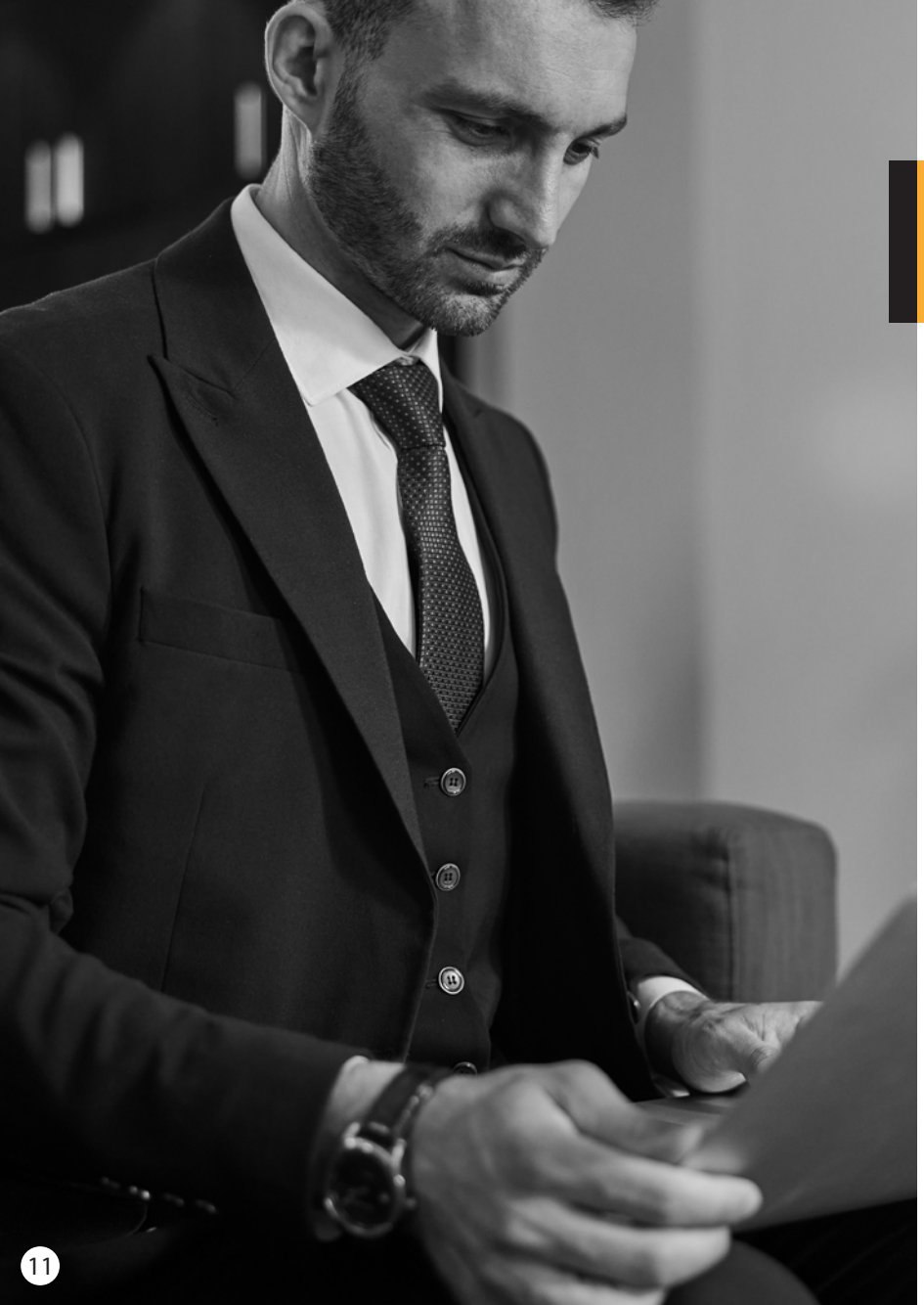
Looking at GRC from the angle of these observations will give some indicators why top management has not experienced the potential value of GRC, but rather the opposite.

In most businesses the primary business objective is performance, and most top managers approve the importance of GRC. Risk and compliance managers, security professionals, management consultants, tactical managers, HSEQ professionals, project managers – they all are convinced of the value of GRC. To them it is evident every day.

They experience the improved performance at the operational and the tactical level, but it is complicated to emphasize the P to demonstrate the sustainable business benefits with top management and the board.

As an illustration; reputation and non-conformance are considered strategic and compliance risks from an ERM (Enterprise Risk Management) view because they have the potential to impact performance.

But reputational and compliance risk do not exist in their own silos, nor on the strategic level alone. The negative reputational and legal impacts from risk events can even originate from one of the operational domains or from the transactional level.



Examples of highly relevant and recently published risk events, without mentioning specific companies, include hacking, money laundering, and bribery. If a diminished reputation equals diminished market value, then companies today should be more susceptible than ever to risk events that damage market perceptions.

There is no gap between business strategy, tactics and operations from an external point of view, and the market does not care if the CEO's explanation for the risk event was unpreparedness, unawareness or rather a statement that demonstrates ignorance. The point is that GRC has an immense effect on performance. The two go hand in hand and feed each other as a true symbiosis to drive the business beyond its competition. With mature GRC comes new business opportunities.

FROM THE BACKBENCH TO THE BOARD ROOM

That being said, a lot of companies are embracing the power of GRC – or GPRC, because they have experienced how integrated GRC can impact their performance. They are moving risk and compliance management from the back-bench to the board room in an enterprise context, achieving a holistic view of their risk profile, bridging the gap between strategy, tactics and operational silos, and they are embracing both regulatory and voluntary compliance from a selection of readily available proven best-practice frameworks to drive business performance.

Owe Lie-Bjelland

Director - Program Management GPRC
Corporater
lie-bjelland@corporater.com

Reference:
(i) http://www.drminstitute.org/what-is-digital-risk-management/
(ii) https://www.gartner.com/it-glossary/integrated-risk-management-irm
(iii) https://www.forrester.com/report/GRC+Vision+20172022+Customer+Demands+Escalate+As+Regulators+Falter/-/E-RES136452
(iv) https://www.oceg.org/about/what-is-principled-performance/

CORPORATER

Corporater enables organizations to seamlessly connect the areas of governance, performance, risk, and compliance (GPRC).

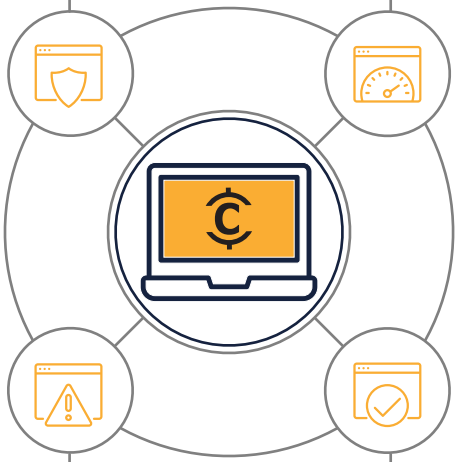
Contact us for demo at
www.corporater.com/requestdemo
info@corporater.com

GOVERNANCE

- Business Integrity Monitoring
- IT & Information Security Management
- Data & Information Governance
- Strategy Management
  - Balanced Scorecard
  - Strategic Planning
- Policy Management
- ++

RISK

- Enterprise Risk Management
- Operational & IT Risk Management
- Project & Portfolio Risk Management
- Barrier & Hazard Risk Management
- KRIs, Dashboards, and Analytics
- Integrated Risk Management
- 3rd Party Risk Management



PERFORMANCE

- Corporate Performance Management
- Employee Performance Management
- Project & Portfolio Management
- KPIs, Dashboards, and Analytics

COMPLIANCE

- Individual Accountability and Conduct
  - BEAR (Australia)
  - MAS IAC (Singapore)
  - SMCR (UK)
- Regulatory Compliance Management
- Information & Cyber Security
- ISO Management Systems
- Data Privacy
- Financial Crime
- ESG
- Operational Resilience
- ++

Learn More ›

Request Demo ›