Governance, Risk Management and Compliance (GRC) and Effective Implementation and Monitoring

GRC - Governance, Risk Management, and Compliance is a concept around only since about 2007 in the corporate management system that integrates these three crucial functions into the processes of every department within an organization. GRC is in part a response to the "silo mentality," as it has become disparagingly known. That is, each department within a company can become reluctant to share information or resources with any other department. This is seen as reducing efficiency, damaging morale, and preventing the development of a positive company culture. Therefore it becomes important to understand concept of Governance, risk management and ensure the required compliance which is a key element of any organization's management for a long time prospective.

CS R Balakrishnan, FCS
Governance Professional Cor.Governance Institute (UK), Pune
bala.hitsafrica@gmail.com

INTRODUCTION

Governance Risk and Compliance (GRC) is the backbone of each and every organization – let it be small, medium or large. The whole objective of GRC is to ensure that all the organization's capabilities are working to the fullest extent i.e. to the optimum use and the efforts are being made towards achieving the said strategic goals and targets of the company. GRC is to ensure that the organization is on the right track and not pathless. The development which has taken place after the Enron scam, one of the big five auditing firms vanishing and the big five auditing firms becoming big four has brought out the concept of governance, risk and compliance (GRC). Ever since, especially from the year 2007, governance, risks and compliance are increasing the need for conscious planning, initiatives, and allocation of the resources by the organizations not only in India but world-wide to create resilience against the exposures and sustained business growth in the long term.

To meet the goals and targets of the organization, almost all the organizations need to draft out suitable policies and processes and put in place to promote excellent governance practices to inculcate a robust culture of compliance and risk mitigation in each and every operation of the organization. In the light of aforesaid, all the organizations need to adopt a broad range of governance, risk and compliance (GRC) policies, practices and processes to meet the requirements of the stringent regulatory environment, increasing business complexities and enhanced focus on accountability. As these processes are interdependent, when orchestrated in a well synchronized manner, will enhance the economic value for all the stakeholders of the organization and enable sustainable growth for in the long term on an ongoing basis.

Objective

When we talk about the objective of the Governance, Risk & Compliance, it is the framework which enhances organizational effectiveness by integrating processes and components of Governance, Risk and Compliance of the organization. The framework in any organization is to be put in place which is capable of, removing overlaps and redundancies and carrying out timely course correction as and when called for. The framework would also set out the organizational approach to governance, risk & compliance in an integrated manner to ensure the best supply of goods and services rendered by the organization on the principle of on time delivery in full (OTIF) and ensure at the end of the day the framework delivers the organization's strategic objectives and lay out a cohesive framework where all the governance related initiatives are monitored more objectively and at a regular periodical interval – the frequency as decided by the organization.

Scope

This framework set out by the organization would imply implementing the governance/ corporate policies in a manner that the framework produce the desired goals /

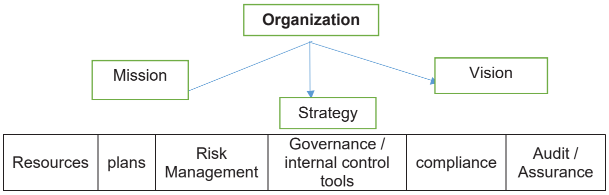
targets of the organization together with evaluating the impact on business performance. The framework also considers all the GRC components as a group and therefore serves as the group governance framework in terms of the provisions under the Companies Act, 2013 in respect of all organization and as well as per the provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 in respect of listed companies, are in addition to the provisions of the Companies Act, 2013.

Applicability

The framework should be made applicable across the company, and it is to be adhered by all the employees of the organization – top to bottom and in addition to the framework also should be made applicable to the organization's subsidiaries and Joint Ventures and to all the custodians, key stakeholders, committees etc., wherever applicable.

Understanding the GRC

In order to understand the GRC in a better way, we can put the following pictorial presentation to make the things clear.



Mission, Vision & Strategy

All the organizations – small, medium, and large have their own mission along with their vision which they like to pursue and achieve in the longer run and on sustainable basis. In order to achieve the desired vision, the organizations need to set their own strategy, set the goals / targets and then have an implementation programme / business plan.

Components of GRC

The GRC has three elements i.e. Governance, Risk and Compliance and let us have a brief of each element.

Table 1 - Elements of GRC

Sr. No.	Elements	Details
1	Governance	Governance is all about setting the plans, policies and procedures that are required for the achievement of the strategic goals of the company.
2	Risk	Risk management is all about mitigating the impact of uncertainties that could trigger during the course of working towards the achievement of the strategic goals / target set for the company.
3	Compliance	Compliance is nothing but strict adherence to the regulatory requirements, obligations and the set of rules, policies and procedures including any standards specified by the regulators in order to ensure that all the organizational capabilities are working together as per the strategy. Let us also understand that the compliance is not just ticking the boxes, stating yes or no – but is working ethically and responsibly.

Benefits of GRC

Having a GRC programme in place, the organizations are getting benefits as stated below:-

Table 2 - Benefits of GRC

Sr. No.	Benefit	Details
1	Identify / assess and manage risk	Assists / helps organizations, to identify, assess and manage regulatory risks and effectively ensure that their operations and practices are aligned with legal requirements.
2	Risk management framework	Ensures an effective risk management framework in place and GRC helps organizations identify, assess and manage risks that may impact their operations, finances, reputation and stakeholders amongst others.
3	Governance and Compliance	Assist the organization to address the governance issues, managing the risk and ensuring absolute compliance by creating policies, procedures, regulatory controls, risk assessment, risk monitoring and internal controls.
4	Promoting morale and efficiency	All the employees across the organization must adhere to company-wide the laid down policy, codes procedures etc. without any exception which would promote excellent morale and utmost efficiency.

Definitions

The framework may contain a definition clause which may spell out the various concepts. For example, the definition clause could be as under by way of illustration.

Table 3 – Illustrated definition clause

Sr. No.	Concepts	Defined
1	Policy	Internal corporate policies as published and amended by the organization from time to time.

2	Risk	Risk is any kind of risk included but not limited to economic risk, business continuity risk, compliance risk, financial Risk, reputation risk, operational risk, etc., as detailed in Risk Management Policy of the organization.
3	Committee	Committees formed by the Board under the Companies Act 2013 and LODR regulations 2015 and includes the – name of the committees may be mentioned.
4	GRC Committee	Committee formed under this framework and is responsible for the implementation and the smooth functioning of the GRC framework at the organization.
5	Custodian	Custodians are the identified people/ personnel who are responsible to administer, track and keep a record of the Policies/Standard operating procedures assigned to them.
Similarly other concepts could be defined under this clause		

GRC Committee

The organization could set Governance, Risk and Compliance (GRC) committee in order ensure smooth functioning of the integrated framework which is being put in place by the organization and GRC committee could have organizational structure with CFO as the chairperson assisted by senior GM-Operations, Company Secretary and Compliance Officer and Secretary to the GRC committee.

Responsibilities of the GRC Committee

To name the responsibilities of the GRC committee, we could list down the following:-

Table 4 - Responsibilities of GRC committee

Sr. No.	Responsibility	Details
1	Providing expert advice	To provide expert advice and support in relation to the company's governance, risk and compliance management.
2	Effective risk management	To establish link between the GRC components along with the GRC custodians that enables effective risk management and compliance activity to be carried out consistently across the organization.
3	Effective reporting	To ensure an appropriate level of understanding and engagement in risk and compliance management through effective education, reporting, escalation and discussion.
4	Business continuity	To establish a business continuity framework to ensure risks that threaten the ongoing operation of the organization are effectively planned and managed.
5	Continuous improvement	To review and continuous improvement of this framework and governance, risk and compliance management across the organization.
6	Facilitating	To facilitate the process outlined within the enterprise risk management and compliance framework and ensuring the ongoing reporting of the outcomes of those processes.
7	Measuring the impact and improving	To measure impact of various GRC components and making use of the same to improve the company's strategies.

> When we talk about the objective of the governance, risk compliance, it is the framework is meant to enhance organizational effectiveness by integrating processes and components of governance, risk, and compliance of the organization. The framework in any organization is to be put in place which is capable of, removing overlaps and redundancies and carrying out timely course correction as and when called for. The framework would also set out the organizational approach to governance, risk & compliance in an integrated manner to ensure the best supply of goods and services rendered by the organization.

EXECUTION OF BUSINESS PLAN

First and foremost, requirement for the execution of the business plan is that making the resources available and planning for the same. When we talk about the resources, we mean the required man power, material needed, equipment / machinery and above all the money i.e. finance. In addition to the above, the organizations may be needing various other ancillary plans which may be called for in order to executive the business plan / implementation of the set programme such as; (i) resource allocation plan; (ii) resource mobilization plan; (iii) planning of required finance;(iv) material procurement plan; (v) production plan; (vi) plan to have better quality i.e. quality control plan; and (vii) close our plan and many more depending upon the nature of industry in which the organization is operating and also with reference to the geographical location of the organization.

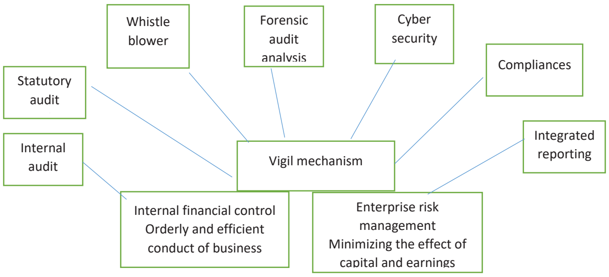
INTEGRATION OF GOVERNANCE, RISK & COMPLIANCE COMPONENTS

Organizations may put in place a wide range of monitoring tools in form of policies, procedures and SOP's in place falling under different categories in order to aiming to integrate these monitoring tools to create a strong mechanism. The organizations may formulate a broad governance framework comprising of the components such as; (a) internal financial control (IFC); (b) enterprise risk management (ERM); (c) internal audit (IA); (d) business code of ethics & compliance; and (e) health & safety & environment amongst others.

Every organization could develop their own values and they continue to maintain such values. In order to maintain the organizational values, the organization needs to have in place the various governance policies, internal control tools i.e. having in place a standard operation procedures (SoPs). Organization may need to put in place many policies and following are some of the illustrative examples in this respect.

	Table 5 - Policies / Procedures (illustrative)
Sr. No.	Details of policies / procedures etc.
1	Segregation of duties.
2	Workflows.
3	Delegation of Authority documentation.
4	Physical & IT recruitment policy.
5	Policy on health safety and environmental (workplace).
6	Quality policy.
7	Policy on familiarization programme of Directors.
8	Terms and conditions of appointment and payment to director.
9	Policy on gift & hospitability.
10	Procedure access control policy.
11	Business code of conduct and ethics.
12	Policy on dissemination of information to market.
13	Policy for determination of material event and information.
14	Code of fair disclosure.
15	Policy on Anti-bribery and anti-corruption.
16	Risk management policy.
17	Integrated management system policy.
18	Code of conduct to regulate monitor and report by insider.
19	Data privacy policy.
20	Record keeping plan of the organization.
21	Policy on preservation of documents.
22	Archival policy.
23	Policy relating to Conflict of interest.
24	Related party transaction policy.
25	Policy on POSH (Prevention of Sexual Harassment at Workplace).
26	Dividend distribution policy.
27	Code of fair competition and prevention of unfair trade practices.
28	Policy on Environmental, Social and Governance.
29	Corporate social responsibility policy.
30	Whistle blower policy / vigil mechanism.
Many more depending upon the organization need...	

The organization may aim at achieving an integrated framework as depicted below:


Whistle blower
Forensic audit analysis
Cyber security
Compliances
Statutory audit
Integrated reporting
Internal audit
Vigil mechanism
Internal financial control Orderly and efficient conduct of business
Enterprise risk management Minimizing the effect of capital and earnings

Each of the components mentioned above where output of one component serves as an input to another component will not only help to create a holistic approach towards governance but also facilitate continuous control monitoring and a robust integrated mechanism removing redundancies if any.

PUTTING THE GRC FRAMEWORK IN PLACE

The organization could put the GRC frame work clearly stating as to who are the custodians along with key stakeholders and the governance structure in place and the governing policies etc. An illustrated suggestive framework which could be put in place by the organization is provided below by way of illustration.

Table 6 - Suggested GRC framework (by way of illustration)

GRC components	Policies & Practices for monitoring specific areas	GRC custodians	Governance structure	Key stakeholders
Annual Internal Audit	Annual Internal Audit Plan	GM – operations Head and Internal Controls	Audit Committee	Board/Audit Committee/ Statutory Auditors
IFC	Delegation of Authority	GM – operations / CFO/ Head and Internal Controls	Audit Committee	Committees/Employees
	Control Self Assurance	CFO /GM - Head and Internal Controls	Audit Committee	Board/ Audit Committee
	IFC testing	CFO, Senior / GM - Head - and Internal Controls	Audit Committee	Board/Audit Committee/ Statutory Auditors
Governance, Ethics & Compliance	Whistle Blower	Company Secretary & Compliance Officer	Audit Committee /HR	Board / Committees/ Employee
	Business code of conduct & ethics	Chief financial officer, Company Secretary & Compliance Officer / Senior executive (like general manager	Audit Committee / Statutory Auditors / Internal Auditors / Human Resources Department.	Stock exchanges / Investors
	POSH	Internal Compliance Committee (ICC) General Manager Chief Human Resource Officer	Internal Compliance Committee (ICC)/ Human Resource Department	ICC /State government / District Officers
	Related party transactions – policy and practices	CFO / GM – Finance & Accounts/ Company Secretary & Compliance Officer	Audit Committee	Board & Audit Committee, Investors, MCA & Stock Exchanges
	Materiality policy	CFO / GM – Finance & Accounts / Company Secretary & Compliance Officer	Audit Committee	MCA
	Dividend distribution policy	CFO, Company Secretary & Compliance Officer	Board	Share holders
	Prevention of insider trading	GM – operations GM – operations CFO, Company Secretary & Compliance Officer	Audit Committee	Board, Investors, MCA & Stock Exchanges
	Ethics & compliance framework	GM – operations CFO, Company Secretary & Compliance Officer / GM	Audit Committee	Board & Audit Committee
	Composition, Charter & Policies relating to Board and its committees	GM – operations CFO, Company Secretary & Compliance Officer /	Board	Investors Bankers & other stakeholders
ERM	Risk Management Policy & practices	CFO /GM – operations Company Secretary & Compliance Officer	Risk Management Committee	Board, Investors, Bankers, SEBI, Credit Rating Agencies
SHE	Safety, health & environmental Policy & practice	Chief Human Resource Officer	HR	Employees / Customers / Regulatory authorities

CORPORATE GOVERNANCE, ETHICS & COMPLIANCE

We could discuss this into two aspects i.e. one on Corporate Governance and the other on business code of conduct and ethics.

CORPORATE GOVERNANCE

Corporate Governance encompasses the entire system of managing and supervising an enterprise. The Board and the committees are committed to a responsible and transparent style of management and supervision aimed at increasing the Company's value over the long term. Every organization would like to stress upon great importance on responsible Corporate Governance and would like to achieve excellence in governance practices. All organization have been putting their maximum efforts year after year in order to maintain a high standard of governance and have been striving in continuing with the same. In this respect, the organization are working through forming various committees in order to scrutinize and look over various governance activities. To name some of the committees we could state; (a) Audit Committee; (b) Nomination & Remuneration Committee; (c) Stakeholders Relationship Committee (d) Risk Management Committee; and (e) Corporate Social Responsibility Committee and these committees are formed under the provisions of the Companies Act, 2013 by all companies and the LODR Regulations, 2015 for listed companies. The organization are also annually publishing their financial statements giving the disclosures about the details on the duties and activities of the Board committees in their Corporate Governance Report which forms part of the annual report.

BUSINESS CODE OF ETHICS AND CONDUCT

All organizations have their business responsibility to ensure the compliance with the statutory and regulatory requirements as applicable to the organization. Organization by and large defines compliance as legally and ethically impeccable conduct by all employees in their daily work, because the way they carry out their duties affects the reputation and the brand image of the company. Organization does not tolerate any violation of any laws, company's policy, business code of conduct and ethics or other internal regulations as applicable. It may be noted that ethics and compliance is not a one-time event and it's a continuous process and that's where the need of a robust compliance framework arises. All organizations are aiming to achieve this through flexible controls hierarchy, assessments and audits, issue tracking and remediation and analytics. To track and achieve high standards of ethics and compliance, the organization are framing their policies, codes, procedures and systems as outlined in Table 5 above.

RISK MANAGEMENT

With the frequent amendments in the regulatory from work from time to time, the organization are mandated and required to take actions and also with the rising of shareholder activism, many organizations have become sensitized to identifying and managing areas of risk in their business: whether it is financial, operational, brand or reputation related risk. These risks are no longer considered the sole responsibility of specialist executives, and the Board's demands clear accountability and visibility into exposure and status of mitigation measures so they can effectively implement the organization's long-term strategies.

Therefore, it is essential for every organization to put in place a risk management mechanism which aims at identifying, measuring, mitigating and managing risk. In every organization, the Risk Management Committee, the Audit Committee and the Executive Management Committee form the governance structure for each of the policies in order to take adequate measure to control and mitigate risks while putting in an exhaustive risk management policy. The organization may suitably adopt the guidelines brought out by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004 framework for its enterprise risk management process. The Company's risk management should set up a framework for the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management capability.

RESPONSIBILITIES OF CUSTODIANS

The custodians of the GRC are expected to work in an integrated manner and share outcomes, issues, learnings, developments & amendments relating to their field/GRC component. To achieve this integrated flow the GRC custodians shall meet on a quarterly basis and discuss the following issues so that suitable monitoring and actions could be taken:

Table 7 - Responsibilities of the custodian

Sr. No.	Responsibility	Details
1	Compliance arising from GRC component	Compliances arising from GRC component for which they are custodians.
2	Workflow & automation	Deciding workflows and automation.
3	Future initiates	Future Initiatives.
4	Integration	Integration opportunities & redundancy/overlap removal.
5	Tacking	Key developments which shall include tracking regulatory, statutory & external environment development with relation to GRC component.

6	Repository of decision for future reference	Centralized repository of decisions for future references and record.
7	Measuring impact	Measure the impact of the GRC framework on the business and functions.
8	Implementation of recommendations	Implementation of the recommendations of the respective committees and follow up.
9	Confidentiality	Maintain high degree of confidentiality of the matters discussed at the GRC Committee This quarterly meeting of the GRC custodians shall be chaired by the Group CFO and the Action Taken Report shall be reviewed jointly.

In addition to the above responsibilities, the GRC custodians shall ensure that the governance policies are not treated as a static document. Policy audits shall be undertaken by the GRC custodians to ensure that the policies are effectively implemented and aid the purpose of achieving the objectives relating to; (a) efficacy and relevance of policy; (b) managing compliance levels; (c) deviation management; (d) testing of controls; (e) SOP and responsibility matrix; and (f) policy audits on a half yearly basis.

Finally any change in these policies will be apprised during the GRC quarterly meet and then will be taken up for the Board's approval for implementation of changes and carrying out required modifications and bring out the revised policy.

RESPONSIBILITIES OF EMPLOYEES

It is the responsibility of the governance, risk and compliance (GRC) custodians to undertake a training programme as and when needed i.e. need based training sessions to bring the awareness for the employees on the various components of GRC. Besides the custodians and the committees, it is equally important for each and every employee of the organization to be responsible for:-

Table 8 - Responsibilities of employees

Sr. No.	Responsible for	Details
1	Understanding the objectives of GRC	Actively seeking to understand the objectives, risks, controls and obligations that relate to their activities and participate in governance, risk and compliance management.
2	Compliance with the regulations policies and procedures	Undertaking activities in compliance with legislation and our policies and procedures.
3	Identifying the risk events / non-compliance	Identifying and reporting risk events and instances of non-compliance.
4	Promptly reporting	Reporting new risks, risks exceeding tolerance, breaches or weaknesses of controls to their supervisor and as and when required.

Effectiveness of the GRC

The effectiveness of the integrated GRC framework could be monitored and measured through the following:-

a. Direct and indirect impact on operations in terms of profitability and sustainability;

b. Impact of each GRC component and measures taken;

c. Audit Committee and Internal/External Auditor feedback;

d. Communication of the impact – dash boards, score cards on an annual basis;

e. Calibration of the impact with external environment.

CONCLUSION

From the foregoing, we could conclude that the Governance, Risk and Compliance (GRC) framework implementation aims to provide effectiveness in order to reduce risk and improve control effectiveness, security and compliance through an integrated and unified approach that will ultimately reduce the ill effects of organizational silos and redundancies and take the organization to a much higher level with long term prospective and sustainability. Needless to mention that the frameworak will have to reviewed periodically with reference to the regulatory changes and amendments in the law and required to reviewed and revised.