Systems Audit of GRC Using COBIT 5

Using globally recognised framework such as COBIT 5 makes available a large repository of best practices which can be used to enhance compliance and improve auditability. Enterprises as well as auditors and consultants can use this systematic approach and knowledge repository to institutionalise GRC processes and its implementation. CAs with the domain knowledge of GRC and functional expertise of business processes can provide assurance or advisory services to enterprises in the GRC domain. This article provides an overview of regulatory requirements of GRC and outlines how a GRC program can be implemented or reviewed by using COBIT 5, the business framework for governance of enterprise IT. Read on to know more…

CA. A. Rafeq

(The author is a member of the Institute. He can be reached at rafeq@vsnl.com)

Introduction

Failures of some large enterprises in the last decade due to lack of adequate level of Enterprise Risk Management has compelled regulators to mandate its enforcement, thus necessitating compliance with Governance, Risk Management and Compliance (GRC).GRC implementation and certification is a regulatory and business requirement for large enterprises, but could be used by Small and Medium Enterprises (SME) as well because it provides a robust process oriented structure and system enabling compliance and value addition. Effective implementation of ERM requires consideration of multiple factors such as using a holistic approach which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs. As IT is a key enabler for most enterprises, it is imperative to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance. The principles of GRC applied in SME provide the benefit of a safe and secure environment, although the scope and level of ERM would be lesser. This has led to an increasing demand for GRC related services, which is being provided by vendors and solution providers ranging from consulting firms to large IT vendors.

Section 49 (C) outlines the need for Board Disclosures relating to Risk management and states: "The Company shall lay down procedures to inform Board members about the risk assessment and minimisation procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.

What is Governance, Risk Management, and Compliance (GRC)

Let us first understand by having a clarity on what is meant by GRC. Different vendors are providing their own interpretations of GRC to suit the varied solutions they have to offer. GRC, in general, is the umbrella term which encompasses corporate governance, enterprise risk management (ERM) and compliance with applicable laws and regulations. GRC has gained prominence globally after enactment of Sarbanes Oxley Act (SOX) in the US and similar legislations across the world. In India, Clause 49 of the listing agreements applicable for listed companies *inter alia* includes all the key aspects of SOX and covers corporate governance requirements including GRC. Some key definitions related to GRC aspects which need to be understood while implementing/reviewing GRC are:

Corporate Governance: The systems and processes, by which enterprises are directed, controlled and monitored.

Compliance: The systems and processes that ensure conformity with business rules, policy and regulations.

Governance: ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.

Management: Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

Governance of Enterprise IT (GEIT): Concerned with IT value delivery to the business and the mitigation of IT-related risks. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals.

Risk Management: The culture, processes and structures that are directed to the effective management of potential opportunities and adverse effects.

Risk: The potential for an event to occur that could have an effect on the Enterprise objectives or operations.

Need for GRC Review from Corporate Governance Perspective (Clause 49)

Specific provisions highlighting the regulatory requirements for implementing GRC in enterprises as per Clause 49 listing requirements, are given below:

Risk Management

Section 49 (C) outlines the need for Board Disclosures relating to Risk management and states: "The Company shall lay down procedures to inform Board members about the risk assessment and minimisation procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.

CEO/CFO Certification

Section 49 (V) deals with CEO/CFO certification and states that the CEO, i.e. the Managing Director or Manager appointed in terms of the Companies Act, 1956 and the CFO i.e. the whole-time Finance Director or any other person heading the finance function discharging that function shall certify to the Board and includes *inter alia* the following:

(c) They accept responsibility for establishing and maintaining internal controls and that they have evaluated the effectiveness of the internal control systems of the company and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies.

Auditor Certification

Section 49 (VII) deals with compliance aspects and states that the company shall obtain a certificate from either the auditors or practicing company secretaries regarding compliance of conditions of corporate governance as stipulated in this clause and annex the certificate with the directors' report, which is sent annually to all the shareholders of the company. The same certificate shall also be sent to the Stock Exchanges along with the annual report filed by the company.

GRC Programme Implementation

Although a GRC programme (project) can be implemented primarily from a compliance perspective, it is advisable to consider business requirements also so as to optimise the investments made in implementing relevant processes, control structures and systems. GRC programme implementation requires:

- Defining clearly what GRC requirements are applicable.
- Identifying the regulatory and compliance landscape.
- Reviewing the current GRC status.
- Determining the most optimal approach.
- Setting out key parameters on which success will be measured.
- Using a process oriented approach.
- Adapting global best practices as applicable.
- Using uniform and structured approach which is auditable.

Successful implementation of GRC in enterprise can be measured in general by the assurance provided to the senior management on the adequacy of controls implemented. However, it is important to set specific success criteria for measuring how well GRC program is implemented. Sample goals and metrics which can be adapted are given below:

1. The reduction of redundant controls and related time to execute (audit, test and remediate)
2. The reduction in control failures in all key areas.
3. The reduction of expenditure relating to legal, regulatory and review areas.
4. Reduction in overall time required for audit for key business areas.
5. Improvement through streamlining of processes and reduction in time through automation of control and compliance measures.
6. Improvement in timely reporting of regular compliance issues and remediation measures.
7. Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.

Using COBIT 5 for Effective GRC Programme

Governance of Enterprise IT (GEIT) focuses on benefit realisation, risk optimisation and resource optimisation. Benefit realisation focuses on creating new value for the enterprise through IT, maintaining and increasing value derived from existing IT investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. Risk optimisation addresses the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT-related business risk consists of IT-related events that could potentially impact the business. Resource optimisation focuses on ensuring that the right capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided.

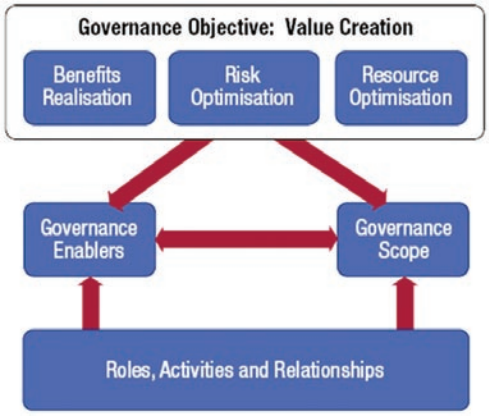
Source: COBIT® 5, figure 3. © 2012 Courtesy: ISACA

Responsibility of Senior Management in GRC

The responsibility of senior management in implementing and monitoring functioning of requisite GRC measures is not only a regulatory requirement but also makes business sense as an effective GRC implementation helps in not only ensuring compliance but also meeting business requirements. Using the best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented. It is advisable that the board should mandate adaption of a GEIT framework such as COBIT5, as an integral part of enterprise governance development. COBIT 5 framework would provide the overall approach and based on this, relevant guidance can be selected from specific standards and good practices for designing specific policies, processes, practices and procedures. This ensures that appropriate governance processes and other enablers are developed and optimised so that GEIT operates effectively as part of normal business practice and becomes a supporting culture as demonstrated by top management. Alignment with COBIT 5 best practices

would also result in faster and more efficient external audits, since COBIT is widely accepted as a basis for IT audit procedures.

The COBIT 5 framework describes seven categories of enablers which need to be implemented as applicable in an enterprise. These enablers are: principles, policies and frameworks, processes, organisational structures, culture, ethics and behaviour, information, services, infrastructure and applications and people, skills and competencies. Implementing an effective GRC programme would require selection of required enablers as applicable to the enterprise. COBIT has published "COBIT 5 enabling process" guide which has detailed guidance on the "processes" enabler. The following section illustrates how to scope a GRC review by using relevant content from COBIT 5 enabling process guide.



Source: COBIT® 5, Figure 8. © 2012 Courtesy: ISACA

How to Scope a GRC Review using COBIT 5

GRC review helps an enterprise to obtain objective evaluation of existing policies, procedures and practices and to confirm whether it meets governance, compliance requirements and enterprise objectives. A GRC review will provide assurance on how far the enterprise has been successful in achieving set objectives of GRC programme. Further, it may also identify gaps in control weaknesses or areas of improvement and provide actionable recommendations for mitigating risks, ensuring compliance and meeting business needs.

Using the approach outlined in the COBIT 5 Goals Cascade, the relevant processes as applicable to GRC can be selected, using the step by step approach given below. *Readers are requested to refer to the articles published in the Tech for you section in May/June 2012 for more details. The COBIT 5 framework is available to all as a free download from ISACA at www.isaca.org/cobit.*

1. **Identify Stakeholder needs:** Based on the Governance objectives: Benefits Realisation, Risk optimisation and Resource optimisation, relevant governance objectives are to be selected. *The primary objective of a GRC review would be Risk optimisation, although other objectives may be combined depending on the need.*

2. **Select Enterprise Goals:** Based on the Governance objectives, select the relevant enterprise goals from the list of 17 enterprise goals. *Using Figure 5 of COBIT 5 Business Framework, the following Enterprise Goals (EG) would be selected: EG 3: Managed business risks (safeguarding of assets), EG 4: Compliance with external laws and regulations and EG 15: Compliance with internal policies,*

3. **Select IT Related Goals:** Based on the identified enterprises goals, select relevant IT-related Goals from the list of 17 IT-related goals. *Using Figure 22 of COBIT 5 Business Framework, the following IT Related Goals (ITG) which are primarily impacted are selected. These are ITG 2: IT compliance and support for business compliance with external laws and regulations, ITG 3: Managed IT-related business risks, ITG 10: Security of information and processing infrastructure and applications, ITG 15: IT compliance with internal policies.*

4. **Select IT processes:** Based on the selected IT-related goals, using the Primary criteria, select relevant COBIT 5 process. *Using Figure 23 of COBIT 5 Business Framework, the following COBIT 5 processes would be selected for the relevant IT Goals:*
   - EDM1 Set and Maintain the Governance Framework
   - EDM3 Ensure Risk Optimisation
   - EDM5 Ensure Stakeholder Transparency
   - APO1 Define the Management Framework for IT
   - APO12 Manage Risk
   - APO13 Manage Security
   - BAI6 Manage Changes
   - BAI10 Manage Configuration
   - DSS5 Manage Security Administration
   - MEA1 Monitor and Evaluate Performance and Conformance
   - MEA2 Monitor System of Internal Control

- MEA3 Monitor and Evaluate Compliance with External Requirements:

5. **Filter and Short-list applicable IT processes:** The above list of processes may be filtered further based on applicability of the contents, depending on scope and relevance for the enterprise.

6. **Use the relevant contents:** The relevant content from each of the relevant components of COBIT 5 Processes such as: Process description, purpose, Goals cascade and metrics, Process Goals and related Metrics, RACI Chart, practices with Input-output document references, list of activities and related guidance, can be used to prepare the benchmark of COBIT as applicable for the assignment.

7. **Customise the extracted contents:** The extracted contents that are relevant, are to be customised as required by integrating with other frameworks and internal practices and converting them to a benchmark of best practices or audit procedures to be used for implementation/evaluation of enterprise specific policies, procedures and practices.

Using COBIT 5 Enabling Process Knowledge Base

COBIT 5 provides complete, consistent, and easily navigable guidance which can be used and adapted for meeting any applicable legal, regulatory and contractual requirements. Detailed information for each of the 37 IT processes are given in a structured manner. This facilitates easy understanding and usage of contents. The structure and purpose for COBIT 5 processes as applicable for specific assignment for example: GRC review is explained here:

1. **Process description:** This can be used for understanding scope of coverage of the process.

2. **Process purpose statement:** This can be used for defining the objective or purpose for which the specific process could be used.

Knowledge of COBIT 5 can empower CAs to provide IT enabled services in all areas including consulting on Implementing/reviewing IT GRC by using it as the single integrated framework with its repository of global best practices to be adapted as applicable.

3. **Goals cascade information:** This can be used for identifying relevant IT-related goals which are impacted.

4. **Process goals and metrics:** This can be used for setting specific process goals with metrics as applicable for the identified processes.

5. **RACI chart:** The RACI chart can be used for establishing the required organised structure and process responsibility for the relevant management practices by clearly outlining the Responsibility: Who is responsible for getting the task done? Accountability: Who is accountable for the success of the task? Consultation: Who is to be consulted to provide inputs? And Informed: Who is to be kept informed by providing relevant information.

6. Detailed description of the process practices for each practice:
   - **Practice title and description:** The management practices can be selected and customised as applicable for implementation or evaluation.
   - **Practice inputs and outputs:** These can be used for identifying the work products which can be used, produced and, shared with relevant stakeholders or process owners.
   - **Activities:** These can be used for implementing the relevant practices.

7. **References of related guidance:** This can be used to integrate information with other standards and direction to supplement information from COBIT as applicable.

Conclusion

Implementing GRC is need of the hour and in an IT enabled enterprise, IT GRC is key to implementing effective GRC. The benefit of GRC implementation can be derived not only by large enterprises but also by SMEs. CAs with their core competencies in compliance can use globally recognised frameworks to provide advisory services as also to review GRC from the perspective of assurance. CAs, who are technologically adept, can advise enterprises on ways to leverage technology in ways that ensure compliance but also add value. Knowledge of COBIT 5 can empower CAs to provide IT enabled services in all areas including consulting on Implementing/reviewing IT GRC by using it as the single integrated framework with its repository of global best practices to be adapted as applicable. ■