

ACCOUNTABILITY, RESPONSIBILITY AND TRANSPARENCY

IS GRC (GOVERNANCE, RISK, COMPLIANCE) AN ART OR A SCIENCE?

BY SANJAY ANAND, CHAIRPERSON, SOX/GRC INSTITUTE, GRC GROUP ©

A BRIEF HISTORY

In 2002, the House passed H.R. 3763 or the Corporate and Auditing Accountability, Responsibility and Transparency Act (CAARTA), which was then modified and approved in the Senate (as Senate Bill 2673) as the Public Company Accounting Reform and Investor Protection Act. The Conference Committee then named the legislation the Sarbanes-Oxley Act after its co-authors, Senator Paul Sarbanes and Congressman Michael Oxley.

Even as the name of the legislation has undergone as many changes as it has since it was first conceived by Michael Oxley in the House as CAARTA, the fundamental tenets that it addresses have remained virtually unchanged. Specifically, the legislation addresses the three elements that led to the Enron and WorldCom accounting scandals and fiascoes, namely accountability, responsibility and transparency.

SOME DEFINITIONS

Let us take a moment to first understand what these three terms really mean. They are often used loosely and interchangeably, but in the strictest sense of their meanings they are intended to convey very specific aspects of Governance, Risk Management and Compliance (GRC) addressed in the Sarbanes-Oxley (SOX) legislation.

Accountability

The Merriam-Webster dictionary defines “accountability” as “the quality or state of being accountable; especially: an obligation or willingness to accept responsibility or to account for one’s actions”. It then gives a specific example of the usage of the word: “public officials lacking accountability”. In addition, it defines “accountable” as “subject to giving an account: answerable” or “capable of being accounted for: explainable”. Likewise, Dictionary.com defines “accountability” as “the state of being accountable, liable or answerable”.

Responsibility

Referring back to the Merriam-Webster dictionary’s definition for “responsibility”, we find that it defines it as “the quality or state of being responsible: as moral, legal or mental accountability; reliability, trustworthiness”. It further defines “responsible” as “liable to be called on to answer; liable to be called to account as the primary cause, motive, or agent; liable to legal review in the case of fault to penalties; able to answer for one’s conduct and obligations: trustworthy; able to choose for oneself between right and wrong” and so on. Likewise, Dictionary.com defines “accountability” as “reliability/dependability in meetings debts and payments”.

Transparency

Finally, the Merriam-Webster dictionary defines “transparent” as “free from pretense or deceit: frank; easily detected or seen through: obvious; readily understood; characterized by visibility or accessibility of information especially concerning business practices”. Dictionary.com adds the following: “free from guile; candid or open”.

GRC DEFINITIONS

As the world of SOX has matured, and as SOX has become more of a globally accepted set of rules, standards and expectations (with its local variations, of course), the world is now looking to go beyond SOX to a more sustainable, inclusive and long-term strategy referred to as GRC. GRC stands for Governance, Risk Management, Compliance and Controls, and refers to the three key areas that SOX begins to address, but it takes it to a whole new level in terms of implementing and integrating SOX with other standards and legislations. Therefore, let’s go ahead and define what these three terms mean, and then we will put the pieces together. Note that while Wikipedia is not generally particularly authoritative in many regards, it is sufficiently authoritative when it comes to definitions of such terms:

Governance

Governance is the act of governing. It relates to decisions that define expectations, grant power, or verify performance. It consists of either a separate process or part of management or leadership processes.

In the case of a business or of a non-profit organization, governance relates to consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility. For example, managing at a corporate level might involve evolving policies on privacy, on internal investment, and on the use of data.

Risk Management

Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, project failures (at any phase in development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary or events of uncertain root-cause. Several risk management standards have been developed including the Project Management Institute, the National Institute of Science and Technology, actuarial societies, and ISO standards. Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety.

The strategies to manage risk include transferring the risk to another party, avoiding the risk, reducing the negative effect or probability of the risk, or even accepting some or all of the consequences of a particular risk.

Compliance and Controls

In general, *compliance* means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that corporations or public agencies aspire to in their efforts to ensure that personnel are aware of and take steps to comply with relevant laws and regulations.

Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

In accounting and auditing, internal *control* is defined as a process effected by an organization's structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives. It is a means by which an organization's resources are directed, monitored, and measured. It plays an important role in preventing and detecting fraud and protecting the organization's resources, both physical (e.g., machinery and property) and intangible (e.g., reputation or intellectual property such as trademarks).

At the organizational level, internal control objectives relate to the reliability of financial reporting, timely feedback on the achievement of operational or strategic goals, and compliance with laws and regulations. At the specific transaction level, internal control refers to the actions taken to achieve a specific objective (e.g., how to ensure the organization's payments to third parties are for valid services rendered.) Internal control procedures reduce process variation, leading to more predictable outcomes.

GRC PYRAMID

I like to think of GRC as a pyramid, with G (or Governance) being the apex of the pyramid (see Figure 1). The goal of any organization, be it for-profit, non-profit, government or academic, is to serve its stakeholders, and good governance is therefore the ultimate goal that needs to be achieved.

In order to achieve that overall goal (G), an organization needs to have various R (Risk Management) strategies in place that can help mitigate the risk of not achieving that goal/objective.

That then brings us to the third rung, or the foundation, of the pyramid. That is where the proverbial rubber meets the road. In order to meet its risk management measures, organizations use compliance (with internal and external requirements) through controls (C).

Figure 1: The GRC Pyramid



ART VS. SCIENCE

One of the questions I often get is whether GRC is an art or a science. The answer is simple if we consider the fact that the real world is never black-and-white, but rather it is always shades of gray. Therefore, to expect GRC to be the panacea and to scientifically solve all problems that a company may face (at least in terms of its disclosures, which is the primary intent of SOX), would be naïve. Instead, GRC should be viewed as a continuum along which organizations can employ the Japanese concept of *kaizen* to continuously move towards greater Accountability, Responsibility and Transparency (ART). See Table 1.

Table 1: GRC is an ART

ART→ GRC↓	Accountability	Responsibility	Transparency
Governance			
Risk Mgmt.			
Compliance			

INTEGRATED GRC

One of the terms that is often heard in SOX and GRC circles is the phrase “integrated GRC”. What this essentially refers to is the coming together of these three disparate areas, which until recently were often treated as silos within organizations (see Figure 2). Even today, very few organizations think in terms of an integrated approach to GRC, and when they do, they typically think in terms of technology being used to integrate G, R and C. But “integrated GRC” is so much more than technology. While it may refer to or be implemented using legacy and ERP technologies, and it typically is implemented like that, the concepts around integration go far beyond just the technological requirements and implementation.

Figure 2: Siloed GRC Approach



Specifically, when we (at the GRC Institute) refer to “integrated GRC”, we are speaking of an approach and a methodology that enables companies to create a harmony within their business processes in terms of how they serve all their stakeholders (including shareholders, customers, employees, vendors etc.) so as to cost-effectively and efficiently achieve the cohesiveness that GRC attempts to drive. This in turn enables organizations to move beyond the bits-and-bytes and the nuts-and-bolts, and to start moving towards a framework and an environment that enables greater Accountability, Responsibility and Transparency, which goes back to the basic goal/objective of legislations in the GRC realm (like SOX).

GRC FRAMEWORKS

It is a bit of a misnomer to refer to a “framework for GRC” since GRC itself is a framework. However, in order to implement (technologically or otherwise) GRC within an organization requires a methodology be adhered to that will help ensure the greatest possible benefit (A-R-T) with the least possible costs, i.e. maximize the ROI (return on investment) of a GRC initiative with a quantifiable outcome. Of course, quantifying the outcome is not always easy given that GRC is more Art than it is Science. Nevertheless, in order to make the business case for GRC, some level of objective quantification, in addition to the subjective qualification, is often necessary (albeit not always sufficient) in order to move the GRC project forward.

The recommended framework for “achieving” GRC within an organization is the familiar COSO (or its expanded and more up-to-date version, ERM) framework. The COSO framework was developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission (hence the name, COSO). These organizations are:

- FEI: Financial Executives International
- AAA: American Accounting Association
- IMA: Institute of Management Accountants
- IIA: Institute of Internal Auditors
- CPA: American Institute of CPAs

Although all the above organizations are US-centric, COSO has quickly been adopted as the SOX, and more recently GRC, framework of choice due to its ability to address all three areas: Governance, Risk and Compliance, and due to its ability to adapt to a wide array of real-world business situations. Table 2 provides a glimpse into how COSO ERM can be used as the framework of choice for GRC.

Table 2: COSO ERM and GRC

GRC	COSO ERM
Governance	Internal Environment
	Objective Setting
Risk Mgmt.	Event Identification
	Risk Assessment
	Risk Response
Compliance	Control Activities
	Info. & Commn.
	Monitoring

SOME CONCLUSIONS

Let's first address the question that was posed at the very beginning of this paper (in the title itself): Is GRC and Art or a Science? I think at this point it is quite obvious that GRC is both an art and a science, but due to the subjective nature of everything related to business and its stakeholders, including but not limited to the core element of GRC which is Risk, GRC is more Art than Science. It is an enlightening coincidence that the SOX legislation's primary tenets of Accountability, Responsibility and Transparency (as espoused in CAARTA) spell A-R-T (see Table 1).

Second, we looked at the concept of "integrated GRC" and it is important to note that this merely refers to going from the traditional siloed approach to G, R and C (as was seen in Figure 2) to the top-down logical approach shown in the GRC Pyramid in Figure 1. Integration of course can be achieved by using a combination of people, process and technology (PPT) as would be the case with any integration initiative, GRC or otherwise.

Finally, the recommended framework for "implementing" GRC is COSO (or its latter version ERM). While several organizations have come forth with business models, capability models, maturity models etc., ERM serves as the foundation of those models, and therefore, for all practical purposes, organizations do not need to do much more or reinvent more wheels than they are already using (e.g. for SOX). Hopefully this suggestion alone starts to take away some of the fear and intimidation that GRC sometimes poses, and helps organizations rest easy knowing that what they did for SOX is a great first step and an excellent foundation in the right direction.

ABOUT THE AUTHOR

Sanjay Anand, CSOX, CGRC is an internationally recognized and renowned expert in Governance, Risk Management, Compliance and Controls (GRC), and he has served as Founding Chairperson of SOX and GRC Institutes where Senator Paul Sarbanes and Congressman Mike Oxley are Honorary Chairpersons. He is a frequent writer and prolific speaker on topics related to Sarbanes-Oxley, Dodd-Frank, and other regulations from around the globe. He has been accorded over a dozen honorary industry credentials and certifications including for example CDE (Certificate in Director Education) from NACD Institute, CFE (Certified Fraud Examiner) from ACFE, CGEIT (Governance) and CRISC (Risk) from ISACA, and Professorship from the Chinese Institute of Directors (CIOD).

He has been featured for years in the official Marquis Who's Who (in America, the World, Finance and Business) publications; and has been accorded numerous industry awards and accolades for his vast contributions to business and technology. He is a Founding Member of the National Association of State Boards of Accountancy's (NASBA) Center for Public Trust (CPT), and is an Executive Member of the SOX Compliance Journal's CEO Roundtable.

He has written books on topics related to J.D. Edwards (with a Foreword by Ed McVaney, the Founder of J.D. Edwards), Sarbanes-Oxley, Dodd-Frank, Corporate Governance, and related topics for such publishers as John Wiley, McGraw-Hill, Prentice-Hall (Pearson) and Van Haren Publishing.

He has an MSc (Technology) and MS (Gold Medal recipient) in Computers, and Ph.D. (ABD) from BITS Pilani in India; and an MBA and MS (summa cum laude) in Finance from Boston College.

For more about him, see his profile at <http://www.linkedin.com/in/anandsanjay> and www.grcg.com.