

From SOX to GRC: Art vs. Science

By Sanjay Anand, Chairperson, SOX/GRC Institute, GRC Group © 2012

Although art and science are often pitted against one another, the lines between the two are fuzzier than one might think. Indeed, the two intersect quite frequently. For example, the rise of modern art in the 19th century dovetailed with a deeper scientific understanding of the ways in which humans perceive color. The science of vision and the development of new pigments arising out of the Industrial Revolution spurred artists to leave their studios and capture the color transformations caused by the ever-changing position of the sun.

The intersection of art and science can also be seen in the regulatory realm. Like watercolors washing away in an unexpected storm, fiscal improprieties at companies like Enron and Worldcom in the early 2000s revealed an essentially blank regulatory canvas. Congressman Michael Oxley and Senator Paul Sarbanes used broad brushstrokes to fill the void. The Sarbanes-Oxley Act of 2002 (known as the Public Company Accounting Reform and Investor Protection Act) was the Senate-approved version of Oxley's House-approved CAARTA (Corporate and Auditing Accountability, Responsibility and Transparency Act).

Due to the ambiguities associated with the SOX Act's implementation – particularly in the realm of Section 404 – those responsible for compliance weren't able to paint by the numbers. Interpreting the SOX Act was initially more of an art than a science, although the available tools were more akin to crayons than a palette of richly hued oils. However, now that the industry has matured, we recognize that SOX was a starting point and are developing a more rigorous approach to business via governance, risk management, and compliance (GRC), which coincidentally rhymes with "science". With GRC, we're now able to capture the nuances of a business vision and employ fine brushstrokes to produce an organizational masterpiece infused with value that adds to the bottom line.

Although CAARTA eventually became the Sarbanes-Oxley Act (which is known by many other monikers) 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.

Basic Definitions

While accountability, responsibility, and transparency are often used loosely and interchangeably, within the SOX Act the three are intended to convey very specific and distinct aspects of GRC.

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 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 “responsibility” 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

Over the past decade, the SOX Act and its country-specific variations (J-SOX in Japan, and the German Corporate Governance Code, for example) have become a globally accepted set of rules, standards, and expectations. SOX implementation has matured, and is now viewed as the launching point for a more sustainable, inclusive and long-term strategy referred to as GRC. GRC stands for governance, risk management, compliance and controls. These are the three key areas that SOX

begins to address, but GRC 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.

Governance

The Organisation for Economic Co-operation and Development (OECD) defines corporate governance as involving “a set of relationships between a company’s management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.”

Risk Management

The Committee of Sponsoring Organizations (COSO) defines risk management as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Compliance and Controls

Compliance can be defined as bringing aspects of an organization into conformance with a regulation or law. This involves training employees, vendors, and other stakeholders about the regulatory landscape, and putting processes in place to ensure that legal mandates are met.

Controls are monitoring processes that are developed and implemented to mitigate risk. While they serve a preventative function, controls also detect wrongdoing, such as corporate fraud, security breaches, and theft. Controls may be manual or automated, and are used to measure the veracity of financial reporting, benchmarks for achieving goals and objectives, and effectiveness in regulatory and legal compliance.

GRC PYRAMID

GRC can be viewed as a pyramid, with governance (G) 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. Good governance, therefore, is the ultimate goal.

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

The foundation of the pyramid is where the paint hits the canvas. 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

Is GRC an art or a science? The answer is simple, considering that the 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→	Accountability	Responsibility	Transparency
------	----------------	----------------	--------------

GRC ↓			
Governance			
Risk Mgmt.			
Compliance			

Integrated GRC

A term often heard in SOX and GRC circles is “integrated GRC.” This essentially refers to the coming together of governance, risk management, and compliance and controls, three disparate areas that 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 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 technological requirements and implementation.

Figure 2: Siloed GRC Approach



Specifically, “integrated GRC” is an approach and a methodology that enables companies to create a harmony within their business processes in terms of how they serve all of their stakeholders (including shareholders, customers, employees, and vendors) 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. This reflects the basic goals and objectives of GRC-related legislation and regulations (such as SOX).

GRC Frameworks

It is a bit of a misnomer to refer to a “framework for GRC,” since GRC itself is a framework. However, implementing (technologically or otherwise) GRC within an organization requires adhering to a methodology that will ensure the greatest possible benefit (A-R-T) with the least possible cost, i.e., maximize the 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 a GRC project forward. Note that with SOX, we do not even attempt to scientifically quantify ROI since SOX is a regulatory requirement sans ROI, and as stated earlier is more Art than Science.

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 of the Treadway Commission in the early 1990’s. 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 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

Conclusion

Is moving from SOX to GRC an art or a science? The process of integrating GRC is both an art and a science, but due to the subjective nature of everything related to business and its stakeholders, it is slightly weighted toward being an art but definitely

more scientific than SOX. It is an enlightening coincidence that SOX's primary tenets of Accountability, Responsibility and Transparency (as espoused in CAARTA) spell A-R-T (see Table 1).

It is important to note that the concept of "integrated GRC" 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 can be achieved by using a combination of people, processes, and technology, 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, and maturity models, ERM serves as the foundation of those models, and therefore, for all practical purposes, organizations do not need to reinvent the wheel and can start with processes already in place for SOX compliance. Hopefully, this suggestion alone will remove some of the fear and intimidation that GRC sometimes poses, and help organizations understand that what they did for SOX is a great first step and an excellent foundation for moving forward toward GRC integration.

ABOUT THE AUTHOR

Sanjay Anand, CSOX, CGRC, is an internationally recognized and renowned expert in Governance, Risk Management, Compliance and Controls (GRC). 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 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.