Dispelling Myths: Facing Reality

The Case for Addressing Governance, Risk and Compliance (GRC) from a Business Perspective

Steve Crutchley
CEO and Founder
Consult2Comply
August 2008

Contents

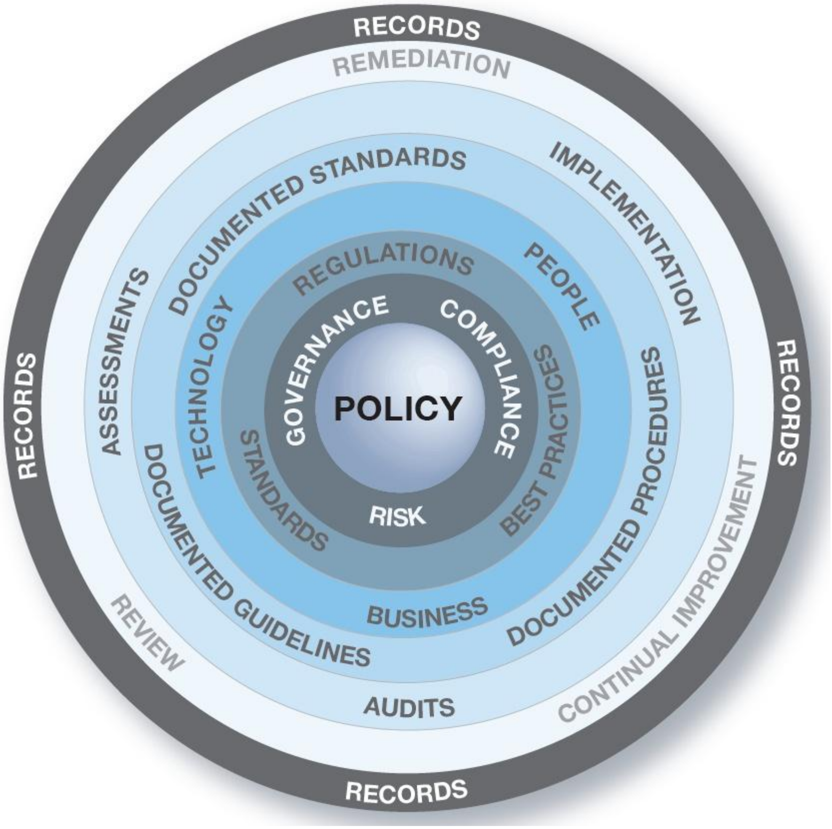
Introduction 3
Consult2Comply GRC Model 3
GRC Rules of Engagement 4
Dispelling Common GRC Myths 5
Definition of GRC Terms 8
Conclusion 10

Introduction

GRC is predominantly Governance Risk and Compliance, but if one delves further into these terms one is faced with many deviations on the theme, including but not limited to legal, audit, Sarbanes Oxley, GLBA, HIPAA, insurance and more. All of these contribute to GRC, but taking each in isolation can lead to legal repercussions. This paper proposes addressing GRC from a business, rather than an IT, perspective. We introduce a GRC Model showing how GRC should be interpreted in organizations; propose “Rules of Engagement” organizations should adhere to for GRC initiatives to be successful; dispel common GRC Myths; define and clarify GRC terminology; and recommend a successful course of action for any organization’s GRC initiatives.

Consult2Comply GRC Model

To help explain GRC requirements, Consult2Comply has created a GRC Model which shows a diagrammatic view of how GRC should be interpreted in any organization. It also provides a view of what should be included in an overall compliance model. Of course there will be logical links to other requirements, but this view is designed to help organizations understand how to determine what they actually *need* to support the GRC initiatives and what they *need to spend* to derive the greatest business value from their efforts.



Consult2Comply GRC Model ©

When starting GRC initiatives, it is imperative to understand organization policy. This is the intent and where the regulatory landscape, risk posture and management responsibilities will be determined. The Consult2Comply GRC model starts with policy and works its way across a myriad of requirements to ensure GRC compliance is being conducted in the appropriate way and can be monitored, measured and managed (the 3 M's of GRC).

Each layer of the model has three specific activities that complement each other and will help the organization understand GRC and the compliance landscape in a practical way. Following this model and understanding each requirement will ensure GRC is met effectively. A more simplistic view is shown in the following table.

Policy – the foundation

Governance	Compliance	Risk
Regulations	Standards	Best Practices
Business	Technology	People
Documented Standards	Documented Guidelines	Documented Procedures
Audits	Implementations	Assessments
Review	Remediation	Continual Improvement

Records – documentary evidence in whatever form they may take

GRC Rules of Engagement

Before embarking on a true GRC initiative, organizations and professionals should adhere to the following rules of engagement to aid their understanding and identification of the appropriate needs required to be successful.

- Information Technology does not dictate the (GRC) compliance initiatives. IT does have a role to play, but the board and stakeholders are the groups responsible to ensure GRC is being met and conducted in the appropriate way throughout the organization.
- Develop your GRC strategy and document your intent.
- Do not "silo" GRC; it's an organization-wide issue. Ensure whoever needs to be involved is involved. Putting Risk in one silo and Legislation in another and Best Practices in another, and not understanding the relationships among them can be detrimental to the overall success of GRC initiatives.
- Understand who will be asking for the budget. Business and IT are in competition for budget – business is most often seen as a contributor; IT is perceived as an overhead – business will normally win the budget battles.
- Unified control infrastructures put a spin on the real controls and potentially cost an organization more money in the long term (too many controls to worry about, and unified control infrastructures are not normally nationally or internationally recognized).
- Set the baseline control infrastructure (e.g. ISO/IEC 27001, CobIT, NIST, and ISF) and work out across the regulations, standards and best practices.

- Do not stop at control infrastructures. Include everything that's needed (e.g. Policy; Procedures; Process Maps; Training Records and so on).
- Do not exclude Management Controls (these tend to be excluded in technology solutions that address IT rather than the business). These are extremely important when understanding responsibilities and metrics.
- Understand the international implications of your GRC initiative (if they apply). Ensure the appropriate regulations, standards and best practices align to the laws of the land nationally and internationally and can work with your organizational requirements.
- Paper mappings (spreadsheets) or out-of-date diagrams are difficult to utilize and use; find something that can automate your requirements.
- Loose mappings do not offer compliance – ensure your mappings are not too high level. Loose mappings tend to skip the actual control and concentrate on the control objective which could mean implementing more controls than necessary.
- Having GRC solutions and associated people in silos is not a good practice to ensure compliance for an organization. A consolidated view is a must, due to the "knock-on" effect if something changes (a new control is implemented; a control is discontinued for whatever reason or changes in the regulation, standards and best practices dictate a major change).

Dispelling Common GRC Myths

It is up to organizations to develop a solid understanding of their specific GRC needs. We have identified fifteen GRC Myths that must be dispelled before organizations can better understand the GRC landscape and identify any shortfalls in their own GRC initiatives. This list is not exhaustive but covers the most important aspects.

Myth #1 - IT is the center of GRC
Reality
IT is not the driver of GRC. Business is the only driver and where the buck stops. IT is only a component of the overall picture.

Myth #2 - It is acceptable to operate GRC in silos
Reality
If GRC is placed in silos, then coordinated efforts will undoubtedly fail. Placement in silos may also lead to political games being played out and competition for budget being fought for and potentially lost.

Myth #3 - Technology is the basis for GRC
Reality
Technology has in reality been a serious contributor to the GRC issues addressed earlier in this paper. Having technology solutions to assist with assessing is a requirement, but remember, GRC must support the people efforts as well. You can't take a firewall to court; GRC is a "people issue" to deal with.

Myth #4 - Risk assessments ensure all GRC requirements are met
Reality
Like IT, Risk is another component of GRC and cannot be depended upon for the final work on compliance across the organization. Risk has many guises; it is imperative that the organization understands the risk methods being employed and that the coordinated results are combined to provide an overall risk posture and understanding to the organization.

Myth #5 - The more controls you have the easier it is to adhere to regulations
Reality
Having many controls to choose from is like going to a restaurant that has an extensive menu. The dilemma is too many choices, and when you eventually order the meal you think you want you quickly find out it's not what you really wanted. Too many controls can drive a company down this road. All of the main control infrastructures are designed to support business and be internationally recognized, providing a good level of assurance and trust.

Myth #6 - Unified Control Infrastructures save money and make life easy
Reality
Unified control infrastructures are a combination of many control infrastructures and have been created primarily to try to ease the use of control infrastructures across an organization. The thought behind unified control infrastructures is to work with only one infrastructure rather than many. Unfortunately, the more controls you create the bigger your problem becomes. There is a saying in the compliance industry, "Every control you implement has a cost to the organization." Using unified infrastructures could force organizations to implement controls where controls are not necessarily needed, incurring unwarranted costs. One GRC technology solutions provider has 2,500 main controls and 10,000 sub controls supporting their infrastructure. To work with this number of controls is a potential issue and can be extremely costly to organizations trying to comply.

Myth #7 - International regulations applied to national requirements is an acceptable practice
Reality
Only the actual laws of the land are acceptable to each area. During Consult2Comply's review process in GRC, we have seen vendors offering alignment to regulation and standards from other countries, specifically Australia and New Zealand – the AS/NZ prefix.

Myth #8 - If a business adheres to regulations alone, the business is compliant
Reality
Regulations are the "tip of the iceberg." (Refer to the Consult2Comply GRC Model and definition of terms for additional requirements.)

Myth #9 - Self Assessment is a waste of time
Reality
Self assessment and self review of results are essential parts of complying with GRC requirements.

Myth #10 - Once a control infrastructure is implemented you can forget it
Reality
GRC is a moving target. GRC must be coordinated throughout the organization to ensure overall adherence. Continual improvement is a specific requirement of GRC activities. Unless

this is undertaken, the chances are your GRC initiatives will become redundant and the organization will be:

- Wasting money, and
- Open to litigious opportunities from the outside.

Myth # 11 - You don't need policy to adhere to GRC
Reality
Policy is the foundation of all GRC activities. Without effective policy there is no intent in the organization to effectively monitor measure and manage GRC. Before embarking on any GRC initiative, ensure policy that supports the initiative is present and has been endorsed by the appropriate management.

Myth #12 - Conforming to certain controls of a control infrastructure ensures compliance to the infrastructure
Reality
Technology solutions have a tendency to offer a compliance score based on a minimal number of controls being implemented in specific areas. These scores can be extremely misleading and provide management with an incorrect assumption on compliance adherence. For example: Physical Security of a computer facility - Locks and controls for physical access ensure conformance to the specific controls but do not offer compliance to the overall standard. In other words, receiving a 77% score for compliance to a standard instead of receiving a conformance score of 77% to the specific controls misleads compliance professionals and provides a false sense of security (In security terms a "false positive").

Myth #13 - People aren't important; technology is the way forward
Reality
People are the mainstay of GRC – Compliance. GRC covers many aspects of the business from hardware, information, software, people, facilities, branding and so on. People are the ones to undertake GRC activities and report on the overall compliance – technology can only support this.

Myth #14 Delegation of accountability and responsibility is acceptable
Reality
This happens all too often. Management must accept accountability for GRC. Responsibility can be delegated but only if there are measures to ensure GRC responsibilities are being met.

Myth #15 – Budget won't be a problem
Reality
Budget is always an issue with Management. Common faults are:

- Buying technology solutions that only serve part of the GRC landscape
- Buying Risk tools that need significant amounts of training for staff before they become effective
- Underestimating the GRC requirements
- Having unskilled or untrained staff responsible for, and actively involved in GRC initiatives
- Employing consultants with little to no skill
- Not having a cohesive strategy in place
- Duplication of effort

Definition of GRC Terms

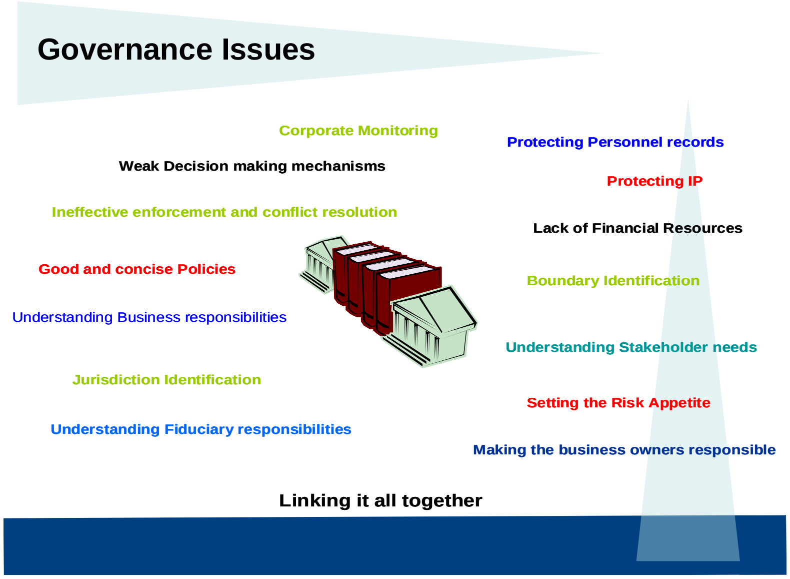
One of the issues facing GRC compliance professionals is gaining a firm grip on terminology. GRC is often risk, governance and compliance for whatever it stands for in a conversation to suit the presenter and listener. Invariably, the presenter and listener have differing levels of understanding which can lead to misunderstandings in both directions. Unfortunately, today GRC is a "buzz word," and the meaning still needs to be understood when listening and projecting a view. My personal view is: set the criteria for understanding before entering into a GRC discussion. If you are talking Governance – understand Governance terminology. When discussing Risk - understand what type of risk is being discussed (for example, business; technology; asset; fraud; operational and so on). If you get confused here you may find yourself struggling later and veering off course with understanding. With Compliance - understand whether compliance or conformance is at stake. Although Compliance and Conformity are closely linked, there are subtle differences. Furthermore, it is important to stress that standards and best practices are *elective* (not mandatory) within an organization, whereas some regulations are mandatory - therefore not *elective*, but *compulsory.*

For the sake of completeness the following glossary and diagrams provide additional information:

Conformity:
- Fulfillment of a requirement being a standard or best practice
- Nonconformity can lead to suspension or revocation of registration

Compliance:
- Fulfillment of legal/statutory requirements
- Noncompliance can lead to fines/incarceration

Governance:
- A method or system of management – the following graphic provides some understanding of what areas need to be addressed when reviewing Governance.



Governance Issues

Corporate Monitoring

Protecting Personnel records

Weak Decision making mechanisms

Protecting IP

Ineffective enforcement and conflict resolution

Lack of Financial Resources

Good and concise Policies

Boundary Identification

Understanding Business responsibilities

Understanding Stakeholder needs

Jurisdiction Identification

Setting the Risk Appetite

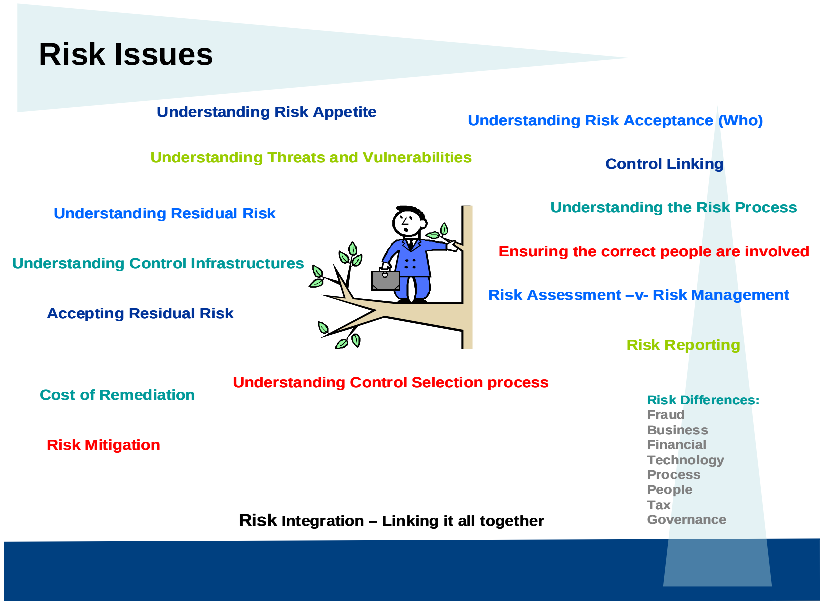
Understanding Fiduciary responsibilities

Making the business owners responsible

Linking it all together

Risk:

- Exposure to the chance of loss – as stated risk comes in many guises - organizations must understand what risk they are trying to mitigate. They must also understand the risk appetite and know what residual risks are acceptable based on the business objectives. When talking Risk – there is operational; fraud; technology; business; financial; people; and asset. The following graphic provides an understanding of what areas need to be addressed when reviewing risk.



Risk Issues

Understanding Risk Appetite

Understanding Risk Acceptance (Who)

Understanding Threats and Vulnerabilities

Control Linking

Understanding Residual Risk

Understanding the Risk Process

Ensuring the correct people are involved

Understanding Control Infrastructures

Risk Assessment –v- Risk Management

Accepting Residual Risk

Risk Reporting

Understanding Control Selection process

Cost of Remediation

Risk Differences:
Fraud
Business
Financial
Technology
Process
People
Tax
Governance

Risk Mitigation

Risk Integration – Linking it all together

Compliance and the Art of Conforming:

Compliance is a complicated and mostly misunderstood discipline. Many vendors have tried to reduce the overall emphasis, offering compliance solutions based purely on technology - based on regulations and standards that fall outside of the jurisdictional borders of where you are in the world - based on combining controls into a unified framework that are not understood or approved by governmental agencies or laws of the land. These issues alone can derail any GRC initiative and cost the organization entering into these supposed “silver bullet solutions” significant amounts of money and resources - achieving nothing.

To reiterate, technical infrastructures do not control and establish compliance in an organization; management must understand the requirements and assure the organization is aligned to the needs of the business objectives and regulatory landscape.

To put overall compliance in perspective, should something go wrong, a firewall *cannot* be taken to court or serve jail time. Management *cannot* admit to being unaware of the laws of the land or to doing their best based on another country’s regulations and standards which do not meet specific jurisdictional requirements. Management *cannot* or *should not* implement unrecognized control infrastructures (unified) due to potential legal liability of unrecognized and unapproved controls being used. Implementing unrecognized control infrastructures also has a “knock-on’” effect - the more controls being implemented costs the organization more to monitor, measure and manage.

It is recommended that an organization’s compliance structure be developed in such a way that it can create and allocate responsibilities for a compliance framework, including applicable and known regulations, risk scenarios, implemented standards and implemented best practices, linked/mapped to policies, procedures and other business-supporting activities to gain an overall view and complete understanding of the business.

Conclusion

Any GRC initiative that an organization undertakes must be given the appropriate priority and not allowed to be worked on in individual silos, such as:

- Business Risk not taking account of the overall business, including IT
- Sarbanes Oxley compliance being implemented and isolated from other processes that could take advantage of the implementation
- IT undertaking GRC initiatives without the appropriate knowledge of the overall business objectives
- Management standards being implemented without effective involvement of affected parties

It is also recommended that organizations address the myths surrounding GRC, recognize the importance of GRC, and act accordingly by:

- Understanding the GRC landscape effectively
- Developing a cohesive strategy, including mappings for needs
- Assigning responsibilities to appropriate personnel and monitoring, measuring and managing
- Using the actual regulations, standards and best practices
- Utilizing actual controls infrastructures rather than unified controls
- Not letting GRC initiatives be dominated by IT issues and technology
- Involving all stakeholders in the process
- Assessing and auditing on a regular basis
- Making adjustments where necessary
- Continually improving the process

In conclusion, organizations that act in this business-focused and responsible manner will have effective strategies and solutions in place to help them achieve, manage and maintain compliance to regulations, standards and best practices in accordance with the laws of the land and conformant to their stakeholders’ “needs and wants.” Achieving this will also provide the capability for compliant business opportunities worldwide (trading successfully in the global village).

Steve Crutchley, Chief Executive Officer and Founder, Consult2Comply
A serial entrepreneur, Steve's string of successes include the sale of his previous venture 4FrontSecurity to Symantec, the sale of Systems Solution to AST in South Africa which culminated in the listing of the respective company and the subsequent acquisition of a number of local and international businesses.

Steve is a recognized leader and foremost authority in the field of compliance, risk and governance. With more than 25 years experience in Business Protection, combined with an extensive knowledge of the industrial, commercial, government and financial areas, Steve has dedicated his career to be highly focused on risk, governance, compliance, information security and information assurance.

Steve has held senior positions in government, corporate and private businesses for many years and has a solid track record of prior achievements. In a sector where the noise is mixed and confusing, Steve is able to help organizations navigate through the business protection (security) and compliance maze and assist them to select and deliver the processes and solutions that will mitigate risk and support corporate governance. Steve has extensive experience, knowledge and deep understanding of various standards and control structures such as ISO 20000 ISO27001, BS 25999, COBIT, ISF, COSO, GLBA, HIPAA, NERC, PCI to mention just a few. Steve is an accredited IRCA trainer for ISO/IEC 27001, a renowned Lead Auditor and implementer for ISO 27001, ISO 20000 and BS 25999. Steve is also CISM and CGEIT and holds a Bachelor of Science in Management Information Systems (B.Sc. Management Information Systems) with the concentration in Information Security.

Consult2Comply
Consult2Comply delivers innovative Governance, Risk and Compliance (GRC) products and consulting services to organizations that help them simplify compliance, build business value, measure and manage information, and restore confidence and trust. Consult2Comply draws on its subject-area experience, expertise and global perspective to deliver comprehensive compliance solutions and strategies which enable organizations to achieve, manage and maintain compliance to National and International Regulations (Sarbanes-Oxley/HIPAA/Basel 2), Standards (ISO/IEC 27001/20000/38500 and BS25999) and Best Practices. The company has developed a set of industry leading tools that offer high functionality and exceptional value to help simplify an organization’s assessment, implementation, and management of GRC, resulting in significant savings in time and expense. With headquarters in Herndon, Virginia, an office in the United Kingdom, and a global network of partners and affiliates, Consult2Comply can support simple or the most complex GRC engagements. For more information visit: www.consult2comply.com or call 703-871-3950.