White Paper

Collaborative Accountability in Governance, Risk, & Compliance: Creating Harmony Across Business Roles

Mitratech Holdings, Inc.
5900 Wilshire Boulevard, Suite 300
Los Angeles, CA 90036
(800) 445-0924
www.mitratech.com
info@mitratech.com

Copyright © 2010 by Mitratech Holdings, Inc.
Executive Summary

- Collaborative Accountability brings the individual areas of governance, risk, and compliance (GRC) into harmony. It enables different areas of the business to be accountable while promoting collaboration and information-sharing for a holistic view across the business.

- Collaborative Accountability Applications designed for GRC give the business a complete system of record — providing accountability, efficiency, and effectiveness across business processes, roles, and relationships.

- The governance roles of the corporate secretary, board of directors, executives, and audit are the aggregation point for a Collaborative Accountability Application for GRC. They are concerned with the consolidation of corporate performance, compliance, and risk metrics communicated to stakeholders, which becomes a permanent record when entered into corporate financial statements and reports.

- Legal and regulatory compliance is one of the most significant risk challenges to the organization with rapidly increasing requirements that burden business, along with increased penalties and aggressive regulators around the world.

- A manual and ad hoc approach to GRC results in poor visibility, high costs, and error prone processes across the organization and its control environment, since there is no framework or architecture for managing risk and compliance as an integrated part of business.

- A common GRC technology architecture provides accountability and allows risk and compliance processes to deliver on business agility, efficiency in human and financial resources, and effectiveness in meeting requirements. As such, GRC applications help protect the integrity of the organization while enabling it to carry out core functions.

- Intricate relationships and presentation of risk and compliance information is the heart of a successful GRC Collaborative Accountability technology architecture. Policies, risks, controls, events, requirements, enterprise assets and processes, responsibilities, and objectives all map to one another. A GRC application designed for Collaborative Accountability allows the organization to achieve: (1) agility; (2) consistency; (3) efficiency; (4) transparency; and (5) accountability.

- Achieving value and economies of scale in GRC through Collaborative Accountability requires a common user experience and seamless application and data integration across GRC modules. Such value and economies are achieved when the GRC suite of applications delivers a common: (1) User and role-centric experience; (2) workflow and task management model; (3) environment focused on flexibility; (4) integrated security model; and (5) collaborative and information-rich experience.
## Contents

Executive Summary .......................................................................................................................... 2  
Contents ........................................................................................................................................... 3  
GRC Harmony through Collaborative Accountability ................................................................. 4  
   Harmony – Not Discord: Critical Roles Working Together ........................................................ 4  
   Changing Approaches to Corporate Governance .................................................................... 6  
   Business Challenged by Risk and Compliance ....................................................................... 7  
   Manual Processes Drive Inefficiencies and Raise GRC Costs ................................................ 7  
Enabling Collaborative Accountability Through a GRC Technology Architecture ............... 8  
   GRC Technology Delivers Agility, Efficiency, and Effectiveness ........................................... 8  
   Enabling Enterprise Visibility and Accountability ................................................................. 10  
   Key Components of a Collaborative Accountability Platform .............................................. 11  
Conclusion .................................................................................................................................... 13  
About Mitratech ............................................................................................................................ 13
Collaborative Accountability in Governance, Risk, & Compliance: Creating Harmony Across Business Roles

GRC Harmony through Collaborative Accountability
Harmony - Not Discord: Critical Roles Working Together

The challenge for organizations from top to bottom is to provide harmony between silos of governance, risk, and compliance. Maintaining harmony is vital: Different roles — such as legal, risk mitigation, audit and compliance — have different and unique purposes, but must remain in tune with each other.

The goal of high-performance GRC is to drive accountability, efficiency, effectiveness and agility across its processes to support a dynamic and extended business environment.

Collaborative Accountability brings the individual areas of governance, risk, and compliance into harmony. It enables different areas of the business to be accountable where they excel without dominating others, while promoting collaboration and information-sharing to achieve a holistic view of GRC across the business. Consider the following roles and how they can collaborate to provide a comprehensive view of governance, risk, and compliance:

**Legal**: Today’s corporate legal environment demands that general counsel effectively balance a growing portfolio of litigation and internal investigations, while being held to the same operating standards and performance metrics as other areas of the business. The demand for greater business agility and responsibility in legal operations drives the need to connect disparate team members including outside counsel, experts, compliance, risk, and the CFO, while providing a finely-tuned system to track and manage all of the many related processes.

**Corporate secretary**: The burdens of risk and compliance oversight fall squarely on the board of directors and senior executives of the organization. In an environment focused on placing accountability on corporate officers and directors, corporate governance roles are tasked with seeing the big picture of risk and compliance.

---

1 The official definition for GRC is from the OCEG GRC Capability Model (www.OCEG.org).

Copyright © 2010 by Mitratech Holdings, Inc.
The corporate secretary is the focal point of consolidating GRC-related information to communicate to the board and stakeholders.

**Corporate compliance:** The corporate compliance department faces the challenge of integrating disparate compliance processes and sources of information across the enterprise. Compliance must comprehend and demonstrate adherence to external laws and regulations, as well as corporate policies and procedures. A manual approach to compliance management hinders the organization from forming an accurate, real-time view of the compliance landscape and delivering information to executive leadership and regulators on short notice.

**Finance:** Finance executives struggle to define internal controls, assess those controls, respond to internal and external audits, defend financial performance results to stakeholders, maintain segregation of duties, and overall insure the accuracy and integrity of financial reporting processes. This takes a toll on the business, which must respond to frequent assessment and validation requirements. Finance executives must stay abreast of financial risk and internal control over the accounting processes.

**Information technology:** IT has typically focused on deep technical risk and compliance challenges — attempting to keep hackers, viruses, and worms at bay and systems in a state of recovery in the event of a disaster. IT is struggling to build its legal acumen to comply with increasingly complex laws and regulations impacting information, and how it is protected and presented throughout the enterprise.

**Audit:** Auditors are in a state of flux — audit programs are going beyond the validation of controls and financial statements. Auditors today are challenged to validate the structure, processes, policies and controls across a number of domains of governance, risk, and compliance. Auditors are required to understand and validate a number of business domains beyond the financial and accounting processes they have traditionally assured. The job is taxing, as it requires a level of understanding and analysis to detect what is unseen. Auditors must know how to evaluate the design and effectiveness of the organization’s control environment.

**Risk:** Risk managers understand the challenges of integrating disparate sources of information across the enterprise to form an aggregate view of operational, strategic, financial, and security risks. However, there has been an over-reliance on spreadsheets and email as primary tools for conducting risk assessments, collecting information, and reporting risk data. Unfortunately, these tools do not provide an effective way to correlate assessments or monitor risk trends within critical business infrastructure. With a growing focus on operational risks, risk managers are extremely challenged to reinvent their role and processes.

**Line of business:** The line-of-business bears the brutality of GRC silos bearing down on it with individual assessments, policies, and controls. It is the line-of-business that has to respond to different GRC assessment and reporting processes pushed on it from other roles. The line-of-business also holds the front line of managing other GRC issues such as quality, environmental, health and safety, and labor practices. The line-of-business demands efficiency, and wants to move from an “ask many answer many” state of GRC assessments to an “ask once answer many” state of GRC, where assessments are streamlined by a collaborative and common process and technology architecture.
This new approach to GRC seeks to correct the scattered and siloed methods of the past that introduced greater risk and regulatory threats to the business. Correcting an outdated GRC strategy means understanding:

- Has the organization been operating efficiently (from both human and financial perspectives), effectively meeting internal and external requirements, and with proper agility for a dynamic and extended business environment?
- Does the current approach make sense, or are there better ways to do things that bring greater process efficiency?
- Is there clear accountability and collaboration across GRC areas in the organization?

GRC applications designed for Collaborative Accountability give the business a complete system of record — providing accountability, efficiency, and effectiveness for GRC across business processes, roles, and relationships.

**Changing Approaches to Corporate Governance**

Increased pressure for governance oversight is drawing board-level attention to how collaboration and accountability is distributed across operations. The board of directors is rolling up their sleeves and becoming more involved as directors face greater personal risk and responsibilities. Further,
organizations face weariness with increased regulatory actions, the risk inherent in a highly competitive
global environment, corporate litigation, demands of corporate social responsibility, as well as
stakeholder and shareholder retaliation.

The governance roles of the corporate secretary, board of directors, executives, and audit are
responsible for making sure the organization is on course and meeting strategic plans and objectives,
while staying within defined boundaries of laws, regulations, values, and code of conduct. These roles
are the aggregation point for a GRC application designed for Collaborative Accountability. They are
concerned with the consolidation of corporate performance, compliance, and risk metrics
communicated to stakeholders, which becomes a permanent record when entered into corporate
financial statements and reports.

**Business Challenged by Risk and Compliance**

Risk to the business is like the hydra in mythology — organizations combat risks to find new ones taking
their place. Executives battle to find, manage, and monitor risk that is pervasive throughout the
organization. If risk management is an ad hoc process without clear processes and structure for
Collaborative Accountability, the organization will soon find itself in peril as it lacks integrated risk
oversight, and demands little or no accountability.

Organizational complexity and the distributed nature of business make risk management all the more
difficult. This is particularly evident as organizations expand operations, their risk profile grows
exponentially. Organizations need to stay on top of the game by monitoring risk to the business internally (internal controls and processes) and externally (competitive, legal, and geographic environments). Success in global business requires an organization to be keenly aware of global financial markets, economic directions, environmental issues, global supply chains, and more.

Legal and regulatory compliance is one of the most significant risk challenges to the organization. One
large international bank recently catalogued more than 80,000 regulations they must comply with
around the world. Just within the U.S., there are more than 3,000 employment and labor laws and
regulations across federal, state, and local jurisdictions. Organizations face an expanding regulatory
environment with rapidly increasing requirements that burden business, along with increased penalties
and aggressive regulators around the world. Management is all too familiar with terms such as non-
defered prosecutions, consent decrees, and corporate integrity agreements.

Compliance is not just about meeting requirements of external mandates — it is also concerned with
accountability across the business, to keep it within voluntary boundaries of ethics, values, code of
conduct, and a culture of risk-taking and management. Additionally, reputation and brand protection is
a significant compliance and risk management issue in today’s distributed business environment. Clients
want to trust in the values and integrity of the organizations they do business with. Businesses want to
make sure business partners share the same values as their brand, and are in line with what they have
communicated to their clients.

**Manual Processes Drive Inefficiency and Raise GRC Costs**

With new risk and compliance issues constantly coming to bear, organizations need to tackle the
problem at its roots — defining a structure of collaboration and accountability across GRC processes.
This requires a common GRC methodology, framework, process, and technology architecture to manage
governance, risk, and compliance across the range of issues burdening the business.

Copyright © 2010 by Mitratech Holdings, Inc.
The old paradigm of reactive with fragmented risk-management is a recipe for disaster. A reactive approach leads to siloed initiatives that never consider the big picture. The result is complexity, redundancy, and failure. These outdated processes do not look at how accountability processes can be architectured to meet a range of risk and compliance needs, nor do they gain an understanding of how risk management and compliance impact corporate performance. An ad hoc approach to GRC results in poor visibility across the organization and its control environment, as there is no framework or architecture for managing risk and compliance as an integrated part of business.

Enabling Collaborative Accountability Through a GRC Technology Architecture

GRC Technology Delivers Agility, Efficiency, and Effectiveness

Whether the enterprise uses the “GRC” acronym or not, the fact is, every organization practices GRC. There is not a single executive that will tell you that they lack corporate governance, do not manage risk, and completely ignore compliance. The truth of the matter is, GRC has been here since the dawn of business.

In today’s environment, ignoring a Collaborative Accountability view of GRC results in processes, partners, employees, and systems that behave like leaves blowing in the wind. Risk and compliance issues and corresponding processes are constantly coming to bear on the business. GRC solutions that operate autonomously introduce further risk in today’s complex, dynamic, and distributed business environment. Organizations require an enterprise view of GRC accountability and collaboration that not only brings together silos, but integrates them into a common GRC process.

A targeted strategy that addresses GRC through a common technology architecture gets to the root of the problem, and delivers cost savings and efficiency. A common GRC architecture provides accountability and allows risk and compliance processes to deliver on business agility, efficiency in human and financial resources, and effectiveness in meeting requirements. Organizations implement a GRC application designed for Collaborative Accountability to achieve an enterprise view of risk and compliance, with a specific need to identify interrelationships in today’s complex and distributed information and processes. This requires that GRC initiatives involve a federation of professional roles — legal and compliance, risk, audit, IT, finance, finance, etc.

The Cost to the Business

Some areas where organizations report significant issues and cost include:

Excessive paper and spreadsheets: Organizations rely on manual paper trails, email, and spreadsheets to deliver surveys and assessments with little to no accountability or follow-through. This approach lacks a clearly defined audit trail, and does not allow for non-repudiation. It’s not possible to verify that someone who answered a question did not change their response later to cover a trail, get themselves out of trouble, or paint a rosier picture. Multiply this by the thousands of documents and emails that manage risk and compliance and it grows quickly out of control.

Limited and fragmented reporting: Trying to make sense of data collected in manual processes and electronic documents is a nightmare. How do you aggregate and provide meaningful reports from hundreds or thousands of disparate sources of information? The answer: A lot of labor and time.

Files and documents out of sync: Adding to this behemoth of labor is the effort to track and control versions of all of these documents, which quickly become out of sync and lose relevance to the organization. The accuracy and relevance of the information being reported soon comes into question.

Significant spend on auditors and consultants: Legions of out-of-date documents mean more work for auditors and consultants who come in to validate and attest to risk and compliance practices. The more incomplete, inaccurate, and complex sources of data they have, the more these resources cost.
and the line-of-business among others — working collaboratively to define common processes and accountability. It also involves implementation of GRC technology that shares a common technology architecture.

Diagram 2 – As with any enterprise process, it is possible to realize a future state where GRC processes are organized, streamlined and efficient. Organizations that accomplish this will unlock hidden value and help drive toward their enterprise objectives. Source: OCEG Illustrated Series

GRC applications designed for Collaborative Accountability help respond to and manage a growing body of risk and legal processes and mandates, while providing deep visibility into actions by team members and related expenditures. It represents a fusion of the features of traditional groupware tools with granular tracking of tasks, events and communications, and is enabled by multifaceted access control. Collaborative Accountability GRC software implementations are a command center, enabling policy makers to map policies to regulations, information security managers to review metrics and enforce controls, and legal professionals to defensibly identify and protect confidential data. As such, they protect the integrity of the organization while enabling it to carry out core functions.

A GRC strategy focused on Collaborative Accountability enables organizations to proactively protect the organization by aggregating and reconciling risk and compliance with multiple regulations and requirements, the policies that result from them, and the processes that ultimately monitor and control them. GRC systems help manage the effectiveness of those controls by enabling precise tracking and reporting. When risks materialize or there are incidents to respond to, Collaborative Accountability enables team members inside and outside the enterprise to securely work in concert, while leaders track actions in a manner that can be safely offered into evidence during a legal proceeding. Giving all
GRC team members ready access, while limiting that access to only to the information required for their role, allows the team to react swiftly while containing threats to the organization.

**Enabling Enterprise Visibility and Accountability**

The solution to GRC’s Collaborative Accountability requirements is a process automation platform — a single, secure, process-oriented platform that manages GRC processes, incorporates multiple legal and regulatory mandates, provides accountability through task management and audit trails, and facilitates collaboration across these roles and their external relationships.

Adopting a GRC application designed for Collaborative Accountability allows the organization to reduce the risks associated with the constant changes that directly impact and drive the business, manage risk holistically, and demonstrate compliance with a variety of regimes while keeping a close watch on the overall spend.

A GRC application designed for Collaborative Accountability is akin to the customer/client relationship management (CRM) systems of the 1980s. Before CRM systems and processes entered the organization, client information and relationships were still being managed. The challenge was that they were being managed in scattered silos that created inconsistent and redundant data, with no view of the entire profile of the client and its interaction with the business. CRM systems entered the picture to create a single view of customer information and interaction across business processes and roles. GRC systems and processes aim to achieve the same thing — an integrated picture of governance, risk, and compliance information and processes across the business. An integrated view of GRC requires establishment of business processes and technology architecture.

Intricate relationships and presentation of risk and compliance information is the heart of a successful GRC Collaborative Accountability technology architecture. Policies, risks, controls, events, requirements, enterprise assets and processes, responsibilities, and objectives all map to each other. Organizations must know:

- Which policies set management thresholds for specific risks.
- Which events violate specific policies, materialize risk, and cause infractions to regulatory requirements.
- Which controls are established for specific policies and are defined to control specific risks.
- Which business objectives and risks are related to multiple parts of the enterprise.
- How to monitor controls to stay within acceptable tolerance levels of risk, while aiming for objectives.

A GRC application designed for Collaborative Accountability allows the organization to achieve:

**Agility:** Organizations demand a sustainable process and infrastructure for ongoing governance, risk, and compliance processes that have become onerous. Further, organizations need to sustain their risk and compliance management practices on a continuous basis, as business continues to change rapidly. Point-in-time assessments are no longer good enough by themselves. Business changes hour-by-hour and minute-by-minute. The dynamic nature of business demands that an organization address GRC collaboratively and continuously.
Consistency: Organizations require that multiple roles in the organization work together in an integrated framework and technology architecture. Multiple GRC players must understand how their roles fit into the big picture. Consistency must be part of the technology environment where risks, requirements, and controls are defined and directly integrated into business processes and enterprise applications. Effective GRC gets everyone to play their positions out of the same playbook.

Efficiency: The line-of-business is pushing back on redundant assessments, policies, controls, and audit processes. Calls for similar information for different purposes prevent the business from getting business done. Redundant document-centric processes have a negative economic impact on the business. GRC, done correctly, eases the burden on business by leveraging common processes, assessments, and information through technology integration and enablement.

Transparency: Business demands transparency across key performance and risk indicators to monitor the organization’s health, take advantage of opportunity, and avert or mitigate disaster. Corporate performance management is tightly related to risk management.

Accountability: Organizations are in the hot seat — multiple risks, mandates, and requirements are attacking it from every angle. It is the organization’s responsibility to manage GRC issues effectively, efficiently, and responsively. This requires a system of accountability where executives can see the status of GRC issues, events, incidents, and unresolved findings, and hold individuals accountable for their resolution. Organizations must be able to see the big picture, and drill down into specific GRC areas. When issues arise, a lack of accountability and ownership of specific issues is a warning sign for regulators or investigators to dig deeper.

Key Components of a Collaborative Accountability GRC Platform
A GRC solution delivering on Collaborative Accountability integrates multiple processes such as risk, policy, audit, and investigations management. The ability to share and leverage information between these processes is critical. A less obvious and often overlooked key to GRC success lies in the integration and consistent design of each application. GRC systems lacking a common architecture (backbone), common user interface, and consistent processes and functional behaviors seldom deliver the full value and benefits sought by the organization. In fact, use of a collection of disparate GRC applications has been repeatedly demonstrated — in real-world settings — to actually reduce visibility and increase risk.

Organizations looking to achieve value and economies in GRC through Collaborative Accountability include:

- Apply a common vocabulary, approach and, ideally, technology architecture to GRC processes.
- Coordinate activities that ensure a flow of consistent information throughout the organization and enhance efficient use of resources.
- Recognize and use the benefits of GRC processes embedded in an organization’s operations.

This requires GRC architecture with a common user experience and seamless application and data integration across GRC modules. Specifically, value and economies are achieved when the GRC suite of applications delivers a common:

Copyright © 2010 by Mitratech Holdings, Inc.
User and role-centric experience: The GRC application should meet the needs of each user accessing it, with relevant information, tasks, and processes specific to the business role. These must be readily available in the application without having to wade through a great deal of irrelevant information. With a common user interface, employees only need to learn one method of interacting with all of the applications. Frequently-used features such as save, copy and edit behave consistently, and text fields (such as names, addresses and descriptions) are in the same location on screens with the same data entry process.

Workflow and task management: GRC is about relieving the burden with consistency across risk and compliance processes. A GRC application needs to automate business processes through workflows and elimination of information redundancy. Consistent risk and compliance management is essential to achieving value. A full-featured workflow engine automates conditional task assignments and sequencing based on specified criteria. With a common workflow engine used throughout applications, rules and processes have consistent behavior. Users enjoy consistent application performance, resulting in less frustration and faster adoption. Administrators only need to learn one method for maintaining custom workflows, resulting in reduced training time and support costs, and enhanced productivity.

Environment focused on flexibility: The GRC application must adapt to the business. Collaborative Accountability GRC architecture not only allows for consistency, but also provides agility in adapting GRC processes to a changing business landscape. When the organization deals with multiple applications that lack a common architecture, GRC becomes rigid and slows down the business.

Common integrated security model: Like workflow, security models are necessary and can be very difficult to implement. Nothing is more important in GRC applications than ensuring confidential information is well protected. A common security model ensures the company’s security rules are applied consistently. A system that requires multiple security models increases the risk of mistakes that can lead to damaging breaches.

Collaborative and information-rich experience: GRC is ultimately about reducing redundancy across disparate risk and compliance processes, so the organization has greater oversight. This requires a GRC architecture that facilitates collaboration across business roles and presents information with respect to intricate relationships and within the appropriate business context. Application performance, flexibility and security are maximized only when all data resides in a common, centralized database. Disparate databases often result in slower system performance, duplicate data, increased administration overhead, additional security risks and limited flexibility to support changing requirements.

GRC applications designed for Collaborative Accountability are intended from inception to manage all departments, divisions and related companies in one common framework. A well-conceived and soundly engineered GRC platform enables policies and procedures, documents, filings, controls, assessments, surveys and other assets to be shared and managed across multiple entities (companies, divisions and departments) as needed, or restricted to just one entity when appropriate.

Business today requires a GRC application platform designed for Collaborative Accountability that is context-driven and adaptable to a dynamic and changing business environment. Simply put, a Collaborative Accountability approach to GRC enables a better-performing, less costly, more flexible solution.
Conclusion

Legal and regulatory compliance is one of the most significant risk challenges to the organization. Organizations face an expanding regulatory environment with rapidly increasing requirements that burden business operations, along with increased penalties and aggressive regulators around the world. Governance, risk, and compliance (GRC) is a system of people, processes and technology that enable an organization to navigate and fulfill the many expectations that are mandated by law and voluntarily imposed upon itself. Collaborative Accountability brings those individual areas of GRC into harmony. GRC applications designed for Collaborative Accountability give the business a complete system of record, providing accountability, efficiency, and effectiveness across business processes, roles, and relationships. Collaborative Accountability GRC software implementations act as a command center, enabling policy makers to map policies to regulations, information security managers to review metrics and enforce controls, and legal professionals to defensibly identify and protect confidential data. As such, they protect the integrity of the organization while enabling it to carry out core functions.

About Mitratech

Mitratech provides market-leading Collaborative Accountability Applications for businesses and their trusted partners. With team-oriented domain applications in legal process automation, governance, risk, compliance and security, Mitratech's TeamConnect® Collaborative Accountability Suite improves transparency of financial reporting, reduces exposure to risk, sharpens operating discipline, improves information security and the efficiency of enterprise processes.

Our Collaborative browser application also meets the accountability and collaboration needs of proliferating extraprise teams, wherein vendors, partners and service providers often have to be included in sensitive teamwork projects such as electronic billing, legal hold and collaborative budgeting, or those which expose your business to liability. To learn more, visit www.mitratech.com.