

2008

An IT Governance IT Risk and IT Compliance Management Challenge

IT GRC Management

“A considerable number of organizations are bouncing back and forth between the awareness and corrective phases”



Mauricio Mulé

October 2008

An IT Governance, IT Risk and IT Compliance Management Challenge!

Today, Information Technology (IT) groups are required to fulfill many needs and unique challenges within their respective organizations. Originally, IT's role was to align with corporate objectives and policies to deliver what the business demanded for the firm to function and prosper. With the advent of compliance and regulations for public entities, IT's role expanded to address IT Governance, IT Risk, and IT Compliance Management (IT GRCM). In the current business environment, companies must proactively identify and mitigate risk to maintain brand reputation while effectively servicing their customers.

Throughout the industry, analysts, business executives, and third-party vendors agree that IT GRCM are closely coupled disciplines and in turn, often grouped together in enterprise deployments. The objective of IT GRCM solutions is to help firms to align their IT Governance Policies to Regulatory Compliances. Unfortunately, IT GRCM initiatives are frequently scattered across the enterprise and managed through spreadsheets and manual processes. Companies are struggling to correlate assessment results, monitor risk trends and gauge their overall compliance posture since many organizations lack a centralized, automated tool for performing risk assessments.

One rather large challenge many organizations face when deploying IT GRCM solutions is being subjected to the vast selection of technological tools and services which addresses IT GRCM on various levels. Many attempts to implement these tools and services in a holistic manner often come up short and leave out some critical variables in their applied approaches due to:

- Redundant efforts.
- Inefficient resource allocation.
- Absence of balance and unwanted strengths in one area of Governance or Risk or Compliance Management.
- Focusing on completely re-engineering the business rather than leveraging the current infrastructure in place. Vendors have '*the perfect solution*'. You need to start from scratch and do it their way.
- Lack the right measures to provide clarity on what really needs to be done and the magnitude of the scope of the effort. Usually out of the scope of the tool or service.

Evolution of IT GRCM

The various approaches to IT GRCM have evolved over the years and will continue to do so with more requirements whether from the IT Governance, IT Risk, or IT Compliance perspective. Initially, organizations manage IT Governance, IT Risk, and IT Compliance Management as individual entities and are not integrated. In this early stage, projects involving IT Governance tend to be initiated by the internal IT group and projects related to IT Compliance initiated by the business-side leaving the IT group the difficult task of trying to aggregate, normalize and report on the firm's risk exposure. This is represented in *Figure 1*.



Figure 1. IT GRCM managed as Individual Entities

As organizations recognize the overlap of requirements across all three disciplines, a basic holistic approach to IT GRCM where a process-flow is incorporated across all three disciplines as represented in *Figure 2*. Organizations will have policies and controls in place to help minimize risk and demonstrate compliance. The first step entails ensuring Governance polices includes regulatory Compliances. Next is creating Governance controls to identify vulnerabilities and to start to ascertain potential risk. Once the risks are identified, they are matched against the Governance Risk Posture to derive an action plan (risk assumption/mitigation). This is a good model where all logical components are connected, but also is lacking:

- Does not provide a centralized firm wide Governance Policy depository.
- Does not allow to effectively translating assessment vulnerabilities to Risk Exposure.
- Does not provide real time risk exposure information to dynamically update the firm’s Risk Posture.
- Does not provide real time Risk Analysis to proactively mitigate risk.
- Does not provide Risk Exposure moving averages in response to answering basic questions:
 - Is the firm’s risk exposure better or worse than last month, six months ago, a year ago?
 - What is important?
 - What should we be concerned about?
 - How concerned should we be?
- Cannot monitor the effectiveness of projects created to mitigate risk.

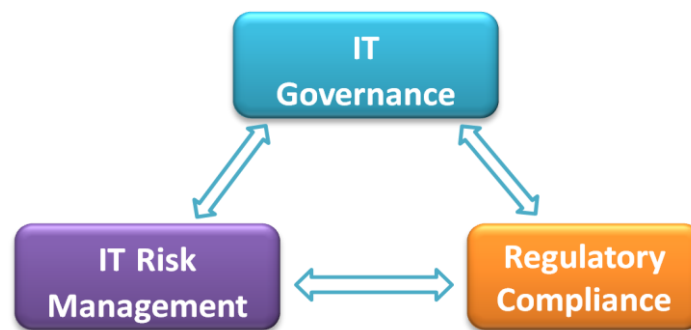


Figure 2. IT GRCM - Beginnings of a Holistic Approach

Most IT GRCM Projects Fall Short

Risk Management and security groups are faced with constant changes from business requirements, policies, compliance, and reporting requirements from an audience with increasing levels of sophistication. They want to know current risk exposure levels in specific areas of concern, determine where these risks come from, what can be done to mitigate it, and determine if they are proactively managing risk as per the firm’s Risk Posture.

These questions often cannot be answered from within a typical IT GRCM deployment because its main function is one of discovery, awareness and basic reporting. It does not include planning, analytics, or forecasting, essential components of performance management tools. In this time of fast changing markets, organizations need to incorporate performance management methodologies into their IT GRCM solution to remain competitive and one-step ahead of the competition.

As reported by Gartner, “Organizations are taking longer to move through the corrective phase than originally anticipated.”

Source: Gartner Compliance & Risk Management Summit
March 3-5, 2008 Sheraton Chicago Hotel & Towers - Chicago, Illinois, Tom Scholtz and Paul Proctor

“An important trend observed during 2006 was that it is taking organizations longer to move through the corrective phase than originally anticipated.

Hence, we have reassessed the percentage of organizations that will have achieved operations excellence during 2007 down to approximately 10%.

Furthermore, not all organizations complete the maturity journey. A sizable number of organizations regress in their practices. Reasons for falling back in maturity include:

- *Not effectively communicating the progress and value of the program, resulting in premature budget cuts*
- *Losing focus, with projects going down the wrong tracks, resulting in rework*
- *Leadership change, resulting in new managers wanting to establish their own, new regimes*
- *Too much focus on technology solutions at the expense of the "softer" issues, such as process, policy, awareness, governance and culture*
- *General return to complacency, resulting from reduced pressure because of less publicity of security incidents and compliance issues*

These factors result in a considerable number of organizations bouncing back and forth between the awareness and corrective phases.”

An Optimal IT GRCM Solution

Changing the perspective from “what had happened - what is happening” to “what we want to happen - what is the gap now” shifts decision makers from simply monitoring what is happening in the business to understand why it is happening. This is achieved by the incorporation of additional two components in the IT GRCM solution as represented in *Figure 3*:

1. Enterprise Project Management – Project Portfolio Management

- **Enterprise Project Management (EPM)** enables organizations to more effectively manage and coordinate work from one-time projects to complex programs across the entire IT GRCM project lifecycle. The added intelligence of EPM allows for management of resources effectively, promotes continuous improvement, gets more from existing technology investments, drives real return on investment, and enables you to take the necessary actions in a timely fashion.
- **Project Portfolio Management (PPM)** allows organizations to automate and enforce governance process, support best practice methods, capture all IT GRCM investments within a central repository, objectively prioritize IT GRCM strategies, effectively prioritize and evaluate competing investments, optimize budget and align selected investments with business strategies, measure and track portfolio performance, consolidate and analyze projects across the firm’s IT GRCM initiatives.

2. Business Performance Management (BPM)

The main function of Business Performance Management regarding IT GRCM is to monitor the efficiency and effectiveness of Risk Mitigation initiatives. After the firm defines and establishes their IT GRCM Management program and identifies the gap between the current organization’s Risk Exposure and Risk Posture, the gap will bring to light metrics requiring corrective action. Thus, current projects are reviewed and new projects are initiated to create a Portfolio of Projects aligned with the IT GRCM initiative. This allows for real time evaluation of the current risk treads, regulatory policies, changes in Governance and Risk Posture, and maintaining a balance between Risk Exposure, Risk Mitigation and Risk Assumption. It provides answers to questions such as:

- What is the current Risk Exposure?
- Are we better off or worst of than last month, last quarter, last year?
- How has the IT GRCM budget been allocated?
- What is our Risk Exposure trend at this time?
- What are the main vulnerabilities?
- How effective are our controls?
- Who is responsible to manage a particular metric?

Some of the benefits of incorporating Business Performance Management include:

- Determining the importance of the metrics presented.
- Identifying the magnitude of the measured risk.
- Identifying outliers and areas of concern.
- Identifying the potential impact of the metrics.
- Determining the IT GRCM effectiveness condition of the firm.
- Maintaining metrics baseline to support trend analysis.
- Trending using Key Risk Indicators (KRI) to alert before risk thresholds are exceeded.
- Providing real or near-real time risk and compliance status dashboards.
- Continuously monitoring progress and results of risk mitigation initiatives.
- Providing IT GRCM reports for regulation and mandated compliance.
- Providing feedback information promoting focus on successful action and increasing effectiveness and efficiency.

Phases	IT GRCM Requirements	Tools and Processes
Planning	What do you want to happen?	BPM and EPM
Executing	Carrying out your plans.	BPM, EPM and PPM
Monitoring	What is happening now?	BPM - Data Collection and Integration - Data Analysis - Dashboard ↔ Scorecards ↔ KPIs / KRIs ↔ Metrics
Analyzing	Why it is happening?	BPM - Data analysis - Business Intelligence - OLAP cubes - Decomposition Trees - Heat maps - Fractals
Forecasting	What is likely to happen in the future?	BPM - Data Analysis - What if Scenario Planning

Table 1. Integrated IT GRCM Tools and Processes

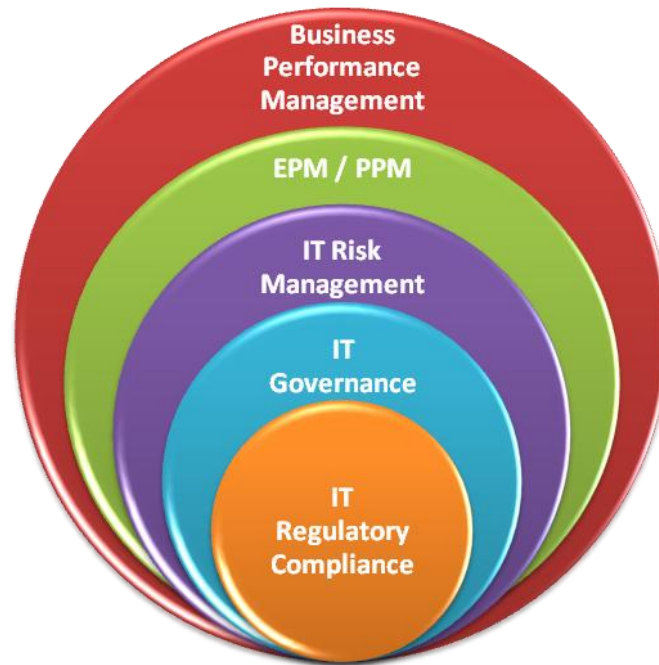


Figure 3. IT GRCM – Optimal Business Performance Model

About CMLgroup

CMLgroup's mission is to assist executives to Define, Measure and Manage customized Business Performance Management solutions that align strategy to execution with sustainable performance improvement over time.

CMLgroup solutions help maximize potential within organizations by providing decision-makers with critical visibility into the factors that affect their business, including knowledge that may not have been uncovered before. This access to more tailored information enables the appropriate individuals to make better-informed business decisions at all levels leading to actions that improve customer interactions, lower costs, and ultimately increase revenues.

Utilizing a proprietary flexible Business Performance Management framework, CMLgroup achieves performance improvement by designing relevant solutions and implementing proven industry best practices with the latest technologies. CMLgroup also helps you leverage your unique competitive advantage consisting of essential resources, the combination of your people and the business data collected in your systems necessary to understand, manage, and excel in your business.