**White Paper**

**IT GRC – The iGATE Way**

**Thursday, April 28, 2016**

**February 2014**

Table of Contents

[Abstract 1](#_Toc381017264)

[1. Key components of IT GRC 1](#_Toc381017265)

[1.1 IT Governance 1](#_Toc381017266)

[1.2 IT Risk Management 2](#_Toc381017267)

[1.3 IT Governance Frameworks 3](#_Toc381017268)

[1.4 Compliance & Assessments 4](#_Toc381017269)

[2. Integrated approach to achieving GRC 5](#_Toc381017270)

[3. iGATE IT GRC Services 6](#_Toc381017271)

[4. Conclusion 7](#_Toc381017272)

[5. References 8](#_Toc381017273)

[6. About the Authors 8](#_Toc381017274)

# Abstract

GRC stands for “Governance, Risk and Compliance”. GRC is an approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically and in accordance with its risk tolerance, policies and regulations through the alignment of people, processes and technology.

Organizations leveraging GRC processes desire to establish a regulatory or internal framework for satisfying governance requirements, evaluate risk across their enterprise and track how the organization complies with the established governance requirements. GRC processes typically fall within one of four key domains: **IT**, **Operations**, **Finance** and **Legal**.

Over the course of the last decade, the role of the IT department has evolved from a simple service provider, usually considered just a “cost center,” to a strategic partner (“profit center”), which generates economic growth for an organization. As a result, IT GRC has gained great importance as IT processes become ever more crucial for executing the core business processes of companies. Unobstructed operations and continuous improvements are an essential success factor for organizations. An effective IT GRC implementation provides significant advantages for an organization:

* Proactive budgeting of IT investments
* Better evaluation of IT process performance
* Secure handling of risks
* Responsible use of IT resources
* Measurable and achievable goals
* Proper handling of company values
* Proper use of information technology
* Compliance

IT GRCincludes the management of IT-related controls. These may include security controls such as firewalls and or security information management system, system controls automation and vulnerability monitoring tools, identity and access management system or disaster planning and recovery systems.

IT GRC is becoming increasingly important as IT organizations drive to ensure the compliance of their businesses and provide a comprehensive view of the IT environment. This discipline has become more prevalent in the last few years due to the US Sarbanes-Oxley Act and increased regulation across financial and medical organizations, but quality standards (like the BS5750 in the UK) and operational frameworks (like COSO, ITIL and COBIT) have also driven this growth.

# 1. Key components of IT GRC

## 1.1 IT Governance

IT governance integrates and institutionalizes good practices to ensure that the enterprise's IT supports the business objectives. IT governance enables the enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities and gaining competitive advantage. IT governance is a structure of relationships and processes used to direct and control the enterprise toward achievement of its goals by adding value while balancing risk vs. return over IT and its processes.

The primary objectives of an IT Governance program are to ensure:

* IT delivers value to business through strategic alignment of IT with business
* IT risks are managed



Source: ISACA

**STRATEGIC ALIGNMENT** focuses on ensuring the linkage of business and IT plans, on defining, maintaining and validating the IT value proposition, and on aligning IT operations with enterprise operations.

**VALUE DELIVERY** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

**RESOURCE MANAGEMENT** is about the optimal investment in, and the proper management of, critical IT resources: processes, people, applications, infrastructure and information. Key issues relate to the optimization of knowledge and infrastructure.

**RISK MANAGEMENT** requires risk awareness by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.

**PERFORMANCE MEASUREMENT** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

## 1.2 IT Risk Management

Risk is defined as the product of the likelihood of occurrence and the impact an event could have. In IT, however, risk is defined as the product of the asset value, the system's vulnerability to that risk and the threat it poses for the organization.

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures (safeguards or controls), if any, to take in reducing risk to an acceptable level (i.e., residual risk), based on the value of the information resource to the organization.

The objective of performing risk management is to enable the organization to accomplish its mission(s) by:

1. Better securing the IT systems that store, process, or transmit organizational information;
2. Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and
3. Assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization’s risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. Risk assessment process includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Risk mitigation refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Evaluation and assessment is the continual evaluation process and a best practice through which an organization keeps a check on its IT risks.

A successful risk management program will rely on:

1. Senior management’s commitment
2. Full support and participation of the IT team
3. Competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization
4. Awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization
5. An ongoing evaluation and assessment of the IT-related mission risks.

**50%** of companies are using outdated risk management solutions

Source: SAP insider Research

Risk management is and will continue to be the biggest focus for organizations. Risk management is top of mind for GRC professionals. Organizations are finding that the cost of complying with a myriad of regulations is very expensive. Taking a risk-based approach toward compliance requirements enables them to focus resources on the most significant regulatory or legal issues facing their organizations.

Too often, risk management is handled by separate teams in multiple departments, resulting in disjointed processes, duplication of effort and conflicting analyses that cannot easily be reconciled due to inconsistencies in data, metadata, sampling, definitions, methods, etc. The answer lies in establishing automated, well-defined, controlled and documented risk management procedures that let you assess the adequacy of internal controls, quickly detect and report all violations and ensure that business units take timely and appropriate corrective actions.

## 1.3 IT Governance Frameworks

An IT Governance Framework is a system by which the current and future use of IT is directed and controlled. At the centre of an IT Governance Framework is the assignment of decision-making authority and accountability of individuals for the decisions they make, particularly when these decisions impact on the organizations strategic goals.

An IT governance framework comprises 3 tiers:

* **At the Board level:** directors Evaluate, Direct and Monitor the performance of IT against plans, internal policies, external obligations and strategic objectives.
* **At the Management Level:** management Plan, Supervise, Check and Act to effectively and efficiently leverage IT resources and to drive continuous improvement. (A management system that includes policies, plans, organizational structures, processes and governance mechanisms is used to enable the effective management of IT resources and ensure continuous improvement.)
* **At the Process Level:** activities are performed, controlled and checked in alignment with business objectives.

The ever increasing risks and regulations have resulted in the development of many frameworks. A few important are mentioned below:



**Control Objectives for Information and Related Technology (COBIT)** is a framework created by ISACA for information technology (IT) management and IT governance.

**ISO/IEC 17799:2005** establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management.

****

****

**Information Technology Infrastructure Library (ITIL)** is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

**Committee of Sponsoring Organizations of the Treadway Commission (COSO)** is a joint initiative of five private sector organizations, established in the United States, dedicated to providing thought leadership to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting.

****

## 1.4 Compliance & Assessments

An initiative to comply with a regulation typically begins as a project as companies race to meet deadlines to comply with that regulation. These projects consume significant resources as meeting the deadline becomes the most important objective. However, compliance is not a one-time event – organizations realize that they need to make it into a repeatable process, so that they can continue to sustain compliance with that regulation at a lower cost than for the first deadline. When an organization is dealing with multiple regulations at the same time, a streamlined process of managing compliance with each of these initiatives is critical, or else, costs can spiral out of control and the risk of non-compliance increases. The compliance process enables organizations to make compliance repeatable and hence enables them to sustain it on an ongoing basis at a lower cost.

Performing regular assessments is an important aspect of GRC programs. Assessments should generally include these steps:

63% organizations fail audits due to problems found with user and application access controls. Other common technical control failures include IT policies and standards (63%), IT configurations and change management (63%), and controls for application development and maintenance (50%)

Source: IT Policy Compliance Group

* Compile a resource inventory – key players
* Prepare an inventory of, systems, applications and processes (both automated and manual)
* Prioritize based on Criticality
* Develop a set of Key Performance Indicators
* Periodically Measure and Report
* Monitor and Respond

# 2. Integrated approach to achieving GRC

The ever-increasing number and sophistication of threats has placed unprecedented pressure on organizations, forcing them to meet external regulatory compliance requirements or internal security mandates in order to protect their businesses. Unfortunately, many organizations achieve compliance through last-minute heroics to generate proof of controls for auditors. This moment-in-time approach to compliance increases the workload and costs, yet provides little protection from IT security threats.

**90%** of companies that have integrated governance, risk, and compliance have had results that met or exceeded their expectations

Source: OCEG 2012 Maturity Survey

As they identify new requirements and risks, most organizations develop new and unique sets of responses and controls across organizational units. They do this instead of building on existing compliance and risk programs and processes. This leads to duplication of effort and an inability to establish a holistic view of risk exposure. As a result, many organizations have a poor understanding of their true compliance status. Furthermore, managing these responses and control efforts through disparate tools does not enable synergies, automation, or the leveraging of existing frameworks.

Although governance, risk and compliance are separate factors, they each have significance, relevance and influence on each other. The integration of Governance, Risk and Compliance Management initiatives into one converged approach is not easy. There are huge benefits to organizations that perform the duties involved in true GRC convergence. A successful, embedded and integrated GRC approach will result in a transparent organization, with streamlined processes, significant cost and time savings, reductions in key controls and risks, and numerous options for business performance improvements.

To gain those benefits an organization needs to develop a GRC strategy. Internal audit, risk management and compliance departments need to work closely and agree on the framework to be used. Consensus must also be made on the language and definition of terms, as well as the GRC platform to be used to embed the GRC strategy into the entire organization. Many questions will need to be answered: How can various risk management and compliance initiatives be integrated into one overall corporate framework? For compliance, how can the enterprise ensure a control is tested once, but used many times for different regulatory reports? Regarding risk management, how do risks roll-up and relate? These are important and difficult questions to resolve.

The purpose of integration is to combine processes and information while preserving variations in how principles are applied when it makes sense to do so. Integration should occur at sensible points designed to move the organization towards an integrated GRC framework that allows for a balance between growth, risk and return.

**60%** of companies indicated that integrating processes reduced gaps in risk and compliance procedures

Source: OCEG Maturity Survey, 2012

Subsequent phases are determined by the level of existing integration, but need to revolve around a principles-based GRC framework that clearly defines responsibility, authority and accountability across the organization.

Integrating GRC practices is an ongoing process, not an end in itself. But significant value can be achieved from the start by getting all stakeholders to work together to take practical, measured steps toward integration. In deciding to the take the first step, an organizations should not only consider the value of reducing risk while driving improved performance but also the value of demonstrating to the market place that it is run based on principled business decisions.

# 3. iGATE IT GRC Services

iGATE is an industry leader and possesses over a decade of rich experience in the IT GRC space. iGATE deploys multi disciplinary teams of professionals that include IT consultants, industry practitioners, business domain experts and thought leaders.

iGATE’s unique approach and framework helps in evaluating and integrating the various risk management, compliance, internal audit and assessment programs thereby providing a holistic view and eliminating the redundancy involved in managing them in silos. Many of the leading organizations’ (including the Fortune 500) trust in iGATE to help manage their IT GRC programs is a manifestation of iGATE’s strong capability and market presence in the IT GRC space. iGATE has established a dedicated Center of Excellence (COE) to manage, improve and improvise its offerings in the IT GRC space.

iGATE has built a comprehensive platform that can support the compliance and regulatory reporting requirements of financial institutions across the globe. The compliance application is an enterprise wide Security Aggregation System to meet the regulation and reporting requirements set by various National/Trans-national Securities Market Regulators worldwide. Some of the highlights are:

* A Rules & Parameters based system that allows the business to change triggers in accordance to specific legal requirements for regulatory reporting.
* Aggregates the proprietary and discretionary positions in order to report breach of threshold values set for each regulation
* Customizable rules engine, with built-in standard rules set, to include/exclude positions data per specific regulation
* Intuitive User Interface with a comprehensive notification engine
* The automated services replace high-maintenance manual processes that are prevalent in the industry.

iGATE’s IT GRC services include:

**IT Risk Management:** Simplified IT Risk management processes, therefore accurately assessing the risks, their mitigation, evaluation and re-assessment.

**Application Security:** Application design and review, vulnerability scan and testing, and security assessments.

**IT Controls Self Assessment & Measurement:** Conducting internal assessments to ensure audit readiness and compliance to regulatory requirements (SOX, HIPAA, FISMA, etc.) as well as internal/non-regulatory requirements.

**Business Continuity Planning & Disaster Recovery:** Conducting Business Impact Analysis (BIA), business continuity planning and testing, disaster recovery planning and testing, documentation review and DR drills.

**Security Operation Center (SOC):** Monitoring security events, log aggregation & analysis, remote management of firewall & security devices, logs consolidation & centralize management of security devices.

**Identity & Access Management:** Design, support & manage the Identity and Access Management processes across the organization.

**GRC Platforms Support:** Implement, manage and support the GRC platform.

**Software Governance:** End to end management of software governance audits, including planning, study, evaluation, testing, reporting and follow-up.

**PMO & QA**: Setting up “Project Management Office” and run the IT Governance program as one unified program and deploying a team of qualified professionals for performing quality assurance reviews and offer consultations for process improvements, remediation and exception management, etc.

**IT GRC Advisory & Consulting**: Advisory and consulting services for efficiently and effectively managing the IT GRC program.

# 4. Conclusion

Driven by a fear of failure or scandal, companies are blindly pouring money into governance, risk and compliance activities and seeing no real return on investment.

Governance, risk and compliance (GRC) spending for Year 2009 stood at $28.7 billion

Source: AMR Research Inc. in Boston.

Companies have invested heavily in governance, risk management and compliance (GRC), increasing the size, magnitude and reach of their GRC functions. Some believe that their reputations, customer loyalty and even credit rating and access to capital depend on it.

As the trend towards massive expenditure in GRC continues, many companies fail to grasp, that their GRC investment, unless properly focused, is potentially being poured into a black hole and will not deliver value. An effective IT GRC program isn’t about spending more but rather about deriving greater value from what is spent. It not only helps the organization in staying compliant to the regulatory and internal requirements, but also safely managing the risks and converting them into potential opportunities for growth.

* Effective governance, risk, and compliance management, like good brakes, allows an organization to speed ahead with the confidence that it will safely negotiate each turn on its chosen course.

**5. How will your use case bring value to iGATE business/vertical**

Firstly, this white paper sets a stage to collectively demonstrate iGATE capabilities in the IT GRC space. It identifies what services iGATE can provide for their clients in this area. IT GRC is a growing field and has been acknowledged as one of the most important areas by IT Organizations as the stakes are huge for falling short of the regulatory and internal audit requirements. Most of the organizations still run their IT Governance programs in silos and there is a lot of potential to streamline, improve and improvise this area. This white paper captures the essence of this prevalent problem and details out steps that could be taken to prevent it.

# 5. References

1. Forrester Research.

<http://www.forrester.com/home/>

1. Information Systems Audit and Control Association.

<https://www.isaca.org/Pages/default.aspx>

1. Ponemon Institute© Research Report.

<http://www.emc.com/collateral/about/news/ponemon-report-egrc.pdf>

# 6. About the Authors

**Mohammed Musthafa Sheriff, Manager - Projects, iGATE**

**Musthafa has 12 years of experience in IT projects management and delivery. He has been working on different projects managing the IT GRC programs for the fortune 10 companies for the last 8 years and possesses very strong experience in IT Governance, Risk Management, IT Auditing & Compliance, SOX & IT Frameworks.**