White Paper

The Governor's Choice: Why Choose IT GRC?

WP0189 | May 2015

Michael Lane

Mike is a respected technology professional with nearly 20 years experience, having held senior manager positions in Information Technology, Communications and Consulting.

Over his career he has managed a vast number of Telecoms, IT, Business and Consulting projects and programmes, and the associated global cross functional teams, with a strong track record of results. Mike is a specialist in many aspects of information technology, including infrastructure, architecture, systems development, business processes, service management, policies and standards, leadership, governance and management.

Summary

Governance is not something new. The origination of the word itself can arguably be traced back to ancient Greece, with Governance derived from the Greek verb kubernáo meaning "to steer". But what is relatively new is the emergent omni-presence and entrenchment of Governance in organizations of the 21st Century. The evolution of Governance, from its financially and auditing centered beginnings into something that is woven into the very fabric of the modern organization, continues unabated. In the last two decades in particular we can attest to having seen a rapid increase in organizations' focus on Corporate or Enterprise Governance, driven by global incidents like Enron and Lehman Brothers, the advent of Sarbanes Oxley, publications such as King III and the Cadbury Report, and even university initiatives like the Harvard MBA review.

Governance is no longer a business afterthought or simply viewed as a means for compliance either. Today, Enterprise Governance is at the forefront of an organization's Strategic Direction, and a key element in all phases of Strategic Management – Planning, Implementation and Control. Governance is an essential ingredient in the recipe for creating and sustaining value, and in 2015's enterprise marketplace, it's survival of the fittest – where no value means no future.

Additionally, as Governance has evolved, so too do we find ourselves in the evolutionary age of information and technology. Information and technology has changed the way enterprises think, operate and improve. Information Technology (IT) is more than just an asset, more than just something that needs to be 'aligned to the business', IT is part and

parcel of everything that Enterprises do, helping them to create value day in day out. IT continues to become increasingly pervasive and of necessity in every aspect of Enterprise life, intrinsically and extrinsically valuable to the Enterprise, making it a strategic asset to any organization.

So where do IT and Governance meet? Enter IT Governance, Risk and Compliance, or as it is better known – IT GRC.

IT GRC: The Governor's Choice

When it comes to defining Governance, independent of functional or industry context, there seems to be a global favorite one-liner – "Doing the Right Things". From project management to financial management, from a Coal Mine to a Telecoms powerhouse, from South Africa to the USA – that line has at times become virtually synonymous with Governance. Sounds easy enough, but let's take a look at Governance definitions in a little more detail to help us understand what it's all about.

The Science Daily provides us with a universally applicable interpretation:

> *"Governance refers to all processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language"*

(www.sciencedaily.com/articles/g/governance.htm)

But when it comes to Enterprise Governance, one of the strongest and most informative definitions comes from the Chartered Institute of Management Accountants (CIMA):

> *"The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly."*

(www.cimaglobal.com/Documents/ImportedDocuments/cid_enterprise_governance__feb08.pdf)

Figure 1 (hesreport.sunocoinc.com/_filelib/ImageGallery/2007/Governance/2_corp_governance_0422_web.gif)

And so we can start to build up a picture of Corporate or Enterprise Governance to include facets of:

- Strategic Direction
- Performance
- Risk Management
- Compliance
- Responsibility

Now Enterprise Governance, as the name implies, is Governance which is Enterprise wide. It takes the entirety of the organization into account. IT Governance on the other hand is a subset of Enterprise Governance, focused on the IT function of the organization, and like IT, other functional departments have their own Governance too – for example: Finance Governance, Project Governance, and so on.

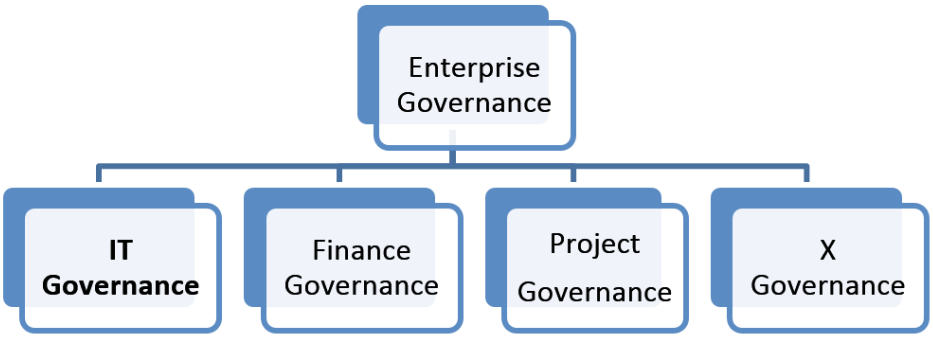

Figure 2

IT Governance specifically, like Governance in general, has many definitions scattered across standards, bodies, and publications. These include Gartner and the International Standards Organization (ISO) -

> *"IT governance (ITG) is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals."*
>
> www.gartner.com/it-glossary/it-governance

> *"System by which the current and future use of IT is directed and controlled"*
>
> [ISO/IEC 38500:2015]

It is worth noting at this juncture that ISO/IEC 38500:2015 is a standard for the Corporate Governance of IT, with a purpose of promoting the effective, efficient and acceptable use of IT. It applies to the governance of the organization's current and future use of IT including management processes and decision making. It defines the governance of IT as a subset or domain of organizational, enterprise or corporate governance.

However, arguably the most relevant and pertinent definition of IT Governance is this one from the IT Governance Institute (ITGI):

> *"The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT* ***sustains and extends the enterprise's strategies and objectives****"*
>
> [IT Governance Institute (ITGI)]

When contrasting the definitions of (Enterprise) Governance and IT Governance, it becomes self- evident that organizations not only need IT Governance for the Governance of IT, but for the achievement of both their Enterprise Governance and strategic goals and objectives. So what then is this IT GRC and where do Risk Management and Compliance fit in? Is there a way or means to manage the interwoven mesh of Governance, Risk and Compliance in the IT domain holistically, without having to bring them together with 'super-glue'? If I was an IT Governor, what choice should I make? All typical questions, and fortuitously, simply answered. When it comes to IT Governance per se, and IT GRC, COBIT 5 from ISACA leads the way.

ISACA defines COBIT 5 as:

> *"A Business Framework for the Governance and Management of Enterprise IT."*
>
> (ISACA 2012)

COBIT 5, with its primary governance objective of value creation, brings together five principles that enable the enterprise to build an effective

governance (and management) framework, based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of all stakeholders.

- COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.
- COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

With the release of COBIT 5 the focus shifted to the holistic and integrated governance and management of information and technology resources, by way of an effective governance and management framework. COBIT 5 brought together Governance, Risk Management and Compliance, or GRC, the preferred 'umbrella term' for these activities of the Enterprise.

COBIT 5 built and expanded on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's **Risk** IT and ISO/IEC 38500 Corporate **Governance** of IT. In moving from COBIT 4.1 to the current COBIT 5, the most significant change was the reorganisation of the framework from being an IT process model into an **IT governance framework** with a set of **governance** practices for IT. Major changes centered on Governance and Risk including:

1. The delivery of a single framework, consolidating COBIT 4.1, Val IT and **Risk IT** and integrating these into one process reference model
2. The introduction of **five new Governance of Enterprise IT (GEIT) principles** to create a principles based framework, bringing it in to line with Val IT, **Risk IT and IOC/IEC 38500** which all use principles in their frameworks and standard respectively.

But it runs much deeper than that. Let's take a look at how Governance, Risk and Compliance are specifically integrated into COBIT 5.

Governance in COBIT 5

Governance forms an integral part of the Enterprise Governance of the business which essentially ensures the business achieves what it set out to do, in the way that it was meant to do it. Sounds like "Doing the Right Things" doesn't it? **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and options; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and progress against agreed direction and objectives.

In COBIT 5, one of the five key principles is separation of Governance from Management. The COBIT 5 process reference model segregates the IT-related practices and activities of the enterprise into these two primary domains—Governance and Management. The Governance domain contains five dedicated and substantial governance processes:

1. Ensure governance framework setting and maintenance.
2. Ensure benefits delivery.
3. Ensure risk optimization.
4. Ensure resource optimization.
5. Ensure stakeholder transparency.

Risk Management in COBIT 5

Risk Management within COBIT 5 is explicit within both the Governance and Management domains.

Within the Governance domain of COBIT 5 is the **Ensure risk optimization** process, which ensures that the enterprise stakeholder's approach to risk is articulated to direct how risks facing the enterprise will be treated.

Process Description

- Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.

Process Purpose Statement

- Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.

Within the Management domain of COBIT 5 is the **Manage risk** process, which provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise.

Process Description

- Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.

Process Purpose Statement

- Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.

All other processes within COBIT 5 include practices and activities that are designed to treat related risk (avoid, reduce/mitigate/control, share/transfer/accept). In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process. These include risk-related roles.

APO12 RACI Chart

Align, Plan and Organise

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Figure 3 (COBIT © 2012 ISACA® All rights reserved)

But when it comes to Risk Management, COBIT 5 didn't stop there. Given the criticality of IT risk management and the stretch target of risk optimization, ISACA took risk management one step further with the COBIT 5 for Risk publication. **COBIT 5 for Risk** defines seven risk principles to provide a systematic, timely and structured approach to risk management, and to contribute to consistent, comparable and reliable results. It also positions Risk Management in context with leading industry risk-related standards including:

- ISO 31000:2009 – Risk Management
- ISO 27005:2011 – Information security risk management
- COSO Enterprise Risk Management

Compliance in COBIT 5

Compliance within COBIT 5 is inherent within the majority of the Governance processes of the Governance domain, and within the Management domain there is a key process specifically focused on compliance.

Within the Governance domain, compliance practices and activities are defined for the following processes:

- o Ensure Governance Framework Setting and Maintenance
- o Ensure Risk optimization
- o Ensure Stakeholder Transparency

Within the Management domain in COBIT 5, is the compliance focused process: **Monitor, evaluate and assess compliance with external requirements (MEA03)**

Process Description

- Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.

Process Purpose Statement

- Ensure that the enterprise is compliant with all applicable external requirements.

- Legal and regulatory compliance is a key part of the effective governance of an enterprise, hence its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03).

In fact all enterprise activities include control activities that are designed to ensure compliance not only with externally imposed legislative or regulatory requirements but also with enterprise governance-determined principles, policies and procedures.

As in the case of Risk, COBIT 5's RACI chart for the MEA03 process includes a specific compliance role:

MEA03 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA03.01 Identify external compliance requirements.					A	R										R	R	R								R
MEA03.02 Optimise response to external requirements.		R	R	R	A	R	I		R							R	R	R	I	R	R	R	R	R	R	R
MEA03.03 Confirm external compliance.	I	R	R	R	R	R	I	I	C							A	I	R	C	C	C	C	C	C	C	R
MEA03.04 Obtain assurance of external compliance.	I	I	I	I	C	C	I		C							C	A	R	C	C	C	C	C	C	C	C

Figure 4 (COBIT © 2012 ISACA® All rights reserved)

Built in to COBIT 5 is everything an organization needs to meet their holistic, enterprise wide IT GRC objectives, with Governance of Enterprise IT processes, governance and management processes for Risk Management, and compliance as a common thread throughout the framework. It's important to note that IT GRC brings together the often many disparate and distinct governance, risk and compliance processes and silos of activity scattered across the organization. In doing so it provides a consolidated view across the Enterprise and directly facilitates the execution and accomplishment of Enterprise Governance. Furthermore, IT GRC commonly delivers the following benefits:

- Contributes to developing a sustainable IT organization aligned to the strategic direction and goals of the Enterprise
- Greater achievement of organizational objectives
- Increased stakeholder confidence
- Improved protection of the organization
- More effective risk responses
- Highly integrated reporting, knowledge sharing capabilities and collaboration
- Economies of scale and cost optimization
- Higher levels of business continuity
- Reduced instances of non-compliance

We all know the impact of the latter two, with business downtime costing in the thousands of dollars a minute and non-compliance per employee weighing in at almost a thousand dollars. Enterprises in the 21st century have many challenges, from ensuring accountability and assurance, to facing significant threats, and satisfying the myriad of regulatory, legislative and conformance demands. Not to mention the need to be continually performing at the top of their game, just to stay alive in a harshly competitive environment.

IT GRC can more effectively and efficiently help organizations to:

- ✓ Create and Sustain Enterprise Value
- ✓ Keep IT risk at acceptable levels, with more Informed risk decisions and risk awareness
- ✓ Support compliance with relevant laws, regulations, contractual agreements and policies
- ✓ Make better and faster Enterprise Decisions with high-quality information
- ✓ Maximize Trust in and Value from Information and Technology systems and investments, for internal and external stakeholders

Conclusions

The pressure on organizations around the globe to practice good governance has never been greater than in the 21st Century. This is not simply because organizations are more attuned to the significant consequences of failing to comply, or because of the lessons of yesteryear reminding them of the risks. Enterprises today realize more than ever before that the sustainability of their businesses depends on it, literally. The clear link between continued organizational success and good governance has been established, and woe any enterprise that believes it to be an unnecessary evil.

In the day to day delivery of products and services, and the operation of the organization, information technology has become paramount, and even the smallest entities have some degree of technology in place to manage people, processes and information. Enterprises have become unequivocally dependent on information technology to not only exist, but to provide competitive advantage in a challenging global market place. And it doesn't stop there. Delivering the required level of governance within the Enterprise undoubtedly also relies on the information technology resources of the modern organization, to provide information on all aspects of conformance and performance. And beyond 2015, the trend is for exponential growth in the demand for real time information and analytics - gone are the static reports of yesteryear saying what went wrong last week, last month and in some cases even last year. Never mind the arrival of Big Data…

The saying goes 'Fail to Plan, and you Plan to Fail'. When it comes to making a plan for managing governance, risk management and compliance with your organization, it doesn't make sense to treat these as mutually exclusive silos, or even interdependent. Smart Enterprises in the second decade of the new millennium are taking an integrated and holistic approach – one of IT Governance, Risk and Compliance or as its become known – IT GRC. And they're reaping the rewards of a happy and synergistic union.

Whatever the industry or organization type, local or global, Enterprises around the world are looking for a comprehensive and coherent approach to create value, manage risk and ensure compliance. Choosing a solution with integrated IT GRC can not only provide just that, but help your organization derive maximum value from its investment in IT, whilst minimizing risk and optimizing costs. If your Enterprise wants to survive and thrive, there's no debate that Governance, Risk Management and Compliance are required… The only question on some Governor's minds is whether to let IT Governance, Risk Management, and Compliance go their separates ways, or bring them all together. The choice should be an easy one. Make the smart choice today Governor – choose IT GRC!

Additional Reading

Orbus Software provide a comprehensive IT Governance, Risk and Compliance Solution, comprising of the COBIT best practice framework, process reference models and assessment templates and reports to support your organizations governance and risk management initiatives

www.orbussoftware.com/it-governance-risk-and-compliance/#

References

Proviti. Growing with Governance, Risk and Compliance (GRC) Solutions [PDF] Available from: www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/Growing-With-GRC-Solutions-Protiviti.pdf

[Accessed April 2015]

CIMA. Enterprise Governance [PDF] Available from: www.cimaglobal.com/Documents/ImportedDocuments/cid_enterprise_governance__feb08.pdf.pdf

[Accessed April 2015]

ISACA. Developing a Successful Governance Strategy [PDF] Available from: www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf

[Accessed April 2015]

www.itgovernance.in/t-itgovernanceandisoiec38500.aspx

www.sciencedaily.com/articles/g/governance.htm

www.gartner.com/it-glossary/it-governance

www.oceg.org/resources/grc-capability-model-red-book/

COBIT5–and–GRC [PPT] Available from: www.isaca.org/COBIT/Documents/COBIT5-and-GRC.ppt

[Accessed April 2015]

ISACA (2012). A Business Framework for the Governance and Management of Enterprise IT [PDF] Available from: www.isaca.org/COBIT/Documents/COBIT5-Ver2-FrameWork.pdf

[Accessed April 2015]

ISACA (2012) COBIT 5 for Information Security [PPT] Available from: www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx

[Accessed April 2015]

Orbus Software UK
London

Orbus Software US
New York

Orbus Software AUS
Sydney

Orbus Software RSA
Johannesburg

enquiries@orbussoftware.com | **www.orbussoftware.com**

Seattle Software Ltd. Victoria House, 50-58 Victoria Road, Farnborough, Hampshire, GU14 7PG. T/A Orbus Software. Registered in England and Wales 5196435