

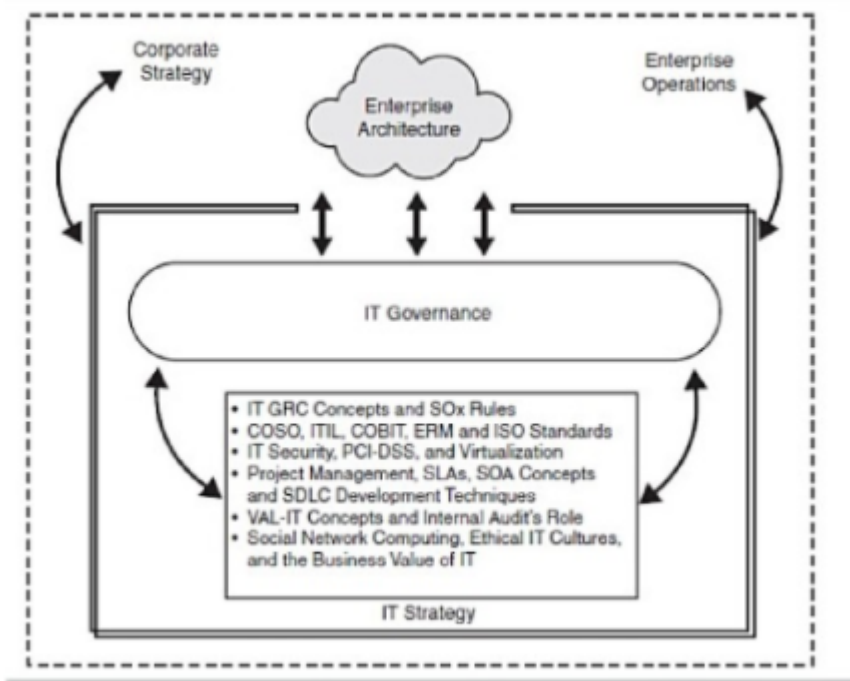
IT GOVERNANCE: AN INTRODUCTION



The defining evolution of IT governance

IT governance serves as a strategic enabling force for the monitoring and improvement of enterprise operations. IT governance helps measure business's growth and success, including financial health. IT governance involves the optimal orchestration of aligning information technologies with corporate strategy, enterprise architecture and operations along with the tools and strategies of IT methodologies, controls, and its own network disruptors.

See the following illustration of a traditional IT Governance model from [An executive's guide to IT governance: Improving systems processes with Service Management, COBIT, and ITIL](#):



Such critical method of governance not only includes the best practices and management methodologies which provide the guidelines (e.g., GRC concepts and SOx rules) but also the aligned best practices and processes (e.g., ITIL, [COBIT](#), RM, and ISO standards) that ensure these same guidelines are instituted and remain strategically aligned with the business strategy they exist to support. This however was not always the case or the role for IT controls. A lot changed over the course of a decade.

In 2001 the world discovered how vulnerabilities left unchecked could become monumental actualized risks that had aligned with criminal intention or even worse. Enron's unraveling and meltdown of many related businesses is one prime example of what had happened by simply taking corporate reporting and their balance sheet at face value. Soon after the criminal trials involving Enron and the executive leadership that became accountable, Federal regulations were instituted and have since spread worldwide. IT governance is challenged as businesses come to exploit the new and powerful information technologies which are themselves becoming powerful disruptors of historical industries and the infrastructures they once supported as well as restricted.

Technology has continued to evolve at a rapid and industry transformative pace in which corporate slogans account for the power to be at home anywhere or determine to designing our futures (Airbnb, Autodesk). Today the use of ever-changing and increasingly competitive Information Technologies (e.g., SaaS, Social, Mobile, Analytics and Cloud computing) challenge the very definition and application of IT governing controls. How to maintain compliance and what must co-evolve is the very foundation of what is the customer and what is the new responsive business model in the transformative "just in time" sharing economy of today.

Meanwhile clear controls and secure parameters in which to ensure compliance and minimize new risks that can be and are exploited daily by those with criminal intent or simple curiosity of what one can do in this new frontier. It is understandable from a meta-level of Management that Information management systems and the business's processes, requirements and resources are closely monitored using internal IT governance controls aligned with the strategic objectives of the business.

For IT governance to identify it's maturity within the organization and allowing IT to align to business

strategy both business along with the business of IT infrastructure must follow the alignment of three pillars:

- 1. Leadership
- 2. Organization and decision rights
- 3. Scalable processes and enabling technologies

IT governance at its highest level of efficiency has both focus and its own visibility into the overall (end-to end) business process in which the business and the business customers interact. IT governance represents a journey towards continuous improvement and optimal effectiveness where best practices, industry standards and value methodology such as COBIT provide a set of tools and methodologies to institute good governance within an organization at any level of immaturity to maturity.

In particular, there needs to be an intentional co-evolution of a common language and shared values that ensure the proficient and transparent accounting of optimal performance management. Critical to the success of any IT Governance initiative is an effective communications plan. The communications plan should be based on a well-defined influencing strategy. The strategy should identify opportunities for the active involvement of stakeholders in developing the evolving governance approach, planning and implementing IT management changes, and ideally building specific change objectives/targets into personal performance plans. The stakeholders are likely themselves to be the targets of change and should be involved in discussing/evolving responses to known and imaginable changes via collaborative workshops, focus groups etc. It is in these diverse yet collaborative communication workshops that the stakeholders of change witness together from where they have come, where they are in present time, and where together they desire to go.

Communication Workshop Worksheet

Characteristics	Past (behaviors that reinforce self-other destructive habits)	Present (behaviors that are self/other creative growth enhancing behaviors)	Desired Future
Myths and Stories (informal or formalized)			
Symbols			
Power Structure			
Organizational Structures			
Control System			
Routines and Rituals			

Managing the choreography and performance of joint alignment

Performance management lifeline is dependent on a feedback feedforward information system capable of tweaking and redirecting the whip and tail thrust of supply chain operations to minimize any negative impact to valued business processes that the IT governance aligns with and acts to

modulate as a governing control. All of the challenges of today's performance management requires knowing what and where the risk may be and how risk adverse is each component of the business's overall operations:

- Risk management starting at the C level of the corporation and/or business (small or large)
- An emerging organic practice of ensuring business and customer confidentiality remain intact while maintaining optimal day to day business operations
- The on-going ubiquitous valuation and accounting of optimal performance management
- The strategic value and use of information technology in the development, sustainability and direction of growth for future business

Once a successful risk management implementation has been achieved, CIOs and their teams can focus on higher value activities. Examples include:

- Leveraging automation to increase the level of integration across major business processes, e.g. straight through or cash-to-ledger processing
- Leveraging additional forms of unstructured and structured data to enrich reporting and decision making, e.g. social media, sensor-based, Internet of Things, etc.
- Leveraging enhanced analytics driven by higher quality and higher volume of data being captured and processed to support the end-to-end needs of practically every business function

It is easy to see, in principle, how moving away from a model based on traditional application development, maintenance and IT operations to a model that provides more business process support can benefit the entire enterprise in ways that go well beyond reducing the cost of running an application. What now becomes the results of IT governance? As defined IT governance affects business performance, and ideally helps the business outperform their competition. Good IT governance leads directly to increased productivity, higher quality, and improved financial results. Poor IT governance, on the other hand, leads to programmatic waste, bureaucracy, lower morale, and diminished overall financial performance.

In order to positively impact business performance, IT governance processes must have focus and visibility on the overall (end-to-end) business process with which business and consumers engage. Each point of engagement must be identified and monitored to ensure the interaction of following four:

1. Strategic Alignment
2. Risk Management
3. Performance Management
4. Value Delivery

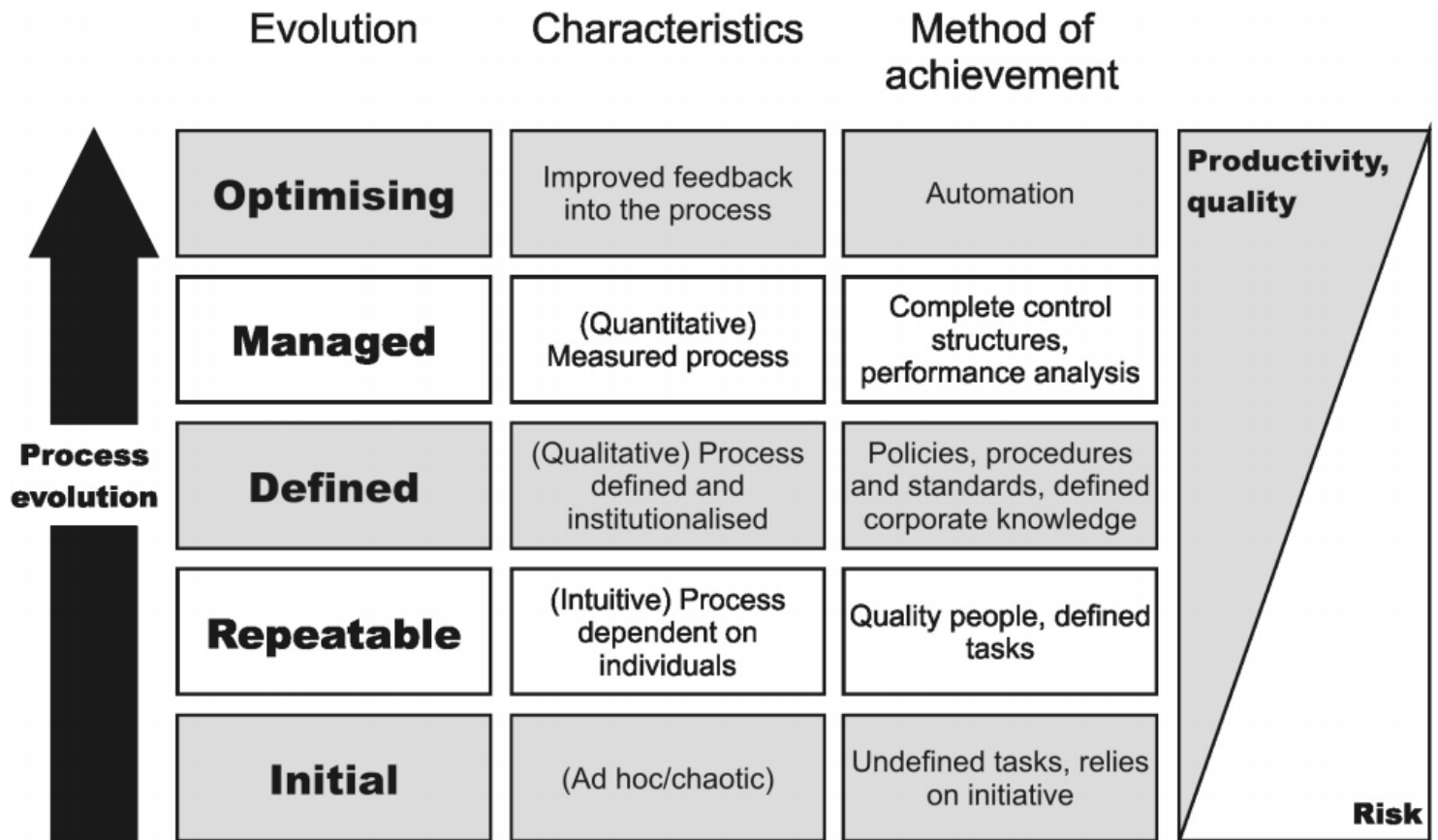
See the illustration below, again from [An executive's guide to IT governance: Improving systems processes with Service Management, COBIT, and ITIL](#):



In order to support the governance and maturation of the above four, IT governance is charged to ensure compliance and the management of any risks identified concerning Federal regulations (e.g., Sarbanes Oxley) and how it helps the business manage the quadrants illustrated above. Much like the governor in the engine of an automobile IT governance has come to serve as the cruise control for both business operations and its strategic growth. In the management of the business performance, information technologies and their alignment to the business strategy, the overall encompassing strategy must be broken down. As such, the strategy becomes a multiple diverse maturing co-evolving feedforward feedback system in which the internal and external aspects of the business co-evolve and are therefore governed in changing ways to accommodate for each variation of business/organizational maturity.

Assessing and responding to desired capabilities

COBIT as a platform establishes the means for IT Governance to be part of the ground floor as it incorporates the initial business strategy and accountability within its framework. COBIT is itself a means to govern communications, systems development and data storage, as well as performance management. The one difference with COBIT is that it not only defines what should be managed but provides a process by which the defined can be managed and governed at each stage of the business/system maturation. A first step in this process of maturation is for the initial stakeholders and multi-disciplinary team of business and IT subject matter experts to assess current maturity level of key business processes/ IT governance components and targeted future state maturity levels for each major business process group and IT governance component. Each must be assigned a current state and be provided a desired future state with desired characteristics and methods for achievement.



The real value of capability assessment comes through the identification and implementation of cost effective improvements, strategic maintenance of inventories and the competitive means to effectively respond to a yet to be defined emerging and/or disruptive environment. A realistic and practical approach is required to ensure that the proposed improvements are based on business priorities, will be supported and funded by management, and will be successfully implemented. As IT governance and the information technologies have become aligned with business strategy, business strategy is itself transformed.

What becomes the highest value takes a second or even third or fourth position of other newly define business capital and capacity optimization. The recommended approach to determine how business and therefore information technologies are to be exploited as IT governance aligns with the business strategy is as follows:

1. Understand the environment
2. Establish capability improvement framework
3. Set realistic targets and respond to environment changes
4. Identify gaps - prioritise improvements
5. Propose achievable solutions

In meeting this recommended approach, there is an ever present importance of communicating via a diverse dialog in contrast to a one-way monologue for the purpose of continuously defining and redefining modes of understanding what were, are, or may becoming strengths, weaknesses, opportunities and threats.

IT governance charged with aligning and moderating business strategy is continuously challenged to address various levels of maturation and further becoming of a business practice, operation or strategy. A simple self-assessment diagnostic can be used to help show overall capability at a high

level, based on the four domains of COBIT, broken down into the 234 COBIT sub-processes.

The extent of the analysis depends on how precise the governing leadership wish to be. A management workshop can be used to arrive at an approximate initial assessment without extensive analysis using the following chart:

Generic Maturity Model for Governance	Understanding & Awareness	Training & Communication	Expertise
Competence (COBIT)			
1 Initial/AD Hoc	Recognition	Sporadic	
2 Repeatable but Intuitive	Awareness	Communication on the overall issues and needs	
3 Defined Process	Understanding of need to act	Informal training supports individual initiatives	IT Governance expertise exists within the Process owner and team
4 Managed and Measurable	Understand full requirements	Formal training supports a managed program	IT Governance expertise is monitored and measured outside the Process
5 Optimized	Advanced, forward-looking, understanding	Training and communications support extend best practices and use leading edge concepts	Use of external experts and industry leaders for guidance, comparison to best practices.

COBIT's management guidelines are generic and action oriented for the purpose of presenting a means to assign and measure optimal governing components at their current maturation level. Despite the fact that corporations are beginning to experience success with implementing IT governance mechanisms to better manage their IT resources, individual governance mechanisms cannot alone promise the successful implementation and execution of IT governance policies and procedures.

Companies must be able to better understand the complex playing field of their competitive environment and be able to put together a reliable set of governance techniques that are simple, are easily shared and implemented, and that engage managers who make key decisions for the company. These mechanisms provide firms, at a minimum cost, with the coordination, control, and trust that is needed to manage and utilize their IT related resources. Hence, well-developed and implemented IT governance mechanisms help firms to establish coordinated mechanisms that link IT- related objectives aligned with the four quadrants of business strategy to measurable goals.

IT governance also helps to provide the necessary checks and balances to better manage and mitigate risk, standardize practices, streamline procedures, and improve returns on technology resources and assets. IT Governance is a continuous process. IT governance can be seen as the continuous process of aligning corporate and IT strategy. IT governance helps to shape organizational changes over time and should be tightly tied to corporate governance procedures and regulations. IT governance is intended to safeguard the organization against criminal activity inside and outside the organization and to develop and implement strategies and processes to

manage the inevitable confrontation of a previously only defined weakness or threat as equally well to a new and previously undefined strength or opportunity.

IT governance and the multiverse of commerce

IT governance currently, through the use of maturation models, the stories and artifacts of business past, current and future, begins to sound like a Grimm's Fairy Tale. IT governance itself, if not carefully moderated and contiguously monitored for new strengths, weaknesses, opportunities and threats at different levels and layers of the organization becomes easily unaligned with the business strategy which it is meant to support. See the world and its global diversity as one example. Where IT governance is still typically the primary responsibility of the board of directors and executive management (including the Chief Information Officer) it is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives in an ever changing consumer time and space. IT governance should typically address IT-related risks and opportunities at different layers of the organization. IT managers should solicit input for the development of IT governance policies and procedures, since such governance affects employees within different levels of the organization and across different business functions. All employees, from front-line employees and their managers to the executives of the board of directors, should contribute to the enforcement of IT governance policies and procedures.

Action items to consider when establishing IT governance include the following:

1. Identify and define the strategic and tactical IT governance roles and responsibilities throughout the organization. In addition, include senior managers from both the IT and business divisions to serve as the key champions to disseminate and encourage the adoption of IT governance procedures and policies within their divisions.
2. Determine an IT governance implementation plan. It is of foremost importance for the board to take ownership of IT governance and determine the direction that managers should follow.
3. Identify champions who have a vested interest. Constrain the number of decision-making structures when determining how IT resources are acquired, utilized, and discarded.
4. Ensure cross-coordination and responsibilities for IT decisions. Overlapping memberships coordinate decisions throughout the enterprise and often ensure that the strategic objectives of managers filter down to decisions made at the individual project level.
5. Create an IT governance road map and plan for long-term strategies. IT governance should be integrated with the broader and strategic Enterprise Governance goals.
6. Walk before trying to run: Identify short-term IT governance issues that can serve as quick wins to get the organization jump-started on its IT governance policy and regulation enforcement. Such wins will also help to provide evidence that IT governance procedures and policies can aid and protect the organization, as well as further establish the credibility for implementing IT governance policies.
7. Go to the place: Identify and manage IT-related risks and opportunities. Survey your users. They can be one of the best sources of input for identifying security gaps or inappropriate use of IT.
8. Revisit IT governance policies on a regular basis. The value of maintaining certain resources and or risk xcac change. When this situation occurs, the IT governance policies must be revisited to address these situations.
9. Increase the transparency of your IT governance. One of the most significant factors that can

influence the success of IT governance policy and procedures is the number of employees who can accurately describe the company's IT governance policies and share the firm's IT governance and future strategic goals and plans.

10. Establish exceptions to governance processes. Establish a process for the firm to follow if the need arises to update or to provide an exception to the IT governance policies that are in place.

Over the next 40 years, the huge burden of the CIO ensuring that IT is effectively managed will become a company and board-level responsibility. However, this change will be more easily accomplished if IT governance is fully incorporated and is properly enforced within companies. It is important to recognize the value of COBIT in the successful implementation of robust, effective and purposeful IT governance that is capable of becoming an organic fabric of the organization at many levels and various layers of one body. In this way there remains at all times management and transparency of what was transmitted and received communication, information, operation and financial management.

IT governing controls aligned with long term business goals and objectives become an ongoing self-defining act. COBIT is not a standard but a best practice and a set of guidance materials to be tailored for each specific situation. And as it has been adopted it has helped break down communication barriers and improve mutual understanding of IT controls and the business value of the same. IT governance not only is charged to ensure compliance and the management of any risks identified concerning Federal regulations (i.e, Sarbanes Oxley). But rather much like the governor function in the engine of an automobile serves as the optimal self-regulating cruise control or in other terms a prima ballerina capable of responding to the moment and desired expression of value. IT governance, however it evolves and matures within the various levels of an organization must at the same time remain transparent and capable of validating data integrity and maintain the security of personal data. Confidence in the delivery system of desired resources while protecting the confidentiality of the consumer's personal data remain prime values within an organization and the fluid environment of commerce. IT governance will remain an integral part of the efficient operations, development, storage and sharing of competitive Information Technology and the creative ever-changing exploitation of the same while protecting oneself from unregulated environments. The process of defining risks and values must be continuous. See the following figure 5.5 from *Developing A Successful Governance Strategy* (National Computing Centre, 2009) as an example of how one might delve into and maintain such a practice.

IT Process/Maturity	Importance	Ad hoc	Repeatable	Defined	Managed	Optimised
Planning & Organisation						
PO1 Define a Strategic Information Technology Plan	H					
PO2 Define the Information Architecture	M					
PO3 Determine the Technology Direction	M					
PO4 Define the IT Organisation and Relationships	M					
PO5 Manage the Investment in Information Technology	M					
PO6 Communicate Management Aims and Direction	L					
PO7 Manage Human Resources	L					
PO8 Ensure Compliance with External Requirements	M					
PO9 Assess Risks	M					
PO10 Manage Projects	L					
PO11 Manage Quality	L					
Acquisition & Implementation						
AI1 Identify Solutions	L					
AI2 Acquire and Maintain Application Software	M					
AI3 Acquire and Maintain Technology Architecture	M					
AI4 Develop and Maintain Information Technology Procedures	M					
AI5 Install and Accredite Systems	L					
AI6 Manage Changes	M					
Delivery & Support						
DS1 Define Service Levels	M					
DS2 Manage Third-Party Services	H					
DS3 Manage Performance and Capacity	M					
DS4 Ensure Continuous Service	L					
DS5 Ensure Systems Security	M					
DS6 Identify and Allocate Costs	L					
DS7 Educate and Train Users	L					
DS8 Assist and Advise Information Technology Customers	L					
DS9 Manage the Configuration	M					
DS10 Manage Problems and Incidents	H					
DS11 Manage Data	H					
DS12 Manage Facilities	L					
DS13 Manage Operations	M					
Monitoring						
M1 Monitor the Process	M					
M2 Assess Internal Control Adequacy	M					
M3 Obtain Independent Assurance	M					
M4 Provide for Independent Audit	M					

Figure 5.5