COBIT (Control Objectives for Information and Related Technology) Management and Governance System (CMGS): Business-IT Alignment for Boardroom Discussion

Murugan.Kuppuswamy
Master Class Certified, IoD Life Member.
An abstract of IoD Master Class Dissertation

Abstract:

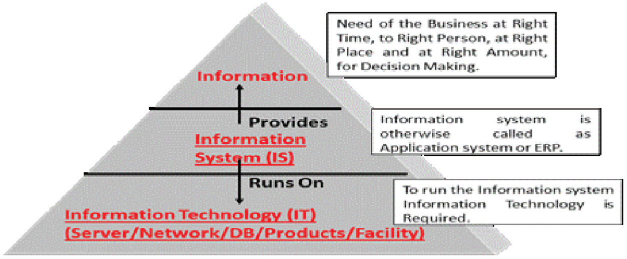
Information Technology (IT) touches every aspect of a business operations; the number of questions boards could pose about IT related decisions is nearly limitless. For any Enterprise, Efficiency and Value creation are two most important factors for sustainable success of a business to increase the Bottom line and Top line.

As a result, today, more than ever, enterprises and their executives strive to:

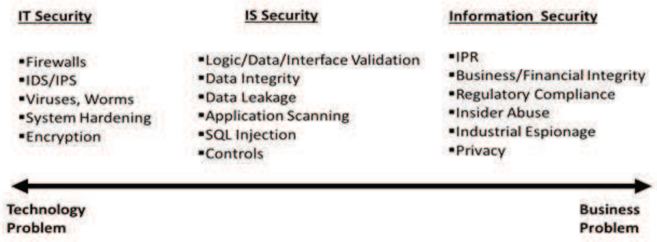
a) Maintain high-quality information to support business decisions.
b) Generate business value from IT-enabled investments, i.e., achieve strategic goals and realize business benefits through effective and innovative use of IT.
c) Achieve operational excellence through the reliable and efficient application of technology.
d) Maintain IT-related risk at an acceptable level.
e) Optimize the cost of IT services and technology.
f) Comply with ever-increasing relevant laws, regulations, contractual agreements and policies.

Information is a key resource for all enterprises, and from the time that information is created to the moment that it is destroyed, Information system (application), Information technology plays a significant role. Below is the relationship of information, Information System and Information Technology.

Information Stack

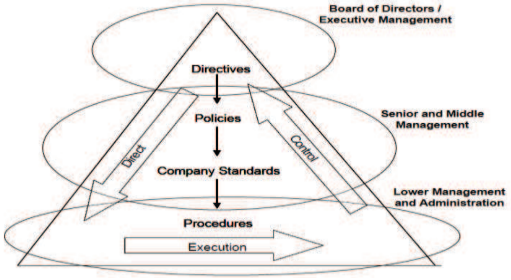

Information
Provides
Information System (IS)
Runs On
Information Technology (IT) (Server/Network/DB/Products/Facility)
Need of the Business at Right Time, to Right Person, at Right Place and at Right Amount, for Decision Making.
Information system is otherwise called as Application system or ERP.
To run the Information system Information Technology is Required.

Security, Governance and Compliance should be addressed across the above stack. Here is an example of Security viewed for the above stack.

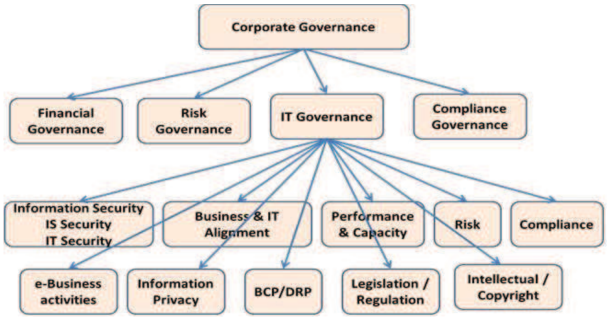


Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Governance Cycle


Board of Directors / Executive Management
Directives
Policies
Senior and Middle Management
Direct
Control
Company Standards
Lower Management and Administration
Procedures
Execution

Corporate Governance and IT governance:



Today without IT investment efficiency and Value creation is not possible. Hence Company invest huge amount of investment in terms of Capital Expenditure and Operational Expenditure for IT. IT is complex but IT Governance need not to be complex.

ISACA (www.isaca.org) , an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the **Information Systems Audit and Control Association**, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves with 95,000 constituents in 160 countries.

Aligning IT governance to COBIT was regarded as a natural extension for the overall organizational governance practices. Implementation of CMGS (COBIT Management & Governance System) using COBIT 5 framework for the Management of IT function and its outcome discussion in the Board room for Governance discussion is proposed as a report in this Dissertation.

An Effective IT Governance model must address three key questions:

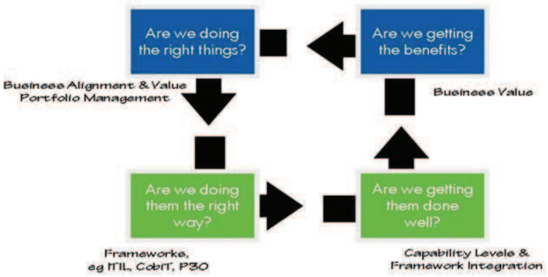
1.What decisions need to be made about IT?

2.Who should contribute and make those decisions?

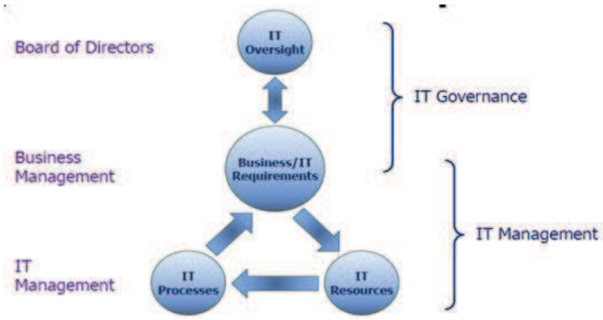
3.How will we monitor and evaluate the results of decisions?

Frameworks are proliferating to help with governance. During the past five years, a number of frameworks, methodologies, and practices have been developed for or adopted by IT to better govern and manage performance. These include control objectives for information and related technologies (COBIT), IT Infrastructure Library (ITIL), International Organization for Standardization (ISO) 17799, CMM, PRINCE, MSP, PMBOK, the Balanced Scorecard, and Six Sigma. It is very easy to get confused by the “alphabet soup” of alternatives, which can lead to paralysis (when CIOs can’t make a decision), or choosing one and then finding out later that it misses the mark.

Key IT Governance Questions


Are we doing the right things?
Are we getting the benefits?
Business Alignment & Value Portfolio Management
Business Value
Are we doing them the right way?
Are we getting them done well?
Frameworks, eg ITIL, CobIT, P30
Capability Levels & Framework Integration

Relationship Between IT Governance & IT Management and Key Stakeholder



ISO/IEC 38500, the international standard for corporate governance of ICT, tends to be more specific. It identifies *‘six principles for good ICT governance’* which are also identically identified in AS8015-2005, the Australian Standard for Corporate Governance of Information and Communication Technology (ICT)

1. ***Responsibility*** – the need to establish clearly understood responsibilities for ICT
2. ***Strategy*** – the need to plan ICT to best support the organization’s business
3. ***Acquisition*** – the need to acquire ICT validly
4. ***Performance*** – the need to ensure that ICT performs well whenever required
5. ***Conformance*** – the need to ensure that ICT conforms with formal rules
6. ***Human Behavior*** – the need to ensure that ICT respects human factors, through ICT policies, practices and decisions.

Management system proposed with sound framework should also four key risk area of the business. Since IT touches most areas of a business, IT risk shouldn't be viewed as a single policy-based issue. Rather, boards should consider IT in the context of a wide range of business concerns. It should also give board members and executives a common language to address IT-related risks.

The four risk areas Business can be exposed to by ineffective management and Governance of IT are

1. *Competitive risk:* The threat of competitors getting to market faster, gaining market share, or achieving an insurmountable first-mover advantage through the use of technology by Value creation.
2. *Portfolio risk:* The danger business is spending too much of its IT budget and resources on basic operational expenses instead of truly transformational investments for value creation.
3. *Execution risk:* The failure to execute IT programs effectively or to deliver critical capabilities to the business on time and on budget.
4. *Service & Security risk: The* risk that systems aren't available to support and/or service employees and customers as needed and that critical data assets of the firm are not properly secured.

The focus of this report is on COBIT 5 framework and how it covers both the governance and management of IT and implements Management system called CMGS, in similar line to QMS (Quality Management System) and ISMS (Information Security Management System) for business.
COBIT5 also integrates various ISACA's frameworks and knowledge resources.

COBIT 5 Principles: COBIT 5 is built on 5 key principles for the Governance and Management of enterprise Information Technology.

1. Meeting Stakeholder Needs. 2. Covering the Enterprise End-to-End. 3. Applying a Single Integrated Framework. 4. Enabling a Holistic approach. 5. Separating Governance from Management.

COBIT 5 defines 7 categories of enablers:

1. Principles, Policies and Frameworks. 2. Processes. 3. Organizational Structures 4. Culture, Ethics and Behavior. 5. Information. 6. Services, Infrastructure and Applications. 7. People, Skills and Competencies

Board room executives need to take three important steps toward building IT Governance:

1. **Get informed.** Take a structured approach to assessing business and IT objectives.
2. **Get aligned.** Implement and enforce internal controls across the extended enterprise.
3. **Get smart.** Use a scorecard methodology to proactively highlight risks and identify, monitor and address.

Following suggestive questions, Independent Directors can place as agenda item about IT investment and Risk before board for discussion.

a) How Strategic Importance of IT to the Business, evaluated, determined and executed?
b) How IT capabilities are evaluated periodically with respect to competition, market structure & Client needs that could threaten business?
c) How funds (Capex & Opex) are allocated across the portfolio of IT investments to ensure an efficient risk return?
d) How IT Portfolio realize efficiency in operation (benchmarked against similar business) in business, in terms of Bottom line?
e) How IT portfolio add Value creation, in terms of Top Line reference to business.
f) What trade-offs are you making in managing the IT portfolio?
g) How effectiveness of major IT programs execution and results are evaluated.
h) How IT staffing expertise, turnover, and talent attracted and retained.
i) How third party service providers and suppliers relationships monitored and controlled.
j) Has board considered for creation of an IT subcommittee?
k) Who on the Management Team has responsibility for IT corporate Governance? Does he/she empower sufficiently?
l) Does management table periodic conduct of Risk assessment report and action items, covering use of IT resources, outsourced services and third party communication based on documented IT Risk Management Methodology policy?
m) Has business identified to comply with privacy regulation? If so does someone from management responsible for privacy policy, privacy legislation and compliance therewith?
n) Has Business identified necessary legislative and regulatory requirements for protecting personal information and developed a policy and procedure for monitoring compliance with them?
o) If the business involved either directly or indirectly in e-business activity. Does business has specific review of Risks and controls over the e-business activities? Does e-business

activities appropriately protected from external and internal threats? Does threat results, lead to loss of customer satisfaction or public embarrassment?

p) Has IT Disaster Recovery Planning and business Continuity policy. Process and procedure in place?

q) Does business have policies covering software licenses, agreements and copyright been formulated and disseminated to relevant stakeholder. Ways to address legal implications.

r) Does Management ensure data integrity, completeness, accuracy and timeliness for key decision making sources like MIS, report & databases?

s) Does Management place before board periodic audit report & action plan of mitigation and remediation controls as per documented Audit policy of the business?

t) How to ensure that a breadth of best practice capabilities and processes are in place to protect the firm from operational, compliance and Information security, Information System Security and information Technology risks—both now and in the future?

Six recommendations are important to achieve and maintain the necessary involvement at the management board level:

1. **Ensuring a transparent assessment framework**—A transparent assessment framework promotes transparent communications and creates clear expectations.
2. **Understanding good points and points for improvement**—Strong points as well as shortcomings must be explained.
3. **Ensuring direct involvement**—Signing off on a completed assessment framework by a board member responsible for IT increases involvement and prevents a lack of engagement.
4. **Benchmarking**—Benchmark information shows the organization's performance relative to its peers.
5. **Translating IT risk factors**—IT risk factors must be linked to the institution's risk appetite or operational strategy.
6. **Monitoring improvement actions**—Active and regular monitoring ensures permanent attention for points for improvement and follow-up thereof.

The results of CMGS implementation provide a determination of process capability and can be used for:

1. Delivering value to the business. This is viewed as an incremental achievement of strategic goals and a clear realization of business benefits through effective and innovative use of IT.
2. Developing IT process improvement. Periodic measurement of IT processes supports the definition of effective governance of enterprise IT (GEIT) road maps to drive continuous improvement.
3. Measuring the achievement of business goals. Each business goal can be evaluated every time the related GEIT processes are evaluated.
4. Generating consistent reports. .
5. Ensuring organizational compliance.
6. Benchmarking. Periodic measurement of GEIT process capabilities allows for constructive and ongoing comparison between businesses employing the same or equivalent industry best practices.