CHAPTER 5

IMPLEMENTING IT GOVERNANCE

This chapter explores the role of IT governance in optimizing information security and proposes an operational model to implement IT governance using COBIT at the strategic level and other standards for devising operational procedures.

5.1. Governance Vs IT-governance

Primarily, governance is not an IT function, and the chief information officer (CIO) does not have primary responsibility for governance. Due to recent developments, IT can automate some governance functions. However, information governance or IT-governance is an IT function and supports organizational governance. Research states that an enterprise needs management level support to achieve effective IT-governance. Research report on CIO, CISO and practitioner guide states that many board of directors have understood that its essential to have a strong and effective IT-governance framework for achieving organizational goals and objectives, fulfilling stakeholder requirements, ensuring compliance with laws and regulations and achieving acceptable levels of risk[107].

5.2. Goals of Governance

Building value and transparency are the goals of corporate executives. Building value creates the pool of wealth which returns a profit to investors and guarantees the ability of the corporation to sustain periodic losses. Creating transparency allows management to understand whether the risks the corporation is taking are prudent and to know how effectively its value-creation and loss-limitation activities are functioning so that these activities can be adjusted if they are not doing the job[108].
It's worth noting that governance and compliance processes are necessary for management's own purposes even in the absence of regulation. Compliance processes are necessary because management needs to guard not just against losses to the public arising from externalities, but also against losses to the corporation arising from risks for whose consequences the corporation is liable.

The following example illustrates the point. Enron's failure to detect a management fraud was a governance failure; Enron’s accounting process failed to create evidence of certain actions, and the lack of that evidence prevented the organizational transparency which could have caused the fraud to become public before the losses reached a critical level. This governance failure devastated Enron itself, but it also created substantial externalities; that is, it created large losses to parties who were not Enron employees or shareholders.

5.3. Need for Organizational Support for IT-Governance

Though governance processes involve management, governance is more than just management. Management is a hierarchical activity performed by designated managers. Governance is a cyclical activity directed by executives and administered by managers, but it places stewardship and reporting obligations on people at all levels of the organization, including line staff. A critical component of a governance process is the system by which people at all organizational levels and in all roles communicates with one another about the status of governance activities.

Governance information must flow in a circle from executive management, through lines of responsibility, to line staff, and then back again to executive management. Without the cyclical flow of information, there can be no organizational transparency. And without organizational transparency, executive management cannot know
whether the processes it has mandated—processes for ensuring that the organization takes risks prudently—are functioning properly.

Governance, therefore, is not “just” management—it is “roundtrip management.” The analogy with roundtrip engineering is deliberate. Recall that in a roundtrip engineering environment, changes to a software system’s specification cause corresponding changes to the system’s code, and changes to the code causes corresponding changes to the specification. Similarly, in a well-governed organization, changes to executive policy cause changes in operational practice, and changes in organizational practice are visible to executive management as changes in policy or status.

Governance in a roundtrip management environment is organized so that policy, responsibility, and resources flow down; and accountability and assessments flow up. This cyclical flow is continuous.

5.4. Data Governance and Information Governance

The use of “GRC” as a marketing term has unfortunately created some confusion about the use of a similar but more specific and useful term: information governance (sometimes called “data governance”). Unlike “GRC” information governance means something specific: the management of information to support governance.

Information governance is largely a chief information officer (CIO) responsibility, whereas governance responsibility originates with senior executive management and devolves upon many different people in the organization. Information governance has two aims as follows:

1. To ensure that sensitive information is treated in accordance with law, regulation, and organizational policy.
2. To ensure that operationally critical information is available, accurate, and up to date area, and problems can linger in this gray area without being recognized as anyone's responsibility.

Here again, the case of Barings Bank provides a good example. Barings' governance processes had established a policy requiring supervision of futures trades. Nicholas Leeson, however, had an unusual reporting structure. He was essentially his own boss and thus responsible for oversight of his own trades. Barings' information governance tools were not sufficiently robust to note this anomaly and report it in a roundtrip fashion to executive management. The oversight deficiency remained unrecognized until after the collapse of the bank[109].

5.5. Information Security Governance using COBIT

An identified enterprise is engaged in the design and development and delivery of content, in addition to providing timely electronic services to citizens of Oman that has grown significantly in the last five years. Assessing and measuring, analyzing and providing corrective strategies to strengthen weak areas of the Identified enterprise’ Information Systems is the purpose of this vulnerability assessment.

In the area of application delivery platforms, the enterprise is the quite vulnerable to security lapses on the one hand and the continual advances in technologies on the other. These two dominant trends in the industry are pulling the company in two directions from an enterprise information security strategy standpoint. Here the concentration is on how to secure the entire platform to ensure a high level of data redundancy and the ability to attain high levels of performance as defined by Service Level Agreements (SLAs)[110]. The security levels for the IT infrastructure are also defined in written contracts to vendors, often specifically defined in clauses within contracts and SLA acceleration clauses that reward the vendors for providing the
necessary services. By actively providing seamless access to get more of their applications and content, the vulnerabilities with regard to their security systems and practices are placed under increasing stress, thus exposed to more threats. This vulnerability assessment explains the most pressing threats and provides insights into how best to alleviate them.

The vulnerability assessment of identified enterprise provided insights into three major security issues the company faces today as it attempts to grow its application hosting service. The first and most significant is protecting the proprietary nature of citizen’s data. During the vulnerability assessment and audit, the ability of technicians to get access to several different private accounts’ data when stored on the same physical server was the most severe. The second-most significant security issue facing the enterprise’ Application Hosting Services Division is the lack of consistency to audit data history and analysis. There are security audits back through 2007, none for 2004 to 2006, and a very preliminary one when the company first launched this aspect of their service. There are literally no records or audit data for 2004. This lack of audit data is very significant and puts it at significant risk in terms of managing its SLAs and with greater accuracy than others. The third most significant finding is how integration between the many legacy and 3rd party systems that it relies on are not functioning with real-time data feeds and a high level of secured communication. These legacy systems lack encryption; support for single sign-on authentication and advanced proxy server support across all on application platforms.

5.6. IT-Governance Framework

The above said problems call for a robust IT-governance framework like COBIT that delivers measurable value to the business while improving the productivity. COBIT 4.1 is identified as a widely adopted framework for IT governance. However, research
articulates that, the breadth and depth of COBIT is exhaustive which makes it almost impossible for medium and large enterprises to implement and reap the benefits. In order to achieve governance through COBIT with limited resources and time, IT Governance Institute recommends using the “COBIT Quick Start” as the baseline which can further be broadened depending on the size and type of the enterprise[111]. So, it becomes evident that focusing on the critical success factors will address the most important processes which directly influence the enterprise’s performance. The critical success factors were identified by exploring the processes and control objectives that are listed in quick start guide. The various dimensions of the enterprise such as Simple Command Structure (SCS), Short Communications Path (SCP), Span of Control (SOC), IT Sophistication (ITS), IT’s Strategic Importance (ITI), IT Expenditure (ITE) and Segregation (SEG) was tested using the suitability assessment tool [112]. The analysis of the results which is shown in figure-6 illustrates that quick start is suitable for the identified enterprise.

![Figure 6 Suitability Assessment](image-url)
After evaluating the 210 control objectives, 24 were carefully selected that are constructively aligned to the enterprise’s goals. Although COBIT provides direction to IT governance, it rarely defines the implementation details.

Analyzing and providing corrective IT governance strategies by mapping the four domains of COBIT with various best practices and to secure the entire infrastructure to ensure a high level of data availability and the ability to attain high levels of performance through accountability is the main purpose of this effort. Literature provides mapping of COBIT with various best practices such as PRINCE2, ISO 27001 and ITIL but the overall mapping of COBIT with any one of the above said best practice is still not suitable from an implementation perspective.

To reap the benefits of best practices based on their proven strength, each domain of COBIT is mapped with a specific best practice which is shown in the figure7. For example Plan and Organize (PO) domain should make use of PRINCE2 since it provides structured methodology to manage and organize resources strategically. Similarly, ISO 27001 is an internationally acclaimed standard for Information security management in order to protect the confidentiality, integrity and availability of information. Hence this standard is mapped with Acquire and Implement (AI) and Monitor and Evaluate (ME) to achieve compliance through auditing and operationalizing security policies. Likewise, Delivery and Support (DS) domain perfectly maps with the ITIL which is the most popular IT service management framework.
5.7. Summary

In this chapter the role of governance, IT-governance and its goals are briefly discussed. A case study of an anonymous enterprise in Oman was carried out. Exhaustive literature review was done for selecting an IT-governance framework and its implementation issues and suitability assessments were done. A practical model for implementing IT-governance was devised and presented in a reputed conference and the extended version is published in the reputed journal.

5.8. Contribution from this Chapter

A paper titled “Information Security governance using COBIT: Focusing on critical success factors” was presented in the World Congress on Internet Security (WorldCIS-2012). The proceeding was published by IEEE, indexed in IEEE explore.
The extended version of the article was accepted (article in press) for publication in International Journal of Internet Technology and Secured Transactions, Published by Inderscience Publishers, with ISSN: 1748-5703.