CHAPTER 3

DESIGNING IT-GRC MODEL FOR OPTIMIZING

INFORMATION SECURITY

This chapter discusses about the role of IT-GRC in information security and proposes an IT-GRC model to optimize enterprise information security.

3.1. Strategically Balanced Governance, Risk and Compliance Model

There is a need for a model that can balance the interrelationships between the four strategic elements such as enterprise risk management, enterprise information security policy, governance and the processes of certification & evaluation. Kadam argues that an enterprise information security program’s effectiveness depends on a well-designed and implemented security policy. To run any business successfully we need both financial and human resource policy. Similarly in modern business where information systems play a significant role an information security policy is highly critical[91].

The model should also create a real-time level of integration through Business Process Execution Language (BPEL) based technologies. BPEL will be useful to define collaborative business processes that span several enterprises having disparate platforms and architectures. Thereby BPEL can also assist the assessment of compliance activities with local information security policies and executed in a distributed infrastructure[92]. Taken together the areas of risk management, enterprise information security policy, governance that relies on the COBIT framework, and the processes of evaluation, certification and audit need to be contained into a strategically balanced IT-GRC framework. In order to achieve this, a strategically balanced model is required that considers the changing business environment and the
influence of cross border regulatory laws which needs to be supported by latest technological infrastructure. Auditing needs to be done tactically since extended enterprises produce information supply chains which create interdependencies among business partners which are mostly ignored by the managers. COBIT and ITIL can be used for this purpose since they provide directions from a technology management perspective and service management perspective respectively[93]. Auditing is inherently tactically in nature as it seeks to find gaps in performance and reports generated and reviewed from the standpoint of what needs to be improved over time. It is a critical component of the proposed model to ensure a high level of agility and information flexibility within the model. The reliance on BPEL as a unifying technology for ensuring processes that span multiple departments and divisions can also create greater inter-process efficiencies is key to any framework to succeed[94]. The reliance on process-based approaches to re-engineering an enterprise however fall short over time as they also must be anchored in metrics of performance as well [95]. This reliance on auditing as a tactical input to a strategic process can be seen in manufacturing industries[96]. Performing gap analysis and variance analysis is a core activity in auditing, and that analysis is the basis for creating dashboards and benchmarks that in turn provide direction, context, prioritization and focus for more strategic and all-encompassing GRC frameworks [97]. It is so significant to review auditing from a manufacturing standpoint as it integrates the concepts of scorecards for suppliers, strategies for reducing the cost of quality and compliance and managing risks.
3.2. Proposed IT-GRC Model

Above mentioned points necessitate the development of a balanced model that encapsulates the concepts of ERM, Enterprise Information Security Policy, IT Governance and audit for evaluation and certification. Using auditing as an information source, all of these components are combined to create a model that seeks to balance risk and IT investment with potential revenue gains and cost reductions over time.

At the foundation of this model shown in figure-3 is the ERM platform which includes BPEL-based workflow support for recreating process-based integration across all areas of the model.

![Figure 3 Proposed IT-GRC Optimization Model](image)
Relying on ERM as a platform both mitigating risk on the one hand and as a framework or defining cost controls and quantifying revenue opportunities through auditing creates a foundation for ensuring transparency and information velocity. Also defining COBIT Initiatives and strategies in conjunction with the information workflows from audits provides the necessary intelligence for creating Enterprise Information Security Policy.

Taken together this model allows for greater agility in responding to significant change in external environments and more effective levels of risk mitigation as well. Taken from the context of a Service-Oriented Architecture (SOA) the proposed model also creates significant opportunities for creating Web Services that interlink its four key components, as evidenced by previous SOA implementations used as governance, risk and compliance frameworks[94]. Also inherent in the design of the proposed model is the development of strategies to overcome resistance to change as well. Meybodi defines that an integration point between cost controls and audit processes, benchmarks can be created that align with their reporting[96]. Anchoring compliance initiatives within financial results is possible over time using the proposed conceptual model as it has variance analysis inherently built into the structure. Instead of having to rely on specific components for their process-based integration, the proposed governance, risk and compliance model concentrates on creating a more efficient approach to having ERM serve as the coordinating layer of the model. This frees up audit, COBIT and evaluation cycles within the model to create more responsiveness and agility to market conditions over time.

As the more tactically oriented strategies are more focused on auditing and more strategic on ERM and IT Governance, the proposed governance, risk and compliance model aligns these two areas to their unique roles in a corporate-wide governance,
risk and compliance framework. Essential to any research effort in this area is the need to seek out process-based and goal-driven integration points across ERM, Enterprise Information Security Policy, and controls based security and compliance and evaluation and audit workflows as well. Figure 3 shows the proposed conceptual governance, risk and compliance model that puts into context the four strategic areas of coverage within this proposed research effort.

The following chapters will provide in-depth evaluation from scientific perspective and implementation approaches that is logically structured to support the proposed IT-GRC model.

3.3. **Summary**

An integrated enterprise governance, risk and compliance model was developed where ERM acts as a platform both mitigating risk on one hand and as a framework for defining cost controls and quantifying revenue opportunities. The controls can be tightened or loosened based on the evaluation and audit process by applying various security policies. The model will help enterprises to maintain optimized risk management strategy, governance and enterprise information security policies in synchronization with each other and at the same time attain a high level of transparency and consistency with auditing and compliance requirement.

3.4. **Contribution from this Chapter**

A research article featuring the proposed model was presented in The 2010 International Conference on Security and Management (SAM’10) conduct as a part of The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing at Las Vegas, United States of America. The proceeding was published by Security world academy of science, and available at http://www.gbv.de/dms/tib-ub-hannover/654559902.pdf, page 99-103.