ABSTRACT

Due to globalization and stiff completion in the contemporary business, there is a phenomenal change in the way business is being conducted. The advancements in network computing have enabled information systems to act as a scaffold to conduct business efficiently. This has drastically shifted the application of computers as a business tool to automate processes, to IT systems supporting information based assets. As enterprises are extending their operations across borders and becoming more elastic, computer security has evolved into information security. By defining security objectives in the context of the business environment, an enterprise can create and operate a systematic and comprehensive approach to security which can be measurable and optimized. Research studies indicate that the enterprises concern about the possibility of a security breach and loss of confidential information combined with threats from natural hazards is ever growing and reached alarming levels. To address this issue, numerous standards and control frameworks were published such as ISO 27001, COBIT, HIPAA, PCI-DSS, COSO, SOX, FISMA, ITIL and NIST standards. The real challenge for the management is in selecting and implementing information security control measures that are aligned with the strategic objectives and other organizational factors. This issue indicates that a holistic enterprise information security program aligned to enterprise business objectives, considering all functional units of the extended enterprise with measurable metrics is the need of the time. IT governance, risk management and compliance (IT-GRC) solution combines risk assessment, control management, policy management, monitoring and evidence generation activities. Therefore, this research study primary focuses to develop a converged IT-GRC model for addressing information security issues which can quantitatively measure the efficiency, effectiveness, usability and
return of investment by adopting a scientifically proven methodology to assess the interdependencies of security control objectives. Proposed IT-GRC model provides a platform to understand the relation between its components and facilitate what-if analysis by arriving at the Figure of Merit of the selected control objectives in governance, risk and compliance.