Abstract

e-Government services are becoming one of the most important and efficient means by which governments (G) interact with businesses (B) and citizens (C). This has brought not only tremendous opportunities but also serious security challenges. Critical information assets are exposed to current and emerging security risks and threats. In the course of this study, it was learnt that e-government services, implementation and service delivery, are heavily guided and benchmarked by e-Government maturity models (eGMMs). However, the models lack built-in security services, technical as well as non-technical. They also measure quantity rather than quality of e-government services which leads to lack of strategic objectives alignment between e-government services and security services. Information security has an important role in mitigating security risks and threats posed to e-government services. Security improves quality of the services offered, and cuts across entire organizations. It requires involvement of employees at all levels: strategic, tactical and operational. Therefore, it is imperative that confidentiality, integrity and availability of critical information being stored, processed, and transmitted between G, B and C, become an integral part of e-government services, from planning, development, implementation, delivery, to maintenance phases.

In light of the above, the goal of this research work is to propose *a framework that would facilitate government organisations to effectively offer appropriate secure e-government services*. To achieve this goal, an empirical investigation was conducted in one of the developing regions in the sub-Saharan Africa; involving six Tanzanian government organizations. The investigations were inter-foiled by a sequence of structural compositions resulting in a proposition of *a framework for securing e-government services which integrates IT security services into eGMM*s. The framework will facilitate government organisations to effectively offer appropriate secure e-government services; hence contributing into formation of citizens' trust, and consequently the success of e-government initiatives. The research work was mainly guided by a design science research approach complemented in parts by systemic-holistic and socio-technical approaches. Additionally, the proposed framework was qualitatively evaluated using criteria, such as simplicity, coverage and completeness, compliance to security standards, usefulness, and trustworthiness. The evaluation results indicated that the framework is highly accepted in the studied organisations at all levels. All major research results from the studies were reported in the research papers published at the appropriate peer-reviewed internationally recognised conferences and journals in information security and e-government.

The thesis contributes to the empirical and theoretical body of knowledge within the computer and systems sciences on securing e-government structures. It encompasses a new approach to secure e-government services incorporating security services into eGMMs. Also, it enhances the awareness, need and importance of security services to be an integral part of eGMMs to different groups such as researched organizations, academia, practitioners, policy and decision makers, stakeholders, and the community.