# Evaluation and prioritization of information security controls of ISO/IEC 27002:2013 for SMEs Through Fuzzy TOPSIS

Tariq, Muhammad Imran; Tayyaba, Shahzadi; De-la-Hoz-Franco, Emiro; Ashraf, Muhammad Waseem; Rad, Dana V.; Butt, Shariq Aziz; Santarcangelo, Vito.

## Abstract

Managing a large number of Information Security controls with slight impact may increase the extra effort and time in the shape of implementation and mitigation of risk. Therefore, Information Security Controls need to be prioritized. The main goals of this paper are to an in-depth study of ISO/IEC 27002:2013 that consists of 114 information security controls with 35 security domains and to rank/prioritize these controls. In this study, a questioner was designed and distributed it among Information Security Experts having experience of Information Security deployment in Small Medium Enterprises (SMEs). The study initially studied different methodologies for prioritization of Information Security Controls, developed criteria including effectiveness, implementation time, mitigation time, risk and budgetary constraints to evaluate ISO/IEC 27002:2013 control. The study applies a Fuzzy Technique for Order of Preference by Similarity to Ideal Solution TOPSIS technique to evaluate and rank the information security controls. A fuzzy TOPSIS methodology comprising linguistics data is used to get unclear conditions and, therefore, fuzzy TOPSIS is used as a tool to allow a more precise calculation of inaccurate parameters than old-style methods. We contend that evaluating of ISO/IEC 27002:2013 using fuzzy TOPSIS leads to a great accurate assessment and, therefore, supports an effective selection/ranking/ prioritization of information security controls in SMEs.

## Author keywords

Fuzzy logic; Information security; Information security controls; ISO/IEC 27002:2013; TOPSIS