Abstract

Information security control assessment provides a comprehensive control analysis approach to assist an organization in measuring the effectiveness of its current and planned security controls. ISO/IEC 27005 is a risk management framework that can manage and treat risks in organizations. However, ISO/IEC 27005 does not define a clear guideline on how to select and prioritize information security control despite the need for an efficient security analysis method. The ISO 27005 framework mostly depends on subjective judgment and qualitative approaches for security control analysis. This paper aims to improve the ISC analysis method by proposing the concept of multiple attribute decision making to provide clear guidelines in solving these issues. Order performance by similarity to ideal solution (TOPSIS) method was utilized to determine the critical vulnerable controls on the basis of different evaluation criteria. We argue that evaluating ISC by using TOPSIS leads to a cost-effective analysis and an efficient assessment in terms of testing and selecting ISCs in organizations.
- Douglas W. Hubbard. The Failure of Risk Management: Why It is Broken and How to Fix It. Willy, New Jeresy, USA, 2009.
- ISO/IEC. Iso 27005 information technology security techniques information security risk management, 2008.
- K. Paul Yoon and Ching-Lai Hwang. Multiple Attribute Decision Making: An


**Index Terms**

Computer Science  
Security

**Keywords**

Information security controls assessment  
multiple attribute decision making  
security controls analysis.