ABSTRACT

In this ever-evolving era, organizations are faced with increasingly complex challenges in managing their information security. The use of one security management standard or framework is considered less than optimal because there is no one solution that covers the entire organization. Therefore, there is a need to describe activities that integrate information security management based on existing standards and frameworks. This research aims to provide an overview of the implementation of security management activities in four organizations based on the integration of ISO 27001, NIST CSF, and CIS Control V8, data collection was carried out by conducting interviews with sources in each organization. Organization A which operates in the informatics sector has a good level of implementation of security management with a score of 3.3. Meanwhile, Organization B in the cultural sector only achieved a score of 1.9 in the sufficient category. Organization C in the health sector is also at a fair level with a score of 2.5. On the other hand, Organization D in the education sector showed satisfactory results with the highest score, namely 4.8. By assessing the implementation of security management that has been carried out, the organization can make improvements that are appropriate to the scope of the organization. First, Organization A and Organization C. It is recommended that these two organizations implement a 'Defense in depth' approach, which involves implementing layered security. Meanwhile, Organization B can focus on "Information Security", this is related to the purpose of using computer networks in that organization. On the other hand, organization D, which is considered to be very good in implementing security management, can make improvements to preventive activities in the organization.

Keywords – security management, standards, framework, assessment, ISO 27001, NIST CSF, CIS Control V8.