ABSTRACT

XYZ University has developed XYZ application to support academic and non-academic activities of the academic community. Application development continues to be carried out both in terms of interface, user experience, and security. During the first interview with the XYZ development team, cases were found that had the potential for risk. Therefore, information security evaluation and risk mitigation are needed to improve information security in XYZ applications. This research is conducted with the guidance of the ISO 27001: 2022 standard, and the use of the FMEA (Failure Mode and Effect Analysis) method to identify and determine the level of potential risk levels. As well as providing control recommendations based on ISO 27002: 2022. The results of risk identification in this study found 10 clauses out of 93 clauses in Annex A ISO 27001 which are the focus of risk handling. Of the 10 clauses, risk mitigation recommendations are given based on the level of risk level. The recommendations given are based on the ISO 27002: 2022 practical standard guide. This implementation is expected to help XYZ manage information security more effectively and in accordance with international standards.

Keywords: *ISO 27001, ISO 27002, FMEA, information security*