ABSTRAK

Intensitas ancaman terhadap keamanan sistem yang semakin meningkat menjadi hal yang konsen saat ini. Ancaman muncul dikarenakan adanya sebuah celah kerentanan yang dapat dimanfaatkan. Untuk mencari celah pada SIA perusahaan dilakukan *scanning* kerentanan menggunakan OWASP *(The Open Web Application Security Project)* dan hasilnya diketahui bahwa terdapat kerentanan pada sistem terkait dengan *Content Security Policy (CSP)*. Berdasarkan hal tersebut dilakukan tanya jawab terkait dokumen milik perusahaan yang berkaitan dengan keamanan informasi dan didapatkan hasil bahwa belum adanya aturan tertulis terkait dengan keamanan informasi dan risiko yang menyertainya. Untuk itu penelitian ini berusaha mengidentifikasi, menilai, mengurangi, dan mengendalikan ancaman dan kerentanan pada SIA perusahaan melalui manajemen risiko keamanan informasi.

Penelitian ini akan berfokus pada standar ISO/IEC 27005:2018 dalam melakukan manajemen risiko keamanan informasi dan rekomendasi kontrol kemanananya mengacu pada ISO/IEC 27001:2013. ISO/IEC 27005 mendukung konsep umum yang berlaku di ISO/IEC 27001 dan disiapkan untuk mendorong implementasi keamanan informasi berdasarkan pendekatan *risk management*. Langkah-langkah penelitian mengikuti *guide* ISO/IEC 27005 yaitu *Context Establishment, Risk Assessment, Risk treatment, Risk Communication,* dan *Risk Monitoring and Review*. Pengambilan data dilakukan melalui peninjauan dokumen perusahaan dan wawancara untuk aktivitas penetapan konteks dan identifikasi risiko selanjutnya dilakukan juga penyebaran kuesioner untuk analisis risiko dan pemilihan penanganan risiko.

Identifikasi terhadap aset, ancaman, kerentanan, dan kontrol terlebih dahulu dilakukan sebelum proses analisis risiko. Didapatkan hasil yaitu 39 aset, 40 ancaman, 93 kerentanan, dan 39 kontrol berdasarkan identifikasi tersebut. Hasil analisis risiko mengungkapkan bahwa dari 234 skenario risiko terbagi menjadi terbagi menjadi 25 risiko dengan level resiko *high (10,7%)*, 119 risiko dengan level risiko *medium (50,9%)*, dan 90 risiko dengan level risiko *low (38,5)%*. Dari evaluasi risiko terdapat 38 kelompok risiko yang tidak diterima sehingga perlu diberikan rekomendasi kontrol keamanan lanjutan dan penanganannya. Pemilihan penanganan risiko/*risk treatment* dari 234 skenario risiko yang ada terbagi menjadi 143 *risk modification* (56,7%), 0 *risk avoidance*, 7 *risk sharing/risk transfer* (2,9%), dan 83 *risk retention* (40,4%). Domain kontrol keamanan yang paling banyak direkomendasikan yaitu A.11 *Physical and environmental security*. Untuk *risk avoidance, risk transfer,* dan *risk retention* tidak diberikan rekomendasi kontrol. Hasil penelitian yang berupa rekomendasi kontrol keamanan beserta dengan alur penanganannya yang diharapkan dapat membantu perusahaan menghadapi permasalahan terkait keamanan yang ada.

Kata Kunci: Manajemen Risiko, ISO/IEC 27005:2018, Keamanan Informasi, Sistem Informasi Akuntansi.

ABSTRACT

The intensity of threats to system security that is increasing is becoming a matter of concern today. Threats come because there is a vulnerability that can be exploited. To find loopholes in the company's accounting information system, a vulnerability scan was carried out using OWASP (The Open Web Application Security Project) and the result was that the vulnerability in the system was related to the Content Security Policy (CSP). Based on this, a question and answer session was conducted regarding company documents related to information security and the results obtained that there are no rules related to information security and the risks that accompany it. For this reason, this study seeks to identify, assess, reduce, and control threats and vulnerabilities in a company's AIS through information risk management.

This research will focus on the ISO/IEC 27005:2018 standard in conducting information security risk management and security control recommendations referring to ISO/IEC 27001:2013. ISO/IEC 27005 supports the general concepts applicable in ISO/IEC 27001 and was developed to encourage the implementation of information security based on a risk management approach. The research steps following the ISO/IEC 27005 guidelines are Context Establishment, Risk Assessment, Risk treatment, Risk Communication, and Risk Monitoring and Review. Data were collected through company documents and interviews for context establishment and risk identification and questionnaires were also distributed for risk analysis and risk treatment selection.

Identification of assets, threats, vulnerabilities and controls is carried out prior to risk analysis. The results obtained are 39 assets, 40 threats, 93 vulnerabilities, and 39 controls based on the identification. The results of the risk analysis revealed that from 234 risk scenarios, they were divided into 25 risks with a high risk level (10.7%), 119 risks with a medium risk level (50.9%), and 90 risks with a low risk level (38.5).)%. From the risk evaluation, there are 38 risk groups that are not accepted, so it is necessary to provide recommendations for further safety control and handling. The selection of risk treatment/risk treatment from 234 existing risk scenarios is divided into 143 risk modification (56.7%), 0 risk avoidance, 7 risk sharing/risk transfer (2.9%), and 83 risk retention (40.4%). The most recommended security control domain is A.11 Physical and environmental security. For risk avoidance, risk transfer, and risk retention, no control recommendations are given. The results of the research in the form of recommendations for security controls along with the handling flow are expected to help companies deal with existing security-related problems.

Keywords: Risk Management, ISO/IEC 27005:2018, Information Security, Accounting Information Systems.