INTISARI

Insiden kebocoran informasi sensitif mengakibatkan dampak bisnis yang signifikan terhadap organisasi. Untuk melakukan mitigasi, organisasi perlu terlebih dahulu melakukan analisis risiko dengan berpedoman pada model risiko. Namun model risiko yang ada memiliki permasalahan terkait dengan obyektivitas dan konteks bisnis yang digunakan untuk merepresentasikan profil risiko. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan model risiko yang memiliki konteks bisnis dan menggunakan prosedur metode penilaian risiko yang lebih obyektif. Penggunaan konteks bisnis dimaksudkan untuk membantu membangun komunikasi yang relevan antara pihak teknis dan manajemen bisnis. Sedangkan obyektivitas dimaksudkan untuk mengurangi bias terhadap hasil model risiko. Untuk merepresentasikan konteks bisnis, model risiko menggunakan metrik berupa dampak keuangan, reputasi, tingkat kritis, ukuran organisasi dan jenis organisasi. Kelima metrik tersebut memiliki tingkat validitas serta reliabilitas yang baik. Untuk mengembangkan model tersebut, terdapat tiga proses dan dua entitas eksternal yang terlibat. Proses tersebut adalah *Adaptable Classification Data*, *Data Measurement* dan *Cross Label Analysis*. Sedangkan entitas eksternal yang terlibat adalah pihak teknis dan manajemen bisnis organisasi. Untuk menghasilkan keluaran, model risiko menggunakan metode *text mining, TF-IDF* dan *K-Modes*. Keluaran model risiko menghasilkan kombinasi risiko sebanyak 108 kombinasi yang terdiri dari 48% peluang tingkat risiko tinggi, 29% peluang tingkat risiko menengah, dan 23% peluang tingkat risiko rendah. Berdasarkan hasil analisis komparatif, model risiko memiliki keunggulan dalam menghasilkan analisis risiko yang lebih obyektif dan detail. Hal tersebut berdasarkan hasil pengujian dan evaluasi bahwa model risiko tidak menggunakan *expert judgement* dalam proses estimasi risiko. Selain itu, model risiko memiliki variansi yang lebih besar dibandingkan dengan model risiko lain. Hal tersebut merepresentasikan bahwa model risiko penelitian memiliki keragaman nilai dan kedalaman inspeksi yang lebih baik terhadap suatu ancaman keamanan informasi.

ABSTRACT

The incidence of sensitive information leakage has a significant business impact on the organization. In order to mitigate those problem, organizations need to carry out risk analysis based on the risk model as reference in estimating risk. However, the existing risk model has problems related to objectivity and business context. Therefore, this study aims to develop a risk model where it has more objective procedure and involves business context in estimating risk. The involvement of business context in risk model is intended to build relevant communication between the technical and business management parties. The approach of objective procedure is used to reduce bias towards the results of the risk model. In order to represent the business context, the proposed risk model uses metrics such as financial impact, reputation, critical level, organizational size and type of organization. Those metrics have adequate level of validity and reliability as measurement variables. In order to develop the model, there are three processes and two external entities involved. The process is Adaptable Classification Data, Data Measurement and Cross Label Analysis. The external entities involved are the technical parties and business management parties in organizations. In order to produce output, the proposed risk model uses text mining, TF-IDF and K-Modes. The proposed risk model generates 108 combinations consisting of 48% chance of high risk level, 29% chance of medium risk level, and 23% chance of low risk level. Based on the results of comparative analysis, the proposed risk model has advantage in producing more objective and detailed risk analysis. It is based on the results of testing and evaluation where the risk model does not involve expert judgment to fill weight of metrics. Moreover, the proposed risk model also has higher variance compared the other model where it is caused that the proposed risk model inspects more detailed a threat in information security.