Perancangan dan Analisis Manajemen Risiko Keamanan Informasi Berdasarkan ISO 27005 (Studi Kasus Pada Audit Management System (AMS) Departemen Audit Internal XYZ) = Design and Analysis of Information Security Risk Management Based on ISO 27005 (Case Study on Audit Management System (AMS) of XYZ Internal Audit Department)

Diar Eka Risqi Hidayatullah, author

Abstrak

Keamanan informasi merupakan aspek penting dan didukung oleh laporan yang dikeluarkan oleh Internal Audit Foundation yang berjudul Risk in Focus 2024 Global Summary disebutkan bahwa risiko paling besar yang akan dihadapi di tahun 2024 adalah Cybersecurity and Data Security dengan skor 73% untuk rata-rata worldwide. Berdasarkan report yang dikeluarkan oleh International Business Machine (IBM) berjudul Cost of a Data Breach Report 2023 dibutuhkan waktu rata - rata 204 hari untuk mengetahui adanya kebocoran data yang dialami pada instansi atau organisasi terdampak, serta membutuhkan waktu 73 hari untuk menanggulangi kebocoran data tersebut. Dalam rangka mewujudkan digitalisasi tersebut dilakukan implementasi sistem Audit Management System (AMS) yang dapat mengakomodir proses audit mulai dari tahap Planning, Execution, dan Reporting serta proses tindak lanjut rekomendasi baik yang dihasilkan dari audit internal maupun audit eksternal. Penggunaan AMS tidak terlepas dari risiko, akses menuju AMS dapat dilakukan tanpa Virtual Private Network (VPN). Dalam penelitian ini dilakukan risk assessment berbasis standar ISO/IEC 27005:2022 dengan mengusulkan metode penghitungan konsekuensi berdasarkan klasifikasi data yang ada dalam sistem dan metode peghitungan kemungkinan berdasarkan proses bisnis yang memiliki dampak ke kerentanan sistem serta risiko yang perlu dimitigasi akan digunakan ISO/IEC 27002:2022 sebagai standar untuk mengantisipasi risiko yang terjadi. Hasil pemeriksaan risiko diketahui terdapat 24 risiko dengan 1 risiko level sangat tinggi, 3 risiko level tinggi, 8 risiko dengan level sedang, 11 risiko dengan level rendah, dan 1 risiko dengan level sangat rendah yang terdapat pada departemen audit internal XYZ.

.....Information security is an important aspect and supported by a report issued by the Internal Audit Foundation entitled Risk in Focus 2024 Global Summary. Biggest risk that will be faced in 2024 is Cybersecurity and Data Security with a score of 73% for the global average. Based on a report issued by International Business Machine (IBM) entitled Cost of a Data Breach Report 2023, takes an average of 204 days to find out about a data leak by an affected agency or organization, and takes 73 days to overcome the data leak. In order to realize this digitalization, an Audit Management System (AMS) system was implemented which can accommodate the audit process starting from the Planning, Execution and Reporting stages as well as follow-up process for recommendations process. Using AMS is not without risks, access to AMS can be done without a Virtual Private Network (VPN). In this research, a risk assessment was carried out based on the ISO/IEC 27005:2022 standard by proposing a method for calculating consequences based on the classification of data in the system and a method for calculating possibilities based on business processes that have an impact on system vulnerabilities and risks that need to be mitigated. ISO/IEC 27002:2022 will be used to anticipate risks. Results of the risk examination revealed that there were 24 risks

with 1 very high level risk, 3 high level risks, 8 medium level risks, 11 low level risks, and 1 very low level risk in the XYZ internal audit department.