ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022

Oleh

Hardiyanti Rohmania

Program Studi Sistem Informasi

ABSTRAK

Manajemen risiko Teknologi Informasi (TI) merupakan bagian penting untuk keberlangsungan hidup organisasi. Saat ini, Unit Penunjang Akademik Teknologi, Informasi, dan Komunikasi (UPA TIK) Universitas Pendidikan Ganesha yang masih perlu perbaikan lebih baik dan pemantauan berkelanjutan terhadap isu-isu keamanan. OCTAVE-S digunakan untuk menganalisis risiko keamanan organisasi yang berskala kecil dan ISO 27001:2022 untuk merumuskan rekomendasi mitigasinya. Berdasarkan hasil analisis, ditemukan bahwa 2 kriteria dampak berada pada level rendah dan 3 kriteria dampak berada pada level tinggi ketika terjadi insiden keamanan informasi. UPA TIK Undiksha memiliki 6 aset yang terbagi menjadi aset layanan atau apliaksi, sistem, informasi, dan SDM. Evaluasi 15 praktik keamanan organisasi, UPA TIK Undiksha memiliki 3 praktik keamanan pada status *Green*, 12 praktik keamanan pada status *Yellow*. Pemilihan aset kritis dilakukan dengan mengurutkan aset sesuai prioritas dan kekritisannya dimana semua aset yang teridentifikasi terpilih menjadi aset kritis yang memiliki persyaratan keamanan utama yaitu Kerahasiaan, Integritas, dan Ketersediaan. Mengidentifikasi ancaman terhadap aset kritis dilakukan melalui jalur akses jaringan, fisik, dan masalah lainnya dengan aktor yang berasal dari pihak *internal* dan *external* UPA TIK Undiksha. Rekomendasi mitigasi ISO 27001:2022 diberikan sebanyak 50 rekomendasi Kontrol ISO yang telah mencakup rekomendasi untuk area praktik keamanan organisasi dan rekomendasi aset organisasi serta diberi referensi beberapa dokumen wajib ISO 27001:2022 terkait dengan rekomendasi yang telah diberikan.

Kata Kunci: Manajemen Risiko, Keamanan Informasi, OCTAVE-S, ISO 27001:2022

INFORMATION SECURITY RISK MANAGEMENT ANALYSIS USING OCTAVE-S FRAMEWORK AND ISO 27001:2022

By

Hardiyanti Romania

Information Systems Study Program

ABSTRACT

Information Technology (IT) risk management is a crucial aspect of an organization's survival. Currently, the Academic Support Unit for Technology, Information, and Communication (UPA ICT) at Ganesha University of Education still requires improvement and continuous monitoring of security issues. OCTAVE-S is used to analyze small-scale organizational security risks and formulate mitigation recommendations in accordance with ISO 27001:2022. Based on the results analysis, it was found that 2 impact criteria were at a low level and 3 impact criteria were at a high level when an information security incident occurred. UPA ICT Undiksha has six assets, divided into service or application assets, systems, information, and human resources. Evaluation of 15 organizational security practices reveals that UPA ICT Undiksha has 3 security practices at Green status and 12 at Yellow status. The selection of critical assets is carried out by sorting assets according to their priority and criticality, where all identified assets are selected as essential assets that meet the primary security requirements, namely Confidentiality, Integrity, and Availability. Identifying threats to critical assets is conducted through network access paths, physical security, and other issues with actors originating from both internal and external parties of UPA ICT Undiksha. The ISO 27001:2022 mitigation recommendations are presented in the form of 50 ISO Control recommendations, which encompass both organizational security practice areas and recommendations for organizational assets. These recommendations are supported by references to several mandatory ISO 27001:2022 documents related to the provided guidance.

Keywords: Risk Management, Information Security, OCTAVE-S, ISO 27001:2022