ANALISIS TINGKAT KEMATANGAN KEAMANAN INFORMASI MENGGUNAKAN *NIST CYBERSECURITY FRAMEWORK* DAN *CAPABILLITY MATURITY MODEL INTEGRATION (CMMI)* (STUDI KASUS: SISTEM INFORMASI AKADEMIK UNIVERSITAS TANJUNGPURA)

Abstrak

Penggunaan teknologi informasi di perguruan tinggi telah memberikan banyak kemudahan terutama dalam hal mengakses suatu informasi dengan cepat dan mudah. Salah satu perguruan tinggi yang mengimplementasikan tekonlogi informasi dalam pengelolaan data-data akademiknya adalah Universitas Tanjungpura (Untan). Data-data akademik tersebut dikelola didalam sebuah Sistem Informasi Akademik (SIAKAD) Untan. SIAKAD menampung banyak sekali data akademik dari seluruh fakultas sehingga akan berdampak pada munculnya risiko keamanan data dan informasi yang bisa mengancam kegiatan operasional karena semakin banyak data dan informasi yang disimpan, dikelola dan di *sharing* maka semakin besar risiko terjadinya kerusakan, kehilangan atau tereksformya data ke pihak luar yang tidak diinginkan. Sehingga perlu diketahui bagaimana tingkat kematangan keamanan informasi pada SIAKAD Untan untuk menjaga keamanan informasi dan melindungi data-data yang ada pada SIAKAD Untan. Pada penelitian ini akan diteliti tingkat kematangan keamanan informasi pada SIAKAD Untan menggunakan *NIST cybersecurity framework* dan CMMI. *NIST cybersecurity framework* merupakan *framework* manajemen risiko keamanan informasi yang digunakan untuk analisis proses manajemen risiko dimana akan dipetakan setiap kontrolnya untuk mendapatakan aktivitas dari kontrol *NIST cybersecurity framework.* Untuk penilaian tingkat kematangan SIAKAD Untan menggunakan CMMI yang merupakan model pendekatan untuk penilaian skala kematangan dan kemampuan sebuah organiasi perangkat lunak. Tingkat kematangan sangat diperlukan untuk mengetahui sejauh mana level operasional pada sebuah organisasi. Adapun hasil penilaian *maturity level* yang telah dilakukan pada *category* ID.AM telah memasuki level 2 dan *category* ID.RA juga telah memasuki level 2 sehingga maturity level *fuction indentify* berada pada level 2. Sehingga dari level tersebut dapat diberikan rekomendasi perbaikkan untuk mencapai level yang diharapkan.

Kata kunci: Keamanan informasi, NIST *cybersecurity framework*, CMMI, *Maturity level*, Sistem Informasi Akademik

ANALYSIS OF INFORMATION SECURITY MATURITY LEVEL USING NIST CYBERSECURITY FRAMEWORK AND CAPABILLITY MATURITY MODEL INTEGRATION (CMMI) (CASE STUDY: TANJUNGPURA UNIVERSITY ACADEMIC INFORMATION SYSTEM)

Abstract

The use of information technology in higher education has provided many conveniences, especially in terms of accessing information quickly and easily. One of the tertiary institutions that uses information technology to manage its academic data is Tanjungpura University (Untan). The academic data is managed in an unstructured academic information system (SIAKAD). SIAKAD accommodates a lot of academic data from all faculties so that it will have an impact on the emergence of data and information security risks that can threaten operational activities because the more data and information that is stored, managed, and shared, the greater the risk of damage, loss, or export of data to third parties. unwanted outside. So it is necessary to know how the maturity level of information security at SIAKAD Untan is maintained to protect existing data and maintain information security. In this study, the maturity level of information security at SIAKAD Untan will be examined using the NIST cybersecurity framework and CMMI. The NIST cybersecurity framework is an information security risk management framework that is used for analysis of the risk management process, where each control will be mapped to obtain activity from the NIST cybersecurity framework controls. Untan uses CMMI to assess SIAKAD's maturity level. CMMI is an approach model for assessing the maturity scale and capabilities of a software organization.Maturity level is needed to determine the extent to which the operational level in an organization is defined. The results of the maturity level assessment that has been carried out in the ID.AM category have entered level 2, and the ID.RA category has also entered level 2, so that the maturity level function identification is at level 2. So from that level, recommendations for improvement can be given to achieve the expected level.

Keywords: information security, NIST cybersecurity framework, CMMI, maturity level, academic information system.