

## **ANALISIS SISTEM MANAJEMEN KEAMANAN INFORMASI PADA PERGURUAN TINGGI MENGGUNAKAN ISO 27001:2013**

**Yohanes Darmawan dan Agustinus Fritz Wijaya**

Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya  
Wacana

Jalan Dr. O. Notohamidjojo No. 01-10 Blotongan, Salatiga, 50715

Telp : (0298) 321212, Fax : (0298) 321433

E-mail : [682013010@student.uksw.edu](mailto:682013010@student.uksw.edu)<sup>1)</sup>, [agustinus.wijaya@staff.uksw.edu](mailto:agustinus.wijaya@staff.uksw.edu)<sup>2)</sup>

---

### **Abstract**

*Security issues are one important aspect of an information system. When disrupting system performance, security is often reduced or even eliminated. Security has always been an interesting issue in the development of communication, interaction, and human socialization even in the world of education. Some universities today also have a security system in each faculty such as Satya Wacana Christian University Faculty of Information Technology (FTI-SWCU) from the door of each classroom that must attach the ID card already inserted into the security system. Security of the Faculty of Tekonolgi This information is handled by the FTI-SWCU Laboratory. FTI-SWCU requires a special international standard to reduce the security problems that occur, of course FTI-SWCU wants to have good security in the field of information technology. ISO 27001 is an international standard in implementing information security management systems or better known as Information Security Management Systems (ISMS). Implementing the ISO 27001 standard will assist organizations in establishing and maintaining an information security management system (ISMS). ISMS is a set of interrelated elements with the organization or company used to manage and control information security risks and to protect and maintain confidentiality, integrity and availability of information. Based on the results of the research, several findings are obtained: FTI-SWCU laboratory safety does not have Standard Operational Procedures (SOP) in writing but only delivered orally so that policies are also delivered orally. The third party in FTI-SWCU also only controls the existing systems but does not take evidence for documentation. Each user's access control is not documented in writing but is accessed on the FTI's own security audit system. External access prevention management for entry into the information system is not set in writing but is delivered only verbally and any system control is not documented. Security procedures only convey system changes and are not documented to employees. Based on the findings, there will be a comprehensive recommendation of the findings. The recommendation is better FTI-SWCU security on every control at ISO 27001: 2013 given documentation on each control such as policies to be undertaken by employees or organizations should have documents and SOPs in the FTI-SWCU security immediately documented so that every employee and organization knows the job duties of existing employees or organizations. The existing supportive safeguards should be upgraded such as providing CCTV to each class and FTI-SWCU aisles. The security system of FTI-SWCU users should be re-developed so that unexpected things happen. When controlling the system or network it is better to have the documentation so that it has the data when the unwanted happens as evidence..*

**Keywords:** Information Security Management Systems, ISO 27001:2013, Faculty, University.

### **Abstrak**

*Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Apabila mengganggu performa sistem, seringkali keamanan dikurangi atau bahkan ditiadakan. Keamanan selalu saja menjadi isu menarik dalam perkembangan komunikasi, interaksi, dan sosialisasi manusia bahkan di dunia pendidikan. beberapa universitas sekarang ini juga memiliki sistem keamanan di setiap fakultasnya seperti Fakultas Teknologi Informasi Universitas Kristen Satya Wacana (FTI-UKSW) yang sekarang ini menggunakan sistem keamanan dari pintu setiap ruang kelasnya yang harus menempelkan kartu ID yang sudah di masukkan kedalam sistem keamanan. Keamanan Fakultas Tekonolgi Informasi ini ditangani oleh bagian Laboratorium FTI-UKSW. FTI-UKSW memerlukan standar internasional khusus untuk mengurangi masalah keamanan yang terjadi, tentunya FTI-UKSW ingin memiliki keamanan yang baik di bidang teknologi informasi. ISO 27001 merupakan suatu standar internasional dalam menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan Information Security Management Systems (ISMS). Menerapkan standar ISO 27001 akan membantu organisasi dalam membangun dan memelihara sistem manajemen keamanan informasi (ISMS). ISMS merupakan seperangkat unsur yang saling terkait dengan organisasi atau perusahaan yang digunakan untuk mengelola dan mengendalikan risiko keamanan*

informasi dan untuk melindungi serta menjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) informasi. Berdasarkan hasil penelitian yang dilakukan, maka diperoleh beberapa temuan antara lain: keamanan laboratorium FTI-UKSW belum memiliki *Standard Operational Procedures* (SOP) secara tertulis tetapi hanya disampaikan secara lisan sehingga kebijakan-kebijakan yang adapun juga disampaikan secara lisan. Pihak ketiga yang ada di FTI-UKSW juga hanya mengontrol sistem-sistem yang ada tetapi tidak mengambil bukti untuk dokumentasikan. Kontrol akses setiap pengguna tidak di dokumentasikan secara tertulis tetapi diakses pada sistem audit keamanan FTI sendiri. Manajemen pencegahan akses dari luar untuk masuk ke sistem informasi tidak diatur secara tertulis tetapi hanya disampaikan secara lisan dan setiap mengontrol sistem tidak didokumentasikan. Prosedur-prosedur dalam keamanan hanya menyampaikan adanya perubahan sistem dan tidak didokumentasikan kepada karyawan. Berdasarkan temuan-temuan yang ada, maka akan diberikan rekomendasi secara menyeluruh dari temuan yang ada. rekomendasi tersebut adalah keamanan FTI-UKSW lebih baik pada setiap kontrol pada ISO 27001:2013 diberikan dokumentasi pada masing-masing kontrol seperti kebijakan-kebijakan yang akan dilakukan oleh karyawan atau organisasi seharusnya memiliki dokumen dan SOP dalam keamanan FTI-UKSW segera didokumenkan sehingga setiap karyawan dan organisasi mengetahui tugas-tugas kerja karyawan atau organisasi yang ada. keamanan pendukung yang ada harus ditingkatkan kembali seperti memberikan CCTV pada setiap kelas serta lorong FTI-UKSW. Sistem keamanan user FTI-UKSW harus dikembangkan kembali supaya hal-hal yang tidak diinginkan terjadi. Pada saat melakukan kontrol pada sistem atau jaringan lebih baik diberikan dokumentasi sehingga memiliki data pada saat hal yang tidak diinginkan terjadi sebagai bukti.

**Kata Kunci:** Sistem Manajemen Keamanan Informasi, ISO 27001:2013, Fakultas, Universitas.

## REFERENSI

- [1] Weill, Peter., Ross, Jeanne W. 2004. *IT Governance: How Top Performers Manage IT Decision Rights For Superior Results*. Harvard Business Press.
- [2] Sarno, Riyanarto. 2009. *Audit Sistem & Teknologi Informasi*. Surabaya: ITS Press.
- [3] Sarno, Riyanarto., Iffano, Irsyat. 2009. *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*. Surabaya: ITS Press.
- [4] Darmawi, H. 1999. *Manajemen Resiko*. Jakarta: Bumi Aksara.
- [5] Indrajit, E. R. 2011. *Peran Teknologi Informasi pada Perguruan Tinggi*. Indonesia: APTIKOM.
- [6] Aprian, R, Rizal, S. & Sobri. M. 2015. *Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO 27001:2013*". Jurnal Informatika Universitas Bina Darma Palembang, [digilib.binadarma.ac.id](http://digilib.binadarma.ac.id).
- [7] Mulyono, Joko. 2013." *Analisis Keamanan Komunikasi pada Internet berbasis SSL (Secure Socket Layer) / TLS (Transport Layer Secutity)*". Salatiga.
- [8] Kongo, Anggrini. 2016. "Manajemen Resiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Standar ISO/IEC 27001:2013". Salatiga.
- [9] Ermana, Fine Tanuwijaya, Haryanto; Adrian Mastan, Ignatius. "Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR Jatim". Jawa Timur.