Jurnal TAM (Technology Acceptance Model) Volume 11, Nomor 2, Desember 2020 Hal. 100-104
p-ISSN : 2339-1103
e-ISSN : 2579-4221

RISK ANALYSIS OF INSAN UNIVERSITY SYSTEM USING ISO 27001

Raniyah Ayu lestari[1], Dedy Syamsuar[2]
[1,2]Prodi Magister Teknik Informatika, Universitas Bina Darma, Palembang
[1,2]Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Seberang Ulu I, Palembang, Indonesia
E-mail: raniyahayulestari05@gmail.com, dedy_syamsuar@binadarma.ac.id

Article history:
Received: Oct 23, 2020
Revised: Nov 11, 2020
Accepted: Nov 18, 2020

Keywords:
UNIBI;
Security Information;
ISO 27001

Abstract

This study aims to apply the governance of Information and Communication Technology (ICT) at Bina Insani University. Governance itself has become a necessity and a demand in the application of ICT management. This study uses the ISO 27001 standard in measuring and assessing information security risks. Data collection is done by using the method of observation and interviews. The stages of research carried out in a row are (1) Identification of assets, (2) identification of security threats and vulnerabilities, (3) assessing CIA risk (Confidentiality integrity availability), (4) BIA business impact assessment (5) Resulting risk value is accepted or carried out management until risk evaluation Risk evaluation results show that there are still many activities that must be improved such as information disclosure and malware spread and implemented to improve the security of assets at the university of human development.

I. PENDAHULUAN

Sistem Universitas BINA INSAN layanan sistem mempunyai memiliki aset yang terpenting sebagai sarana bagi bidang Pendidikan,penetapan tata kelola teknologi informasi dan komunikasi menjadi kebutuhan dan tuntunan setiap Pendidikan seperti BINA INSAN dikarenakan peran TIK semakin penting bagi upaya peningkatan kualitas layanan Pendidikan sebagai salah satu realisasi dari tata kelola yang baik. Keamanan informasi merupakan salah satu aspek penting yang harus diperhatikan oleh organisasi dan perusahaan. Informasi baik berupa teks, gambar, audio, maupun video yang menyimpan asset penting bagi perusahaan, wajib dilindungi dengan sistem manajemen keamanan informasi. Kebocoran, kerusakan atau hilangnya suatu informasi dapat menimbulkan kerugian

Faktor manajemen keamanan informasi merupakan aspek yang sangat penting diperhatikan meningkatkan kinerja tata kelola keamanan informasi, mengalami masalah menyangkut kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability)untuk keamanan pada suatu aset yang ada di BINA INSAN dengan menggunakan standar ISO 27001.merupakan proses yang sistematis, mandiri, dan terdokumentasi untuk menperoleh keamanan suatu aset dengan kata lain yang digunakan oleh institusi termasuk dokumen sistem manajemen mutu yang dimiliki pencapaian sasaran mutu, meninjau keluhan user, dan lain-lainya Beberapa hal penting yang dapat dijadikan acuan mengapa standar ISO 27001dipilih yaitu, standar ini sangat fleksibel karena sangat bergantung pada kebutuhan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai, dan struktur organisasi. slain itu ISO 27001menyediakan sertifikat implementasi sistem keamanan informasi yang diakui secara internasional yang disebut dengan information security management system (ISMS), yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh pihak kampus bina insan atau konsep-konsep keamanan informasi.

Penelitian terdahulu terkait manajemen risiko sistem informasi diantaranya adalah ontology draft ISO 27001 tata cara implementasi ISO 27001 pada Sistem Informasi Manajemen analisis risiko pada sistem informasi akademik di perguruan tinggi dengan menggunakan metode OCTAVE Allegro evaluasi ISO 27001 pada sistem informasi pemerintahan dan evaluasi ISO 27001 pada layanan pelanggan Berbeda dengan penelitian sebelumnya, penelitian ini mengevaluasi kesiapan implementasi ISO/IEC 27001*Information Security Management Systems standard* pada Sistem Informasi Fakultas Teknik UNDIP dengan menggunakan metode *Failure Mode Effect and Analysis* (FMEA).

Dalam peraturan PP 71 tahun 2019 dijelaskan bahwa penyelenggaran sistem dan transaksi elekronik yang menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain untuk memenuhi tuntutan yang adil dan sesuai dengan pertimbangan tentang keamanan dan kewajiban, dalam penyelenggaraan sistem elektronik untuk menghapus informasi elektronik dan dokumen elektronik yang tidak relevan, yang berada dibawah kendalinya atas permintaan orang yang bersangkutan berdasarkan peran pemerintah dan memfasilitasi pemanfaatan teknologi dan

transaksi. Melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi dan elektronik yang mengganggu ketertiban umum dan mencegah peyebarluarsan penggunaan informasi elektronik dan dokumen yang memiliki muatan yang dilarang. Melihat pemasalahan tersebut maka diperlukan pengukuran untuk menganalisa beberapa kemungkinan resiko yang muncul pada sistem suatu aset dari penanganan resiko dan Melihat resiko terhadap universitas, dapat dilihat dari *beberapa* yang di timbulkan akibat kegiatanpengelolaan dan pemeliharaan data dan informasidalam keamanan sistem suatu aset informasi akademik terhadap system tersebut

II TINJAUAN PUSTAKA

2.1 ISO 27001

ISO 27001 adalah meningkat kebutuhan dan pengguna TIK dalam menunjang aktifitas bisnis dalam suatu organisasi akan meningkatkan nilai dari resiko akan gangguan keamanan informasi tersebut, peningkatan gangguan resiko pada suatu organisasi yang sangat tergantung layanan TIK akan sangat perpengaruh pada pencapaian suatu organisasi sehingga saat ini organisasi tersebut harus menyadari dan menerapkan suatu kebijakan yang tepat untuk melindungi aset informasi yang dimiliki salah satu kebijakan yang dapat diambil oleh organisasi untuk mengatasi gangguan informasi adalah dengan menerapkan manajemen keamanan informasi merupakan seperangkat unsur yang saling terkait dengan organisasi atau perusahaan yang digunakan untuk mengelola dan mengendalikan resiko keamanan informasi untuk melindungi dan menjaga kerahasiaan *(confidentiality)* integritas *(integrity)* dan ketersediaan *(availability)* informasi. Dengan menerapkan ISO 27001organisasi atau perusahaan dapat melindungi dan memelihara kerahasiaan dan integrasi informasi untuk mengelola dan mengendalikan resiko keamanan informasi pada organisasi atau perusahaan adalah standar internasional paling banyak digunakan untuk information sequrity management digunakan untuk melindungi *confidentiality integrity* dan *availability* dan informasi ISO 27001 bukan merupakan *technical* detail tapi tidak hanya berfokus pada IT tetapi juga penting didalam organisasiISO 27001 berfokus pada proses dan *bussines*aset pengurangan resiko aset.

2.2 Penilaian Resiko

Penilaian resiko adalah merupakan kegiatan penilaian atas kemungkinan kejadian yang mengancam pencapaian tujuan identifikasi dan analisis terhadap resiko yang relevan terhadap penyusunan laporan menilai resiko pengendalian merupakan suatu proses mengevaluasi efektivitas pengendalian intern suatu entitas menengah setelah menganalisa yang ada sebelumnya mengidentifikasi resiko seperti apa yang akan terjadi dan bagaimana suatu bisa terjadi maka tahapan selanjutnya memberikan penilaian tentang besarnya tingkatan terkaitnya resiko tersebut hal itulah menjadi bagian dari penilaian risiko itu sendiri dimana memberikan makna terhadap suatu bahaya yang teridentifikasi untuk memberikan gambaran seberapa besarnya resiko tersebut sehingga dapat diambil tindakan lanjutnya terhadap bahaya yang teridentifikasi apakah bahaya yang dapat diterima atau tidak.

Bagian dari analisis resiko adalah membuat kategori penilaian resiko. Proses penilaian resiko ini dapat dilakukan secara kualitatif Pada dasarnya untuk nilai resiko dihitung dengan cara mengalikan nilai dampak dan nilai kemungkinan terjadinya ancaman. Kategori penilaian resiko yang akan digunakan dalam manajemen risiko keamanan informasi pada penelitian ini dibagi menjadi tiga kategori yaitu: Risiko rendah (*Low Risk),* risiko sedang *(Medium Risk*), resiko tinggi *(High Risk)*.

2.3 Nilai Data Aset Dalam CIA *(Confidentiality integrity availability)*

Nilai data aset dalam CIAuntuk menentukan sebuah resiko yang diterima atau perlu pengelolaan terhadap resiko tersebut, maka perlu diketahui nilai dari resiko tersebut dihitung nilai aset dengan menjumlah kriteria confidentiality intergrity, availability berdasarkan hasil kuisoner. berikut ini nilai dari aset universitas bina insan menggunakan rumus sebagai berikut.

NC+NI+NV=NA

Dimana

1. **NA**: Nilai aset
2. **NC**: Nilai *Confidentiality* Kerahasiaan
3. **NI**: Nilai *Integrity* keutuhan
4. **NV**: Nilai *Availability* ketersediaan

2.4 Penilaian dampak bisnis BIA

Proses identifikasi atau dampak yang mungkin terjadi yang perlu di antisipasi dimassa depan akibat adanya suatu usulan kebijakan dalam sistem data aset, suatu usulan kebijakan sistem yang dapat memberikan pada aspek lingkungan baik secara lansung maupun tidak secara lansung**.**

Intinya mengevaluasi sistem aset yang ada dibina insan diusulkan berbagai aspek dan kepentingan yang saling berkaitan, dengan adanya analisis keamanan sistem data aset diharapkan adanya penilaian objektif membantu untuk menghindari hak ciptanya, mendorong dampak positif pada suatu keamanan yang menghindari resiko pada aset tersebut,

Jurnal TAM (Technology Acceptance Model) Volume 11, Nomor 2, Desember 2020 Hal. 100-104
p-ISSN : 2339-1103
e-ISSN : 2579-4221

Tabel .1 Penilaian skala impact analysis

Batas Toleransi Gangguan	Keterangan	Nilai
< dari 1 Minggu	*Not very low*	0-20
1hr s/d 2hr	*Low*	21-40
< 1hari	*Medium*	41-60
< 12 jam	*High*	61-80
< 1 jam	*Very high*	81>=100

2.4 Menentukan nilai resiko ancaman diterima atau melakukan pengelolaan resiko

Untuk menentukan resiko yang diterima maka dilakukan dengan rumus sebagai berikut.

NA X BIA X NT = NILAI RESIKO

1. **NA:** Nilai Aset
2. **BIA:** analisis dampak bisnis
3. **NT**: Nilai ancaman

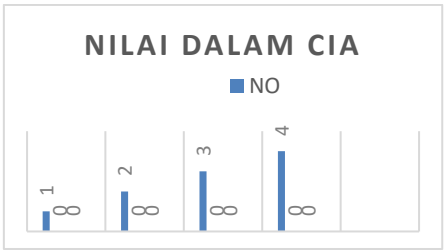
III KERANGKA PENELITIAN

Salah satu resiko yang ditimbulkan adalah kelemahan sistem mengenai timbulnya ancaman sistem Universitas bina insan yang ada di musi rawas yang dapat merugikan cukup besarpada Universita smaka diperluka npeniliaian resiko untuk menemukan dampak yang terjadi dan dapat menghasilkan informasi peringkat resiko, dalam penelitian dengan menggunakan motode ISO 27001. Untuk mengetahui peringkat resiko dari resiko rendah, resiko sedang dan resiko tinggi yang terjadi keamanan resiko akademik manajemen sistem tersebut.Tahap proses metode 27001 yaitu tahap pertama identifikasi ancaman mencari informasi-informasi yang berhubungan dengan sistem Universitasy ang menjadi target sebagai bahan penetrasi, tahap kedua dokumen ancaman keamanan aset yang berisi tentang deskripsi ancaman, target ancaman, dan Teknik ancaman.Tahap terakhir mengenai tentang ISO 27001 ini mengetahui hasil kalkulasi dari ancaman memilik rating penilaian 0-20 dengan peringkat keterangan resiko rendah, rating penilain 41 -60 dengan peringkat keterangan rating peringkat resiko sedang, rating penilain >81> =100 dengan peringkat keterangan resiko tinggi dan *security* report laporan akhir yang berisikan tentang deskripsi ancaman, target ancaman, rating ancaman, Teknik ancaman, dan tindakan pencegahan terhadap ancaman

3.1 Hasil Penilaian dalam CIA

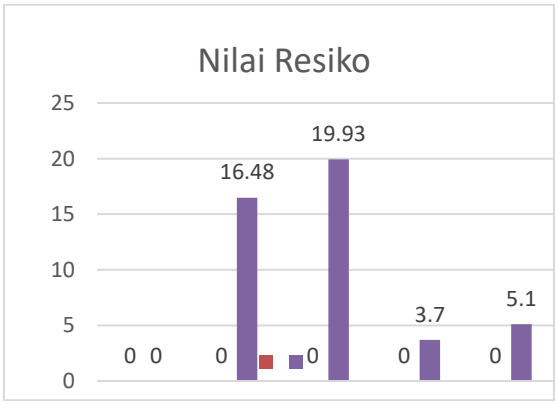
Hasil dalam kategori aset yang mana nilai paling besar ialah yang mengalami resiko yang tertinggi berikut daftar nilai dalam *CIA.* Hasil pengamatan setiap kegiatan dari pihak kampus bina insan atau yang ahli dalam bidang keamanan informasi insiden jika itu terjadi dan Keterangan setiap pemilik atau pengguna aset di universitas bina insan.

1. Ketidak sengajaan manusia Kerusakan hardware dan software atau kehilangan data pada computer Penyingkapan informasi
2. Semua kebijakan tersedia dan disosialisasikan seluruh pihak yang terkait
3. Semua aset yang bertipe informasi sudah diklasifikasikan berdasarkan bentuk dan kesensitifannya



3.2 Nilai analisis dampak bisnis (BIA)

Dari perhitungan yang sudah dilakukan sebelumnya , maka dapat ditentukan nilai dari masing- masing di lihat tabel di bawah ini. Hasil nilai resiko diterima atau dilakukan pengelolaan resiko Dan beberapa perhitungan yang sudah dilakukan sebelumnya, maka dapat ditentukan nilai dari masing-masing aset pada tabel dibawah ini.



3.3 Hasil Identifikasi Kontrol Keamanan

Mengevaluasi tingkat kematangan tingkat kelengkapan pada ISO 27001 data dan gambar, tata kelola kemanan universitas BINA INSAN. Alat evaluasi ini tidak digunakan untuk menganalisis kelayakan atau ektivitas bentuk pengaman yang ada melainkan sebagai perangkat yang untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan infromasi, pengelolaan resiko.

1. **Penilaian Dampak dan Kemungkinan**

   Aktifitas menentukan level resikonya menggunakan metode ISO 27001 antara nilai dampak dan nilai kemungkinan antara aset keamanan kontrol keamanan kerentanan dan penilaian dampak dan kemungkinanya saling berkaitan.

- Data seluruh universitas bina insan ancaman Penyingkapan informasi Kebijakan Kontrol TIK Kurangnya perharian terhadap informasi rahasia sensitif tidak adanya program kesadaran keamanan
- Penyebaran *malware* Kebijakan keamanan TIK Anti virus yang tidak lagi efektif perangkat lunak tidak ter *patch* secara berkala tidak adanya program kesadaran keamanan dan kesalahan pemberian hak akses

2. Penetapan Kontrol Keamanan Dan Sasaranya

Aktifitas ini dilakukan untuk mengurangi lebih jelas beberapa control keamanan untuk memodifikasi resiko *(risk modification)* kebijakan prosedur perangkat lunak atau perangkat keras dan control kdeamanan lainnya sesuaikan dengan panduan ISO 27001 selain itu sasaran keamanan informasi juga diuraikan setiap control keamanan yang ada.

- Pembuatan kebijakan klasifikasi informasi Pembaruan dokumen kebijakan keamanan TIK
- Melakukan sosialisasi terhadap kebijakan dan prosedur tentang keamanan informasi yang ada dan akan diterapkan Menjadwalkan dan melaksanakan program kesadaran keamanan secara berkala detidaknya 6 bulan sekali
- Mendokumentasi klasifikasi kerahasian informasi berdasarkan tingkat publik internal dan rahasia untuk setiap data yang diolah sistem informasi (database) data yang dibuat sistem log backup file konfigurasi id login maupun dokumen yang berbentuk file atau dokumen kertas

IV. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Hasil dari penelitian dapat diberi kesimpulan yang diperoleh setelah dilakukan penguji resiko keamanan aset BINA INSAN yaitu:

1. Berdasarkan hasil penelitian yang disimpulkan dimana hasil analisis kuisoner pada aset hardware terdapat nilai mengalami resiko yang tertinggi untuk diperbaiki terhadap keamanan informasi Membeli lisensi antivirus baru untuk Komputer yang sudah memasuki massa kadarluasa atau menggunakan anti virus yang berisi freeware agar tidak ada masa lisensi lagi Semua prosedur tersedia dan sosialisasikan seluruh karyawan di universitas bina insan yang terkait
2. Mendokumentasi klasifikasi kerahasian informasi berdasarkan tingkat publik internal dan rahasia untuk setiap data yang diolah sistem informasi (database) data yang dibuat sistem log backup file konfigurasi id login maupun dokumen yang berbentuk file atau dokumen kertas
3. Pembuatan kebijakan klasifikasi informasi Pembaruan dokumen kebijakan keamanan TIK

4.2. SARAN

Berdasarkan hasil penelitian,berikut ini adalah saran yang dilakukan oleh penelitian selanjutnya.

1. Penelitian saat ini berfokuspada terjadinya resiko pada sistem keamanan infomasi pada aset yang ada di BINA INSAN diharapkan penelitian selanjutnya melakukan pengukuran mengurangi resiko keamanan pada suatu sistem informasi.
2. Informasi Selanjutnya buat dokumen manual masalah keamanan informasi, prosedur keamanan

DAFTAR PUSTAKA

[1] Antoni, Darius, et al. "Information Technology Governance Profile in E-Government of Palembang." 2018 Third International Conference on Informatics and Computing (ICIC).

[2] Andryani, Ria, Edi Surya Negara, and Dendi Triadi. "Social Media Analytics: Data Utilization of Social Media for Research." Journal of Information Systems and Informatics 1.2 (2019).

[3] Amanda, Riyan, and Edi Surya Negara. "Analysis and Implementation Machine Learning for YouTube Data Classification by Comparing the Performance of Classification Algorithms." Jurnal Online Informatika 5.1 (2020).

[4] Bendi, R. and S. Andayani (2013). "Penerapan Model UTAUT untuk memahami perilaku pengguna Sistem informasi akademik.

[5] Diharja, Anas Akhir, Widya Cholil, and Evi Yulianingsih. "Audit Tata Kelola Sistem Kepegawaian Dinas Tenaga Kerja Dan Transmigrasi Provinsi Sumatera Selatan Dengan Kerangka Cobit Versi 5." Jurnal Mahasiswa Teknik Informatika (2014).

[6] Dewi, N. A. N. and I. G. P. H. Yudana (2016). "Analisa manajemen resiko pada sistem akademik di STIMIK STIKOM Bali,"

[7] Erlika, Yeni, Muhammad Izman Herdiansyah, and A. Haidar Mirza. "Analisis IT Risk Management di Universitas Bina Darma Menggunakan

ISO31000." Jurnal Ilmiah Informatika Global 11.1 (2020).

[8] Ellyusman, S. and R. F. Hutami (2017). "Analisis Kualitas Sistem Informasi Akademik Menggunakan Metode Importance Performance Analysis (ipa)(studi Kasus Pada Website I-gracias Universitas Telkom Bandung).

[9] Ermana, Fine, Haryanto Tanuwijaya, and Ignatius Adrian Mastan. "Audit Keamanan Sistem Informasi Berdasarkan Standar Iso 27001 Pada PT. BPR JATIM." Jurnal Sistem informasi dan Komputer Akuntansi 1.1 (2012).

[10] Fatoni, F., Supratman, E. and Antoni, D., 2017. Pemodelan Sistem Akademik Perguruan Tinggi Swasta Berbasis Teknologi Informasi. Prosiding SNaPP: Sains, Teknologi

[11] Herdiansyah, Muhammad Izman, Suzi Oktavia Kunang, and Muhammad Akbar. "IT strategy alignment in university using IT balanced scorecard framework." Advanced science letters 20.10-11 (2014).

[12] Habibi, R. and I. Firmansyah (2017). "Model penilaian resiko informasi menggunakan ISO 31000`

[13] IMAM, SETIAWAN, Syamsuar Dedy, and Huda Nurul. Meningkatkan Sistem Keamanan Jaringan Proxy Server Menggunakan Squid Proxy Server Di PT. POS Indonesia Kota Palembang. Diss. Universitas Bina Darma, 2019.

[14] Kunang, Yesi Novaria, and Taqrim Ibadi. "Celah Keamanan Sistem Autentikasi Wireless Berbasis RADIUS." Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

[15] LESMANA, A. S. (2018). Perancangan sistem assessment keamanan informasi rumah sakit menggunakan framework ISO 27001

[16] Meilani, Yayuk Ike, Dedy Syamsuar, and Yesi Novaria Kunang. "Assessment Resiko Teknologi Pada Implementasi Sistem Informasi Akademik E-university." Jurnal Bina Komputer 1.1 (2019).

[17] Meilani, Y. I., D. Syamsuar and Y. N. Kunang " Assessment Resiko Teknologi Pada Implementasi Sistem Informasi Akademik E-universitas."

[18] Maryono, Y., S. Suyoto and P. Mudjihartono (2010). "Analisis Dan Perancangan Sistem Informasi Manajemen Aset TIK

[19] Muspa, A. M. and A. Tjahyanto (2010). Perancangan Sistem_Manajemen Sekuritas Informasi (SMSI) Berdasarkan ISO/IEC 27001.

[20] Ritzkal, R., A. Goeritno and A. H. H. Hendrawan (2016). "Implementasi ISO/IEC 27001: 2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik Uika-Bogor." Prosiding Semnastek.

[21] Thaheer, H., S. Hasibuan and F. S. Mumpuni (2010). "Model Resiko Keamanan Pangan Produk Pindang Pada UMKM Pengolahan Ikan Rakyat.

[22] Saputra M, Saputra M, Herdiansyah MI, Herdiansyah MI, Andri A. Perancangan Sistem Basis Data Akademik Pada Smp Negeri 26 Palembang. JURNAL MAHASISWA TI S1. 2013.

[23] Syamsudin, J. R. and S. No "Manajemen Risiko Keamanan Informasi Menggunakan ISO 27005: 2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)

[24] Septriadi, R., F. Firdaus and W. Cholil (2019). "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework Simcobit, Studi Kasus pada Sekolah Tinggi Ilmu Kesehatan Bina Husada Palembang." Jurnal Ilmiah Informatika Global

[25] Salahuddin, S., A. Ambarwati and M. A. A. N. Al Azam (2018). Identifikasi resiko keamanan informasi menggunakan ISO 27005 pada perguruaan tinggi swasta di surabaya

[26] Syafrizal, Melwin. "Sistem Pendukung Keputusan (Decisin Support System)." Data Manajemen dan Teknologi Informasi (DASI) 11.3 (2010):