Analisis Keamanan Informasi Menggunakan Tools

Indeks Kami ISO 4.1

Ade Kornelia & Dedi Irawan

Fakultas Teknik Ilmu Komputer, Universitas Bina Darma

Email: adekornelia1807@gmail.com, dedi.irawan@binadarma.ac.id

Abstract

Information is a very valuable asset for a university institution. Utilization of information technology offers various conveniences in obtaining the information needed. Good information management can make universities have good managerial skills. protecting information security means that it also requires efforts to pay attention to the security factors of all supporting assets such as networks, as well as other facilities that are directly or indirectly related to the process of organizing information. Bina Darma University is an institution that is engaged in the field of education and science, which has a vision that is to become an International Standard University Based on Information Technology By 2025, to realize this there are several efforts prepared, one of which is to improve information security by implementing the ISO 27001 certification process. :2013. So in the context of Bina Darma University will implement ISO 27001: 2013. Using the method of Applied Research (applied research) the author took the initiative to conduct research with the title ANALYSIS OF INFORMATION SECURITY USING OUR INDEX TOOLS 4.1 So as to produce Knowing the maturity level of information security with a status of Inappropriate, Needs improvement , Enough and Good at Bina Darma University.

Keywords : Information Security, WE Index, ISO/IEC 27001:2013, Applied research methods.

1. Pendahuluan

Sejalan dengan zaman yang terus berkembang, kemajuan teknologi informasi sekarang terjadi begitu cepat. Informasi adalah sebuah aset yang begitu berharga untuk sebuah lembaga universitas. Pemanfaatan teknologi informasi tersebut menawarkan beragam kemudahan dalam mendapatkan informasi yang dibutuhkan (Hafasri et al., 2019). Pengelolaan informasi yang baik bisa membuat universitas mempunyai kemampuan manajerial yang baik. melindungi keamanan informasi artinya juga membutuhkan upaya untuk memperhatikan faktor-faktor keamanan dari semua aset penunjang seperti jaringan, serta fasilitas lainnya yang berhubungan langsung ataupun tidak langsung pada proses pengorganisasian informasi. Universitas Bina Darma juga perlu menerapkan keamanan informasi berdasarkan standar kemanan informasi resmi seperti ISO/IEC 27001: 2013 yang merupakan sepaket pedoman serta prosedur yang berhubungan pada keamanan informasi, ISO 27001: 2013 juga menjadi pedoman internasional yang paling banyak di gunakan untuk information security management yang di publikasikan Badan Siber dan Sandi Negara (BSSN)(Riswaya et al., 2020).

Universitas Bina Darma adalah lembaga yang bergerak pada sektor pendidikan dan ilmu pengetahuan, yang berdiri pada tanggal 28 Desember 1993 yang beralamat, Jln. Jenderal Ahmad Yani No. 12 Seberang Ulu Kota Palembang. Visi dari UBD yakni Menjadi sebuah Universitas yang Berstandar Internasional Berbasis Teknologi Informasi di Tahun 2025, guna merealisasikan hal itu ada beberapa upaya yang disiapkan salah satunya yaitu meningkatkan keamanan informasi dengan melaksanakan proses sertifikasi ISO 27001:2013.

Sebelum melakukan sertifikasi ISO 27001 : 2013 Universitas Bina Darma diwajibkan melakukan elvaluasi untuk memenuhi syarat untuk melakukan sertifikasi ISO 27001: 2013 yang telah ditetapkan BSSN, dimana persyaratan tersebut harus melengkapi seluruh klausul dokumen

kelengkapan Indeks KAMI, seperti manajemen resiko keamanan informasi, pengelolaan keamanan informasi, struktur kerja keamanan informasi, manajemen asset keamanan informasi, teknologi keamanan informasi dan pengamanan peranan pihak ketiga penyedia layanannya. Maka dalam rangka Universitas Bina Darma akan melaksanakan ISO 27001: 2013 penulis berinisiatif melakukan “ANALISIS KEAMANAN INFORMASI MENGGUNAKAN TOOLS INDEKS KAMI 4.1” untuk memastikan kesiapan/kematangan Keamanan Informasi di Universitas Bina Darma.

2. Tinjauan Literatur

2.1 Keamanan Informasi

Merupakan sebuah usaha dalam melakukan pengamanan terhadap asset informasi pada berbagai ancaman yang dimungkinkan bisa terjadi. Oleh karenanya keamanan informasi dengan tak langsung bisa menjamin keberlanjutan, menekan seluruh risiko yang terjadi serta memaksimalkan *return* dari nilai investasinya. makin banyaknya informasi yang perusahaan simpan, diorganisir serta dibagikan artinya makin tinggi juga risiko adanya kerusakan, kehilangan maupun terpublikasikannya data ke pihak eksternal yang kurang dikehendaki (Pamungkas & Saputra, 2020).

Keamanan informasi adalah sebuah upaya dalam melindungi informasi lewat berbagai tipe media misalny komputer, mesin fax beserta sarana penunjang penyimpanan data serta informasi misalnya media dokumen yang sudah dicetak dari penyimpangan individu yang tidak memiliki hak untuk mengaksesnya (Hartati, 2017). Keamanan informasi berhubungan terhadap perlindungan aset berharga dari risiko kehilangan, pempublikasian penyalahgunaan, maupun kerusakan (Putra et al., 2016).

Keamanan informasi adalah aspek utama pada upaya menjaga aset informasi pada suatu organisasi. tipe keamanan informasi bisa dikelompokkan dalam sejumlah komponen berikut ini (Basyarahil, 2017):

1. *Physical security*: keamanan yang berfokus pada strategi dalam mengamankan tenaga kerja maupun anggota organisasi, aset fisik, serta lokasi kerja dari sejumlah marabahaya yaitu resiko kebakaran, akses tanpa otorisasi, serta bencana alam.
2. *Personal security*: keamanan yang overlap dari *physical security* untuk memberikan perlindungan terhadap individu pada sebuah perusahaan pada sebuah organisasi.
3. *Operational security*: keamanan yang berfokus pada strategi dalam mengamankan kekuatan perusahaan agar tidak ada hambatan saat bekerja.
4. *Communications security*: keamanan dengan tujuan melindungi media komunikasi, teknologi komunikasi dan isinya, serta kecakapan dalam menggunakan alat tersebut agar meraih tujuan suatu perusahaan.
5. *Network security*: keamanan yang berfokus terhadap perlindungan alat jaringan serta organisasi, jaringan serta isinya, dan kecakapan dalam memakai jaringan itu untuk memenuhi fungsi komunikasi data organisasi itu.

2.2 Sistem Manajemen Keamanan Informasi (SMKI)

Suatu perusahaan wajib mengaplikasikan SMKI dalam menjamin keamanan asset TIK. Sistem Manajemen Keamanan Informasi ialah himpunan dari kebijakan serta tahapan

dalam mengelola data sensitif organisasi dengan sistematis. SMKI bertujuan dalam mengecilkan risiko serta menjamin keberlangsungan bisnis dengan proaktif dalam membatasi pengaruh dari penyalahan keamanan.

SMKI pun wajib merujuk terhadap standar nasional maupun internasional yang terdapat supaya mutu pengamanan yang diberikan semakin tinggi bisa mengatasi ketika terdapat masalah. Standar internasional yang sudah disarankan dalam penggunaan SMKI yaitu ISO/IEC 27001:2013. Standar tersebut sudah berjalan dengan basis risiko jadi bisa menekan bahaya serta mengatasi masalah secara cepat serta akurat (Basyarahil, 2017).

SMKI begitu penting untuk mengelola informasi yang ada pada sebuah perusahaan. Keamanan informasi digunakan dalam memelihara aspek kerahasiaan, keutuhan, serta ketersediaan dari informasi (Wati et al., 2019).

2.3 ISO/IEC 27001:2013

ISO 27001:2013 ialah suatu standar yang dikeluarkan oleh International Organization for Standardization. ISO 27001:2013 adalah pedoman yang digunakan dalam menunjang perusahaan untuk menjaga keamanan aset perusahaan serta dalam menjaga SMKI. Standar dirancang secara khusus dalam menyiapkan persyaratan pada penetapan, pengaplikasian, perawatan serta perbaikan yang berkesinambungan pada SMKI (Apriandari & Sasongko, 2018).

SMKI adalah suatu pendekatan yang sifatnya sistematis dengan tujuan dalam melakukan pengelolaan terhadap informasi penting ataupun informasi perusahaan yang sifatnya sangat sensitif supaya selalu terjadi keamanannya. SMKI pun memberi acuan dalam mengelola unsur yang menjadi bagian untuk menjalankan pengorganisasian informasi yang penting misalnya manusia, proses serta mekanisme Teknologi Informasi melalui penerapan proses manajemen resiko yang sudah berdasarkan standar.

ISO 27001:2013 sudah disusun jadi bisa diselaraskan terhadap penggunaannya dalam organisasi kecil, menengah sampai organisasi besar di seluruh bidang sebagai upaya menjaga aset informasi penting organisasi itu (Basyarahil, 2017).

Berbagai manfaat standar ISO 27001, antara lain:

1. Memberi suatu kepercayaan serta jaminan pada klien maupun relasi dagang, bila perusahaan Anda sudah memiliki SMKI yang baik menurut standar internasional. disamping itu, ISO 27001 bisa pula dipakai dalam marketing perusahaan.
2. Memastikan bila organisasi Anda mempunyai pengendalian mengenai keamanan informasi pada lingkungan proses usahanya yang bisa mencipatakan bahaya maupun hambatan.
3. ISO 27001 mengharuskan Anda agar selalu menaikkan keamanan informasi perusahaan Anda. Hal itu menolong Anda agar semakin menetapkan total keamanan yang sesuai yang diperlukan perusahaan. Sumber daya yang dipakai pas sesuai dengan kebutuhannya.

Indeks Keamanan Informasi (KAMI)

Merupakan instrumen evaluasi dalam melakukan analisis taraf kesiapan perlindungan informasi di suatu perusahaan (Septanto, 2020). Alat evaluasi itu tidak dipergunakan dalam menganalisa kelayakan maupun efektifitas sebagai wujud pengamanan yang

tersedia, tetapi menjadi perangkat dalam memberi petunjuk situasi kesiapan struktur kerja keamanan informasi pada pimpinan lembaga (Wijatmoko, 2020). Evaluasi dijalankan pada beragam kawasan yang merupakan sasaran pengaplikasian keamanan informasi dalam ruang lingkup pembahasannya sesuai pada seluruh aspek keamanan yang dipaparkan standar ISO atau IEC 27001: 2013 (Husin et al., 2017).

Dokumen Kelengkapan Indeks KAMI:

1. Manajemen Resiko Keamanan Informasi
2. Pengelolaan Keamanan Informasi
3. Struktur Kerja Keamanan Informasi
4. Rekaman/Bukti yang harus disediakan
5. Pengorganisasian asset keamanan informasi
6. Teknologi keamanan informasi
7. Perlindungan peran serta eksternal yang menyediakan layanan
8. Perlindungan layanan infrastruktur awan.
9. Pengamanan Data Pribadi

3. Metode Penelitian

Metodenya menggunakan penelitian terapan. Disini penulis menggunakan pendekatan kualitatif. Jenis Penelitian ini masuk pada rancangan penelitian deskriptif. karena pada penelitian ini dijalankan audit keamanan informasi yang mengaplikasikan instrument atau indikator pada teori SNI ISO/IEC 27001: 2009. Penelitian ini pun memuat berbagai kutipan dari data ataupun fakta yang ditemukan dilapangan yang dipaparkan semakin lengkap(Komalasari & Perdana, 2009).

3.1 Tahapan Penelitian

Penelitian ini terdiri dari lima tahapan yaitu :

1. Tahap Identifikasi

Langkah pertama yang dilaksanakan adalah mengidentifikasi masalah dengan menyusun rumusan masalah dan menentukan tujuan dari diadakannya penelitian. Kemudian membuat izin penelitian objek penelitian yang ditentukan. Penelitian literatur memakai berbagai teori yang berkaitan dengan keamanan informasi menggunakan tools indeks KAMI 4.1, misalnya saja buku Manajemen Keamanan Informasi, panduan penerapan pengelolaan keamanan informasi dan serta penelitian yang relevan.

2. Tahap perancangan

Kemudian merancang lingkup analisis menyesuaikan keadaan yang sudah ada di Universitas Bina Darma, supaya rekomendasinya bisa diterima serta sesuai dengan usaha yang dijalankan.

3. Tahap Pengumpulan Data.

Sebelum melakukan ceklist, di buat work paper berisikan susunan pertanyaan ceklist menyesuaikan ruang lingkup yang sudah ditetapkan. Selanjutnya ceklist keamanan informasi dilaksanakan dengan Indeks KAMI Versi 4.1 mempergunakan berbagai teknik pengumpulan data diantaranya wawancara dan pengamatan

4. Tahap Analisa dan Rekomendasi

Kemudian menganalisis datanya menggunakan grafik Maturity Level untuk melihat tingkat kematang kemandirian informasi Universitas Bina Darma yang mengacu pada standar ISO 27001:2013. Dimulai dengan mereduksi hasil wawancara dan observasi kedalam catatan lapangan dan memberikan rekomendasi kebijakan yang berstandar ISO 27001: 3013.

5. Tahap Kesimpulan dan Saran

Tahapan ini menjadi tahapan yang paling akhir.

3.2 Metode Pengumpulan Data

Berikut metode yang dipakai untuk mengumpulkan data penelitian ini, yakni:

1. Observasi

Teknik mengumpulkan data menggunakan cara melihat serta mengamati secara langsung agar memperoleh informasi yang diperlukan (Oleh & Octariza, 2019), sehingga informasi dapat diperoleh dengan benar – benar akurat.

2. Wawancara

Pada teknik ini penulis menghimpun data penelitian melalui bertanya secara langsung pada pihak yang terkait yang bisa member informasi yang diperlukan (Hadinata & Udariansyah, 2015).

4. Hasil dan Pembahasan

Pada tahapan analisa penulis menggunakan metode analisisnya mengacu dengan penerapan Indek KAMI lampiran Panduan Penerapan Pengelolaan Keamanan Informasi bagi Penyelenggara Layanan Publik. Hasil penjumlahannya setiap area ditampilkan dalam tabel berikut:

- a) Tabel Nilai Setiap Area, Tabel ini berisi total mean skor untuk masing-masing area evaluasi.

Area	Skor
Tata Kelola Keamanan Informasi	95
Pengelolaan Risiko Keamanan Informasi	50
Kerangka Kerja Kemandirian Informasi	47
Pengelolaan Aset Informasi	91
Teknologi dan Kemandirian Informasi	86
Total	369

Gambar 4.1 Tabel Total rata-rata skor untuk tiap area Universitas Bina Darma

- b) Diagram Radar dengan 5 sumbu sesuai area pengamanan.

Maksud dari diagram tersebut adalah untuk mengilustrasikan korelasi antara ketaatan dengan standarnya yang ada, status penggunaan, struktur kerja dasar, dan skor dari setiap area.

Berikut diagram radar yang dihasilkan sesuai dengan area pengamanan yang ada di Universitas Bina Dharma :

Gambar 4.2 Diagram Radar Hasil Penilaian SMKI

Dalam diagram tersebut, warna orange adalah kondisi SMKI Universitas Bina Dharma. Dari kelima area keamanan informasi, dapat disimpulkan jika :

- 1) Dari kelima area keamanan informasi tersebut, terlihat jika Universitas Bina Dharma sudah mempunyai Pengelolaan Keamanan Informasi yang semakin baik dibandingkan dengan area keamanannya yang lain
- 2) Selain area aspek Tata Kelola Keamanan Informasi, Universitas Bina Dharma telah memenuhi setidaknya Tata kelola Asset Informasi dan Teknologi Keamanan Informasi yang baik dalam pengelolaan Keamanan Informasi.
- 3) Kecuali 3 (Tiga) aspek diatas, Universitas Bina Dharma sudah sesuai memenuhi paling tidak Kerja Dasar dalam Pengelolaan Keamanan Informasi.
- 4) Hasil Status Kesiapan ataupun Kelengkapan bisa disajikan dengan instrument Bar Chart misalnya yang ditampilkan dalam gambar berikut, pencapaiannya yang masih terdapat di warna merah menandakan masih berstatus “Tidak Layak”, selanjutnya pencapaiannya yang berwarna kuning masih “Memerlukan Perbaikan”, dan yang berwarna hijau memperlihatkan jika statusnya sudah “Baik/Cukup”.

Gambar 4.3 Hasil Status Kesiapan atau Kelengkapan

Pembahasan

1. Tingkat Kematangan terdapat pada posisi III yang artinya Taraf Kematangan Mencapai minimum
 - a) Ketentuan Dasar TKII+;
 - b) Semua bentuk perlindungan TKIII-Tahap 1 statusnya “Diterapkan Secara Menyeluruh”;
 - c) 2 bentuk perlindungan TKIII-Tahap 2 statusnya “Dalam Penerapan/Diterapkan Sebagian”;
 - d) Sisa jumlah perlindungan TKIII-Tahap 2 yang ada statusnya “Diterapkan Secara Menyeluruh”;
 - e) 2 bentuk perlindungan TKIII-Tahap 3 statusnya “Dalam Penerapan/Diterapkan Sebagian.”
2. Peran/Tingkat Kepentingan system elektronik di Universitas Bina Darma sudah masuk dalam kategori tingkat Tinggi (Skor: 25).
3. sedangkan dari kelengkapan penerapan SMK, Universitas Bina Darma masuk dalam kategori “Cukup Baik”, warna “Kuning” mendapatkan skor 369, yang sebagai jumlah dari semua nilai mean di masing-masing tingkat keamanan informasi yang dievaluasi.

Setelah melakukan Analisa pada tools Indeks KAMI, dapat dilihat bahwa Universitas Bina Darma Belum melengkapi sebagian dokumen kelengkapan indeks KAMI, karena masih ada bagian evaluasi yang berstatus Dalam Perencanaan, sehingga hal ini menjadi bagian masalah Universitas Bina Darma sebelum melaksanakan sertifikasi ISO 27001: 2013. Hasil dari analisis menunjukan beberapa bagian evaluasi yang belum bisa dipenuhi berdasar pada setiap tingkat Indeks KAMI. Bagian evaluasi yang belum bisa dipenuhi tersebut akan menjadi dasar dalam membuat rekomendasi (Pratama, 2018).

5. Kesimpulan

Dari hasil penelitian yang sudah dilakukan tersebut bisa ditarik kesimpulan jika rentang tingkat Kelengkapan dan kematangan Keamanan informasi di Universitas Bina Darma saat ini masih ada dalam posisi TK II+ atau telah mencapai tingkat kematangan III yang dimana masih berstatus “Cukup Baik” untuk melaksanakan sertifikasi ISO/IEC 27001: 2013. Universitas Bina Darma diberikan rekomendasi untuk dilaksanakan pada keamanan informasi supaya bisa disebut layak dalam melaksanakan sertifikasi ISO-27001:2013 dan juga bisa mengamankan semua informasi yang sebuah instansi kelola.

Referensi

- Afrianto, I., Suryana, T., & Sufa'atin, S. (2015). Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009. *Jurnal ULTIMA InfoSys*, 6(1), 43–49. <https://doi.org/10.31937/si.v6i1.278>
- Antoni, D., & Akbar, M. (2019). E-supply chain management value concept for the palm oil industry. *Jurnal Sistem Informasi*, 15(2), 15-29.
- Antoni, D., Fikari, D., & Akbar, M. (2018). The readiness of palm oil industry in

enterprise resource planning. *Telkomnika*, 16(6), 2692-2702.

Antoni, D., Herdiansyah, M. I., Akbar, M., & Sumitro, A. (2021). Pengembangan Infrastruktur Jaringan Untuk Meningkatkan Pelayanan Publik di Kota Palembang. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 5(4), 1652-1659.

Antoni, D., Jie, F., & Abareshi, A. (2020). Critical factors in information technology capability for enhancing firm's environmental performance: case of Indonesian ICT sector. *International Journal of Agile Systems and Management*, 13(2), 159-181.

Apriandari, W., & Sasongko, A. (2018). Analisis sistem manajemen keamanan informasi menggunakan SNI ISO/IEC 27001:2013 pada pemerintahan daerah kota Sukabumi (Studi kasus: DI Diakominfo Kota Sukabumi). 8(1), 15.

Basyarahil, F. A. (2017). Security management using indeks keamanan informasi (KAMI) based on ISO/IEC 27001:2013 at direktorat pengembangan teknologi dan sistem informasi (DPTSI) ITS Surabaya. 393.

Fauzi, F., Dencik, A. B., & Asiati, D. I. (2019). Metodologi Penelitian untuk manajemen dan akuntansi. *Jakarta: Salemba Empat*.

Hadinata, N., & Udariansyah, D. (2015). Implmentasi metode web engineering dalam perancangan sistem informasi penerimaan mahasiswa baru dan tes online. 12.

Hafasri, J., Irfani, M. H., & Nopriani, F. (2019). Analisis Pengukuran Kualitas Penggunaan Sistem Informasi Akademik (Studi Kasus Sistem Informasi Akademik STIQ Al-Lathifiyyah Palembang). *JUSIFO*, 5(2), 81-90. <https://doi.org/10.19109/jusifo.v5i2.5190>

Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001: 2013. *KOPERTIP : Jurnal Ilmiah Manajemen Informatika dan Komputer*, 1(2), 63-70. <https://doi.org/10.32485/kopertip.v1i02.24>

Husin, M. F., Wowor, H. F., & Karouw, S. D. S. (2017). Implementasi Indeks KAMI di Universitas Sam Ratulangi. 12, 8.

Komalasari, R., & Perdana, I. (2009). Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001: 2009. *Jurnal Sistem Informasi*, 9(2), 16.

Oleh, D., & Octariza, N. F. (2019). Skripsi analisis sistem manajemen keamanan informasi menggunakan standar ISO/IEC 27001 dan ISO/IEC 27002 pada kantor pusat PT Jasa Marga. 320.

Pamungkas, W. C., & Saputra, F. T. (2020). Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013. *Jurnal Sistem Komputer dan Informatika (JSON)*, 1(2), 101. <https://doi.org/10.30865/json.v1i2.1924>

Pratama, E. R. (2018). Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur). 10.

Putra, A. A., Nurhayati, O. D., & Windasari, I. P. (2016). 3huhqfdqddq gdq, psophqwdvl, qirupdwlrq 6hfxulw\ 0dqdjhpqhqw 6\vwph 0hqjjxqdndq) udphzrun,62 ,(& Jurnal Teknologi dan Sistem Komputer, 7.

Riswaya, A. R., Sasongko, A., & Maulana, A. (2020). Evaluasi tata kelola keamanan teknologi keamanan informasi menggunakan indeks KAMI untuk persiapan standar SNI ISO/IEC 27001 (Studi kasus: STMIK Mardira Indonesia). 9.

Septanto, H. (2020). Penilaian Tata Kelola Elearning Kelas Shift Dengan Menggunakan Kriteria Standar Indeks KAMI Di STMIK Bina Insani Bekasi. 6.

Wati, D. A., Budiono, A., & Fauzi, R. (2019). Analisis dan perancangan manajemen keamanan informasi pada direktorat sistem informasi Universitas Telkom dengan indeks keamanan informasi (KAMI) pada area tata kelola keamanan informasi, pengelolaan risiko keamanan informasi dan kerangka kerja pengelolaan kemanan informasi. 9.

Wijatmoko, T. E. (2020). Evaluasi keamanan informasi. 6.

Yustanti, W., Bisma, R., Qoiriah, A., & Prihanto, A. (2018). Analisis tingkat kesiapan dan kematangan implementasi ISO 27001:2013 menggunakan indeks keamanan informasi 3:2015 Pada UPT. PPTI Universitas Negeri

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>)