ISSN: 2614-8404

Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ

Titus Kristanto[1*)], Mohammad Sholik[2], Dewi Rahmawati[3], Muhammad Nasrullah[4]
[1,2,3]Program Studi Rekayasa Perangkat Lunak, Fakultas Teknologi Informasi dan Industri, Institut Teknologi Telkom Surabaya
[4]Program Studi Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi, Institut Teknologi Sepuluh Nopember
email: [1] tintus.chris@gmail.com, [2]sholih.archive@gmail.com, [3]dewirahmaw4ti@gmail.com, [4]em.nashrul@gmail.com

Abstrak **Manajemen keamanan informasi sangat penting untuk digunakan, terutama bagi instansi pendidikan, dikarenakan mampu mengurangi resiko ancaman terhadap penggunaan teknologi informasi bagi organisasi pendidikan. Manajemen keamanan informasi sangat diperlukan sebagai upaya untuk meminimalkan resiko dalam meningkatnya ancaman data dan informasi. Pelaksanaan manajemen keamanan informasi dimaksudkan untuk mengetahui masalah teknis dan masalah non teknis. Penelitian ini menggunakan standard ISO 27001:2005, dikarenakan standard ISO 27001:2005 dapat menyesuaikan dengan instrumen penelitian pada kebutuhan organisasi yang dikembangkan dan fokus pada manajemen keamanan informasi. Hasil penelitian menggunakan standard ISO 27001:2005 adalah dapat mengurangi resiko tingkat keamanan, dan dapat melakukan evaluasi secara berkesinambungan, serta meningkatkan control keamanan yang direkomendasikan pada institusi XYZ.**
Kata Kunci **– Standard ISO 27001:2005, Manajemen Keamanan Informasi, IT Support.**

Abstract – Information security management is very important to use, especially for educational instutions, because it is able to reduce the risk of threats to the use of information technology for educational organizations. Information security management is indispensable as an effort to minimize the risk of data enhancement and information threats. Implementation of information security management is intended to know technical problems and non-technical problems. The research uses the ISO 27001:2005 standard, as the ISO 27001:2005 standard can adapt to research instruments on the needs of the developed organization and focus on information management. The results of the research using the ISO 27001:2005 standard are able to reduce the risk of security level, and can evaluate continuously, and improve the security control recommended by XYZ institutions.
Keywords – ISO 27001:2005 Standard, Information Security Management, IT Support.

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era industry 4.0 semakin pesat, sehingga resiko keamanan informasi semakin besar [1]. Pencapaian tujuan bisnis dari organisasi instansi pendidikan diperlukan teknologi informasi yang tepat pada pengelolaan data informasi untuk menciptakan layanan yang berkualitas pada proses bisnis [2]. Aset informasi yang lemah, membuat pihak yang tidak berkepentingan untuk mengganggu aktivitas yang berkaitan dengan asset instansi pendidikan. Maka, dibutuhkan keamanan informasi yang mampu mencegah resiko yang timbul dari asset informasi insntansi pendidikan.

Keamanan informasi merupakan asset yang sangat penting bagi organisasi instansi pendidikan, termasuk kepercayaan dan kualitas layanan masyarakat [3]. Seringkali, masalah keamanan informasi kurang mendapatkan perhatian dari pimpinan dan manajemen organisasi instansi pendidikan, khususnya pengelola IT support. Suatu kenyataan, di era industry 4.0 organisasi instansi pendidikan dihadapkan dari sejumlah ancaman keamanan informasi dari berbagai sumber. Permasalahan keamanan informasi mendapatkan perhatian serius jikalau sudah terjadi ancaman yang menimbulkan kerugian bagi instansi pendidikan [4]. Berbagai ancaman diantaranya adalah serangan virus dan malware [5].

Malware merupakan sebuah perangkat lunak yang dibuat berdasarkan aktivitas yang berbahaya atau merusak perangkat lunak, seperti Spyware, Trojan, dan Virus [6]. Virus computer bekerja dengan cara menempel pada *file* yang berada di computer, berupa *file executable*, sedangkan Trojan bekerja dengan *social engineering files* yang berbahaya [7]. Jika ancaman informasi tidak segera dicegah, maka berakibat fatal kehilangan data, sehingga aktivitas proses bisnis instansi pendidikan dapat terganggu dalam sementara waktu [8]. Untuk mencegah kehilangan data, diperlukan audit keamanan informasi sesuai dengan prosedur yang berlaku [9].

Standar yang digunakan dalam penelitian adalah standar ISO 27001:2005 [10]. Dikarenakan standar ISO 27001:2005 merupakan standar yang mudah digunakan sesuai dengan kebutuhan organisasi, tujuan organisasi, proses bisnis, dan jumlah pegawai dari struktur organisasi pendidikan [11]. Pada standar ISO 27001:2005 menyediakan berbagai rekomendasi manajemen keamanan informasi dan layanan IT [12], serta menyediakan sertifikasi Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar internasional [13].

Berdasarkan hasil wawancara dan studi lapangan di instasi pendidikan, maka klausul dari SMKI yang digunakan adalah Klausul 5 (Kebijakan Keamanan Informasi), Klausul 8 (Keamanan Sumber Daya Manusia), Klausul 9 (Keamanan Fisik dan Lingkungan), Klausul 12

ISSN: 2614-8404

(Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi), dan Klausul 13 (Manajemen Penanganan Keamanan Informasi). Hasil dari audit keamanan informasi adalah dapat meningkatkan keamanan informasi dan menurunkan resiko keamanan informasi [14].

II. TINJAUAN PUSTAKA

A. *Penelitian Terkait*

Pada penelitian pertama *"Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información (Implementation of an information security management system under ISO 27001: information risk analysis)"* dari Jurnal *Tecnura vol 19 no 46 2015 pp123-133,* menjelaskan bahwa struktur bisnis dari Kota Ocaña ada di sektor komersial, dikarenakan 71% secara geografis di daerah komersial, terletak di pusat kota [15]. Sebagian besar perusahaan milik keluarga, sehingga mempunyai proporsi yang tinggi dan dikelola oleh keluarga, baik dari segi kepemilikan perusahaan dan jenis manajemen bisnis.

Bisnis di Ocaña diatomisasi dengan Microenterprise yang menjadi dasar dalam menciptakan kekayaan dan pekerjaan. Akun UKM di sector menengah 3%, sedangkan akun UKM di sector teknologi rendah 1%. Maka, perlu kebijakan organisasi untuk menggabungkan ke system manajemen keamanan informasi.

Hasil yang diperoleh dari kelemahan bisnis di Kota Ocaña adalah untuk mengidentfikasi dari kegiatan merancang ruang pelatihan, akuisisi kemampuan dan praktik manajemen pengusaha berupa tantangan dan daya saing yang ada di pasar.

Pada penelitian kedua dengan judul *"Расчет рисков информационной безопасности телекоммуникационного предприятия (Calculation of information security risks of a telecommunication enterprise)* dari Jurnal : *Cyber Leninka vol 22 no 2 2018 pp61-70,* menjelaskan bahwa cara mengidentifikasi dan menilai resiko keamanan informasi dalam tiga bidang yang dikendalikan [16]. Penekanan utama pada penerapan keamanan informasi yang dilakukan untuk meminimalkan kerusakan dari ancaman keamanan yang ditujukan pada integritas dan ketersediaan perangkat keras dan perangkat lunak, serta menjaga kerahasiaan sumber informasi yang diproses dengan bantuan.

Studi memeriksa dari standar internasional dan nasional di bidang keamanan informasi yang mengatur masalah manajemen resiko keamanan informasi. Secara khusus, penilaian dan pemrosesan resiko keamanan informasi berdasarkan standar internasional ISO 27001:2013 tentang metode perlindungan. Metode utama untuk penilaian resiko dan pemrosesan paling ekonomis adalah sejumlah serangan yang diimplementasikan dalam jangka waktu tertentu.

B. *Tinjauan Pustaka*

1. *Keamanan Informasi*

Keamanan informasi berkaitan dengan melindungi asset informasi terhadap kehilangan atau kerusakan data untuk menjamin kelangsungan bisnis *(business continuity)* dan meminimalkan resiko bisnis *(reduce business risk)* [14]. Keamanan informasi bisa dicapai dengan beberapa strategi yang bisa dilakukan berupa kombinasi satu dengan yang lain dan mempunyai focus masing-masing dalam strategi sesuai dengan kebutuhan [13].

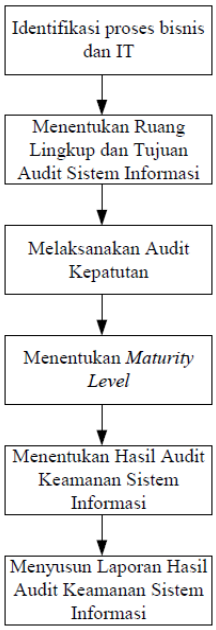
2. *Standar ISO 27001:2005*

ISO 27001:2005 merupakan standar keamanan informasi berupa persyaratan yang harus dilakukan dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) [14].Standar ISO 27001:2005 bersifat independen terhadap produk dari teknologi informasi dan dirancang untuk melindungi asset informasi dari berbagai ancaman atau resiko dari pihak yang tidak bertanggungjawab [1].

ISO 27001:2005 mendefinisikan 133 kontrol keamanan yang terstruktur dan membagi menjadi 11 klausul control keamanan, 39 obyektif control dan 133 kontrol keamanan [13]. Pengelompokkan control keamanan sangat diperlukan untuk memudahkan organisasi instansi pendidikan dalam mengontrol keamanan yang dibutuhkan baik secara manajemen, operasional, maupun teknikal [14].

III. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam melaksanakan audit keamanan informasi, dapat dilihat pada Gambar 1.



Gambar. 1 Metode Penelitian

A. *Pengumpulan Data*

Ada beberapa teknik atau cara pengumpulan data yang digunakan dalam penelitian yaitu [17] :

a. Wawancara
   Tim peneliti melakukan wawancara secara langsung dengan Staff IT Support instansi pendidikan.
b. Studi Lapangan
   Tim peneliti melakukan studi lapangan berupa pengamatan dan kunjungan langsung ke instansi pendidikan.
c. Studi Literatur
   Studi literature yang dilakukan tim peneliti berupa pencarian literature atau referensi dari buku, jurnal, dan prosiding yang terkait dengan ISO 27001:2005.

B. *Identifikasi Proses Bisnis dan IT*

Pada perencanaan audit keamanan informasi, tim

ISSN: 2614-8404

peneliti harus memahami proses bisnis dan IT yang ada di instansi pendidikan. Pemahaman yang harus dipelajari oleh tim peneliti adalah mempelajari dokumen yang berhubungan dengan data instansi pendidikan yaitu profil instansi, visi dan misi instansi, struktur organisasi instansi, serta proses dan bisnis IT instansi pendidikan. Tim peneliti harus mengetahui apakah instansi pendidikan tersebut sudah melakukan proses audit atau belum [18].

C. *Menentukan Ruang Lingkup dan Tujuan Audit Sistem Informasi*

Pada ruang lingkup yang dilakukan dalam penelitian dengan melakukan wawancara dengan Staff IT Support, studi lapangan, dan studi literature. Hasil dari wawancara dengan Staff IT Support adalah terdapat kekurangan dan kelemahan pada keamanan asset, informasi, dan akses dari aplikasi. Penerapan hasil dari ruang lingkup menggunakan standard ISO 27001:2005, termasuk klausul-klausul yang digunakan pada standard ISO 27001:2005. Pada Tabel 1 merupakan pemetaan dari klausul ISO 27001:2005 berdasarkan hasil wawancara dengan Staff IT Support.

Tabel I. Pemetaan Klausul ISO 27001:2005

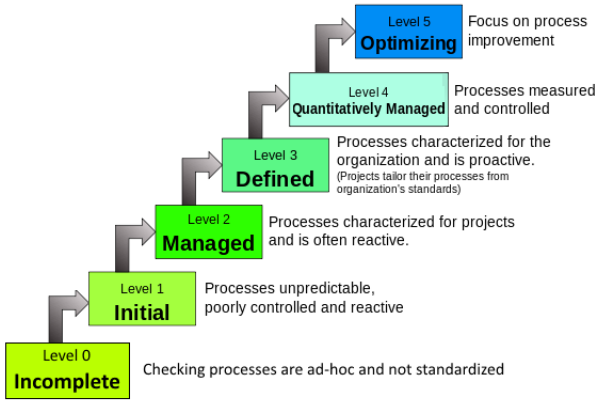
Klausul	Deskripsi
5	Kebijakan Keamanan Informasi
8	Keamanan Sumber Daya Manusia
9	Keamanan Fisik dan Lingkungan
12	Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi
13	Manajemen Penanganan Insiden Keamanan Informasi

D. *Melaksanakan Audit Kepatutan*

Pada pelaksanaan audit kepatutan menghasilkan dokumen wawancara dengan Staff IT Support, bukti audit, temuan audit, dan tingkat nilai kematangan dari control keamanan. Dari semua bukti yang ada, tahap selanjutnya melakukan analisis dan evaluasi hasil nilai tingkat kemampuan dari tiap control keamanan informasi.

E. *Menentukan Maturity Level*

Dari hasil penentuan nilai yang ditetapkan, tahap berikutnya adalah membuat *Maturity Level.* Pada pengelolaan dan pengendalian *maturity level* berdasarkan pada metode evaluasi organisasi sehingga dapat dievaluasi dari level 0 (tidak ada) hingga level 5 (optimistis) [14]. Pada Gambar 2 merupakan urutan tingkatan *maturity level* keamanan informasi.



Gambar. 2 Urutan Tingkatan *Maturity Level*

Jika dikelompokkan berdasarkan nilai dari level keamanan, dapat dilihat pada Tabel 2.

Tabel II. Level Kenatangan *(Maturity Level)*

Indeks Kematangan	Level Kematangan
0.00 – 0.49	0 *Incomplete*
0.50 – 1.49	1 *Initial*
1.50 – 2.49	2 *Managed*
2.50 – 3.49	3 *Defined*
3.50 – 4.49	4 *Quantitatively Managed*
4.50 – 5.00	5 *Optimized*

Pada penelitian menggunakan pendekatan kuantitatif. Data yang diperoleh berasal dari hasil penyebaran kuesioner dari responden. Responden berasal dari Staff IT Support instansi pendidikan dengan jumlah 5 orang.

IV. HASIL DAN PEMBAHASAN

Standar ISO 27001:2005 yang digunakan adalah bagian Kontrol Keamanan *(Security Control)* yang terdiri dari 39 obyektif control dan 133 kontrol keamanan. Untuk mengetahui control-kontrol yang lemah, maka manajemen instansi pendidikan mengambil tindakan untuk memperbaiki control-kontrol yang butuh penanganan.

Nilai *maturity level* didapatkan dari hasil rata-rata jawaban responden yang terdapat pada klausul ISO 27001:2005. Pada Tabel 3 merupakan hasil dari perhitungan kuesioner untuk mendapatkan tingkat kematangan keamanan informasi.

Tabel III. Level Kenatangan *(Maturity Level)*

Klausul	Proses	Nilai	Level
5	Kebijakan Keamanan Informasi	2,31	2
8	Keamanan Sumber Daya Manusia	2,52	3
9	Keamanan Fisik dan Lingkungan	2,03	2
12	Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi	2,19	2
13	Manajemen Penanganan Insiden Keamanan Informasi	2,27	2
Rata-Rata		**2,264**	**2**

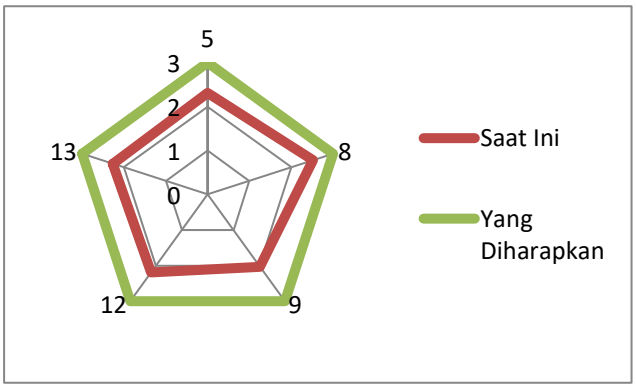
Berdasarkan hasil dari *maturity level* penyebaran kuesioner kepada responden, kemudian dihitung nilai kesenjangan antara *maturity level* saat ini dengan *maturity level* yang diinginkan. Pada Tabel 4 merupakan nilai kesenjangan keamanan informasi pada bagian IT Support instansi pendidikan.

Tabel IV. Nilai Kesenjangan dari Keamaanan Informasi

Klausul	Tingkat Kematangan		Nilai Kesenjangan
	Saat Ini	Yang Diharapkan	
5	2,31	3,00	0,69
8	2,52	3,00	0,48
9	2,03	3,00	0,97
12	2,19	3,00	0,81
13	2,27	3,00	0,73

Pada Gambar 3, merupakan grafik dari perbandingan nilai *maturity level* saat ini dengan nilai *maturity level* yang diharapkan.

ISSN: 2614-8404



Gambar. 3 Perbandingan Nilai*Maturity Level* saat ini dan Nilai *Maturity Level* yang diharapkan

Berdasarkan hasil perhitungan *maturity level* keamanan informasi, tingkat keamanan informasi yang sebagai pedoman berada di Level 3 *(Defined Process)*. Berdasarkan hasil perhitungan *maturity level* yang sudah dilakukan, maka tingkat kematangan keamanan informasi pada bagian IT Support instansi pendidikan rata-rata berada di Level 2 *(Managed Process)*. Berarti keamanan informasi pada instansi pendidikan perlu adanya perbaikan dan perlu dikembangkan pada tahap selanjutnya yang lebih baik, dikarenakan masih berada di Level 2 *(Managed Process)*.

V. PENUTUP

Berdasarkan hasil penelitian yang sudah dilakukan menggunakan ISO 27001:2005, dapat disimpulkan yaitu :

1. Tingkat kematangan *maturity level* keamanan informasi pada bagian IT Support instansi pendidikan rata-rata berada di Level 2 *(Managed Process)* untuk klausul Kebijakan Keamanan Informasi; Keamanan Fisik dan Lingkungan; Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi; Manajemen Penanganan Insiden Keamanan Informasi. Sedangkan klausul Keamanan Sumber Daya Manusia berada di Level 3 *(Defined Process)*.
2. Penerapan dari standarisasi keamanan informasi pada bagian IT Support instansi pedidikan berdasarkan kebutuhan operasional dan teknikal.
3. Responden berasal dari bagian Staff IT Support instansi pendidikan.

DAFTAR PUSTAKA

[1] Kristanto T, Arief R and Rozi N F 2014 Perancangan Audit Keamanan Informasi Berdasarkan Standar ISO 27001:2005 (Studi Kasus : PT Adira Dinamika Multi Finance) *Seminar Nasional Sistem Informasi Infonesia (SESINDO) 2014*

[2] Sidik M, Ade Iriani and Sri Yulianto 2018 Audit Manajemen Keamanan Teknologi Informasi Menggunakan Standar ISO 27001:2005 Di Perguruan Tinggi XYZ *Sitech J. Sist. Inf. dan Teknol.* **1** 1–6

[3] Sulistiyowati N 2015 Evaluasi Keamanan Informasi Berbasis ISO 27001 Pada Dinas Pengelolaan Pendapatan Keuangan Dan Aset Daerah Kabupaten Karawang *Syntax J. Inform.* **4**

[4] Chazar C 2015 Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005 *J. Inf.* **VII** 48–57

[5] Anom Suseyto Aji Nugroho H, Winarno W W and Sudarmawan 2018 Metode Silogisme AND Untuk Validitas Jawaban Dari Responden Dalam Analisis Maturity Level Keamanan Informasi Berbasis SNI ISO 27001 : 2013 Pada Dinas Kependudukan Dan Pencatatan Sipil Kota XYZ *J. Transform. Inf. dan Pengemb. IPTEK* **14** 167–77

[6] Kramer S and Bradfield J C 2010 A General Definition of Malware *J. Comput. Virol.* **6** 105–14

[7] Septani D R, Widiyasono N and Mubarok H 2016 Investigasi Serangan Malware Njrat Pada PC *JEPIN J. Edukasi dan Penelit. Inform.* **2** 123–8

[8] Cahyanto T A, Wahanggara V and Ramadana D 2017 Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis *Justindo J. Sist. dan Teknol. Inf. Indones.* **2** 19–30

[9] Tedyyana A and Supria 2018 Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway *J. Inovtek Polbeng - Seri Inform.* **3** 34–40

[10] IT Governance Ltd 2018 Information Security and ISO 27001 : An Introduction *IT Governance Green Paper* pp 1–10

[11] Ermana F, Tanuwijaya H and Mastan I A 2012 Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM *JSIKA J. Sist. Inf. dan Komput. Akunt.* **1** 1–8

[12] Atmajaya R, Tanuwijaya H and Sutomo E 2016 Audit Keamanan Sistem Informasi Pada Bagian SIMDA Berdasarkan Standart ISO 27002:2005 Di Dinas Pendapatan Dan Pengelolaan Keuangan Daerah Kabupaten Lombok Barat *JSIKA J. Sist. Inf. dan Komput. Akunt.* **5** 1–6

[13] Sarno R and Iffano I 2009 Sistem Manajemen Keamanan Informasi : Teori, Perancangan, dan Implementasi Berbasis ISO 27001

[14] Rosmiati and Riadi I 2016 Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001:2005 Dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ) *Seminar Nasional Teknologi Informasi Dan Multimedia 2016* pp 1.1-1 s/d 1.1-6

[15] Ascanio J G A, Trillos R A B and Bautista D W R 2015 Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información *Tecnura* **19** 123–34

[16] М И Л, К Б Е, Э Е И and И З С 2018 Расчет рисков информационной безопасности телекоммуникационного предприятия Calculation of risks of information security of telecommunication enterprise *Cyber Leninka* **22** 61–70

[17] Budiman A, Wahyuni L S and Bantun S 2019 Perancangan Sistem Informasi Pencarian Dan Pemesanan Rumah Kos Berbasis Web (Studi Kasus : Kota Bandar Lampung) *Tekno Kompak* **13** 24–30

[18] Bakri M and Irmayana N 2017 Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001 *Tekno Kompak* **11** 41