Positif : Jurnal Sistem dan Teknologi Informasi
Volume 5, No.2, 2019

E-ISSN 2460-9552
P-ISSN 2620-3227

Article history
Received Oct 08, 2019
Accepted Dec 01, 2019

AUDIT SISTEM KEAMANAN INFORMASI MENGGUNAKAN ISO 27001 PADA SMKN 1 PUGUNG, LAMPUNG

Pangky Februari[1)] Fitria[2)]
[1,2] Ilmu Komputer, Magister Teknik Informasi, IIB Darmajaya, Bandar Lampung, Indonesia
Email: pangkyfebruari2@gmail.com

Abstract

The implementation of information and communication technology management has become a necessary in every educational institution, especially in SMKN 1 Pugung, Lampung. Hence, in this research is tried to measure the information security standard in SMKN 1 Pugung using ISO 27001. The method used is audit operational which relates with economical and efficiency used of resource as well as the target aimed. Afterwards, the result shows that the analysis of quisionnaire has obtained averages value amounts 3,32 in a whole ISO 27001. It means that information security standard has performed well and written operational procedure standard. Then, the evaluation result which varies from 11 clause I categorized into level 4 (manage and measurable). It means that business process has well-monitored and measured. So therefore, it can be concluded that system audit of security information in SMKN 1 Pugung has been confirmed as good enough.

Keywords: *Audit, ISO 27001, Information Security, SMKN 1 Pugung.*

Abstrak

Penerapan tata kelola teknologi informasi dan komunikasi sudah menjadi kebutuhan dan tuntutan di setiap institusi pendidikan, tidak terkecuali di SMKN Pugung, Lampung. Oleh karena itu, dalam penelitian ini bertujuan untuk mengukur standar keamanan informasi di SMKN Pugung menggunakan ISO 27001. Metodologi penelitian yang digunakan dalam penelitian ini adalah audit operasional yang berkaitan dengan penggunaan secara ekonomis dan efisien atas sumber daya pencapaian tujuan serta sasaran yang diterapkan. Kemudian, hasil dari penelitian ini menunjukkan bahwa analisis penyebaran kuesioner menghasilkan nilai rata-rata, yaitu 3,32 pada seluruh klausul ISO 27001 yang berarti bahwa sistem keamanan informasi telah memiliki standar operasional prosedur yang baku dan tertulis. Lalu, hasil evaluasi temuan yang bervariasi dari 11 klausul dikategorikan ke dalam level 4 (manage and measurable) yang berarti bahwa proses bisnis sudah dimonitor dan diukur denganbaik. Dengan begitu dapat dikatakan bahwa audit sistem keamanan informasi di SMKN 1 Pugung sudah baik.

Kata Kunci: *Audit, ISO 27001, Keamanan Informasi, SMKN 1 Pugung.*

E-ISSN 2460-9552
P-ISSN 2620-3227

1. PENDAHULUAN

Institusi pendidikan SMKN 1 Pugung adalah salah satu bentuk satuan pendidikan formal di kabupaten Tanggamus yang menyelenggarakan pendidikan kejuruan pada jenjang pendidikan menengah sebagai lanjutan dari SMP/MTs atau bentuk lain yang sederajat atau lanjutan dari hasil belajar yang diakui sama/setara SMP/MTs. Penerapan tata kelola teknologi informasi dan komunikasi sudah menjadi kebutuhan dan tututan disetiap institusi pendidikan seperti pada SMKN Pugung Kabupaten Tanggamus. Hal ini dikarenakan peran TIK semakin penting bagi upaya peningkatan kualitas layanan bidang pendidikan sebagai salah satu realisasi dari tata kelola institusi yang baik.

Faktor manajemen keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola keamanan informasi mengalami masalah yang menyangkut kerahasian (*confidentialty*), keutuhan (integrity), dan ketersediaan (availability). Untuk itu diperlukan audit pada keamanan informasi dengan menggunakan metode khusus untuk mengukur dan mengevaluasi keamanan informasi institusi.

ISO/IEC 27001 merupakan salah satu metode dengan standard keamanan informasi yang diterbitkan International Organization for Standarization dan International Electrotecnical Comission (Utomo & Affandy, 2012). ISO 27001 menjadi standar manajemen keamanan informasi yang luas digunakan oleh bisnis dan organisasi, menyediakan referensi tertentu yang paling komprehensif untuk menajemen keamanan informasi di dunia.

Selanjutnya, ISO 27001 juga didefinisikan sebagai dokumen standar sistem manajemen keamanan informasi atau Information Security Management System, biasa disebut ISMS, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah institusi dalam usaha mereka untuk mengevaluasi, mengimplementasikan, dan memelihara keamanan informasi berdasarkan "best practice" dalam pengamanan informasi (Syafrizal & Kom, 2009). ISO 27001 berfokus pada pengurangan risiko terhadap informasi yang bernilai bagi organisasi (Ramadhani et al. 2018). Ada 11 klausul pada ISO 27001, yaitu kebijakan keamanan informasi, organisasi keamanan informasi, pengelolaan aset, kesesuaian, keamanan sumber daya manusia, keamanan fisik dan lingkungan, akses kontrol, akuisisi, pengembangan, dan pemeliharaan sistem informasi, manajemen komunikasi dan operasi, manajemen insiden keamanan informasi, dan manajemen kelangsungan bisnis (Utomo & Affandi, 2012).

Berdasarkan pada penjelasan di atas, itu sistem keamanan informasi sangat dibutuhkan dan diharapkan menjadi pedoman dan standar dengan mengukur seberapa jauh tingkat kematangan keamanan informasi saat ini, terutama di SMKN 1 Pugung.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah audit operasional yang berkaitan dengan penggunaan secara ekonomis dan efisien atas sumber daya pencapaian tujuan serta sasaran yang diterapkan. Audit operasional memiliki 4 tahapan, yaitu perencanaan (*planning*), pekerjaan lapangan (*fieldwork*), pelaporan (*reporting*), dan tindak lanjut (*follow up*) (Gondodiyoto, 2007). Tahapan audit operasional dapat dilihat dalam tahpan berikut ini:

a. Perencanaan (*Planning*)
   Pada tahapan perencanaan, dilakukan dengan kegiatan berikut ini.

   1) Wawancara
      Mewawancarai Kepala ICT untuk mengidentifikasi masalah pada sistem yang berjalan.
   2) Observasi
      Mengamati alur kerja sistem keamanan informasi pada SMKN 1 Pugung.
   3) Studi literatur
      Mengumpulkan bahan referensi berupa teori yang berasal dari buku dan jurnal serta data sekunder yang mendukung hasil penelitian.
   4) Menentukan klausul
      Dalam tahap ini, metode yang akan digunakan untuk mengaudit sistem keamanan informasi menggunakan metode penelitian ISO 27001. ISO/IEC 27001 merupakan sebuah standar keamanan informasi yang secara luas diadaptasi untuk membantu dalam hal menentukan status keamanan informasi. Selain itu, ISO 27001 juga digunakan untuk menentukan tingkat kepatuhan

E-ISSN 2460-9552
P-ISSN 2620-3227

trehadap aturan dan standar keamanan dalam bisnis (Au & Fung, 2016). Kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan (security control clauses), 39 objektif kontrol (control objectives), dan 133 kontrol keamanan/kontrol (controls) (Ermana & Mastan, 2012). Pemilihan klausul pada studi kasus ini disesuaikan dengan sistem keamanan informasi pada SMKN 1 Pugung.

b. Pekerjaan Lapangan (*Fieldwork*)
Pada tahapan pekerjaan lapangan, kegiatan yang dilakukan peneliti adalah sebagai berikut.
1) Membuat kuisioner
Peneliti membuat pernyataan pada kuisioner berdasarkan pedoman pada setiap kontrol keamanan pada ISO 27001.
2) Menyebarkan kuisioner
Peneliti melakukan penyebaran kuisioner kepada bagian ICT sebanyak 5 orang yang dilakukan pada tanggal 1-31 Juli 2019 untuk mendapatkan data primer yang akan digunakan untuk mengukur maturity level sistem keamanan informasi institusi.

c. Pelaporan (*Reporting*)
Kegiatan yang dilakukan pada tahap pelaporan adalah sebagai berikut.
1) Mengukur maturity level
Dalam tahap ini, mengukur maturity level didapatkan dari isian jawaban kuesioner untuk dijadikan laporan hasil audit. Maturity level digunakan untuk mengontrol proses-proses teknologi informasi dengan metode penilaian dan mengetahui posisi maturity level institusi saat ini.
2) Menganalisa *gap* / kesenjangan
Peneliti menganalisa *gap*/kesenjangan *maturity level* untuk menemukan permasalahan yang terjadi.

d. Tindak Lanjut (*Follow Up*)
Pada tahapan tindak lanjut, kegiatan yang dilakukan peneliti adalah sebagai berikut.
1) Membuat rekomendasi perbaikan sistem
Dari hasil pengukuran dapat diketahui kesenjangan yang terjadi pada tingkat kematangan saat ini dan yang diharapkan yang akan dijadikan sebagaitemuan masalah pada sistem keamanan informasi dan memberikan rekomendasi perbaikan yang akan dilaporkan kepada pihak ICT SMKN 1 Pugung.
2) Dokumentasi
Peneliti melakukan dokumentasi terkait aktivitas audit sistem keamanan informasi pada SMKN 1 Pugung.

3. HASIL DAN PEMBAHASAN

3.1. Identifikasi Klausul, Objek Kontrol dan Kontrol Keamanan ISO 27001

Klausul yang akan digunakan dalam penelitian ini ada 11, yaitu A5 (kebijakan keamanan), A6 (organisasi keamanan informasi), A7 (pengelolaan aset), A8 (keamanan sumber daya manusia), A9 (keamanan fisik dan lingkungan), A10 (pengelolaan operasi dan komunikasi), A11 (pengendalian akses), A12 (akuisisi sistem informasi, pengembangan, dan pemeliharaan), A13 (pengelolaan peristiwa keamanan informasi), A14 (pengelolaan bisnis yang berkelanjutan), dan A15 (pemenuhan). Berdasarkan klausul yang ditetapkan, terdapat 39 objektif kontrol yang akan digunakan dalam penelitian ini. Setelah ditentukan objektif kontrol, terdapat 133 kontrol keamanan yang ada didalam objektif kontrol.

3.2. Analisa Kesenjangan

Berdasarkan data yang ada, dapat dianalisa hasil temuan masalah pada keamanan informasi sekolah adalah sebagai berikut.

1. A5 Kebijakan Keamanan

Dari proses perhitungan diperoleh nilai rata-rata pada klausul kebijakan keamanan dengan nilai 3,8 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 4 (*manage*), yang berarti bahwa institusi telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan keamanan informasi yang ada dan telah sesuai dengan harapan pihak manajemen sekolah.

2. A6 Organisasi Keamanan Informasi

Dari proses perhitungan diperoleh nilai rata-rata pada klausul organisasi keamanan informasi dengan nilai 3,06 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*). Hal ini

E-ISSN 2460-9552
P-ISSN 2620-3227

berarti bahwa institusi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul organisasi keamanan informasi terdapat *gap* 0,94 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen. Dibutuhkannya suatu pengaturan pengelolaan resiko dan penjaminan informasi yang dapat diakses oleh pihak luar institusi.

3. A7 Pengelolaan Aset

   Dari proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan aset dengan nilai 3,58 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 4 (*manage*), yang berarti bahwa institusi telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan aplikasi teknologi informasi yang ada dan pengelolaan aset informasi telah sesuai dengan harapan pihak manajemen.

4. A8 Keamanan Sumber Daya Manusia

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul keamanan sumber daya manusia dengan nilai 3,29 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan tentang kegiatan *monitoring*, evaluasi, dan penilaian terhadap keamanan sumber daya manusia untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul keamanan sumber daya manusia terdapat *gap* 0,71 dari perbandingan tingkat kematangan saat ini dengan harapan pihak manajemen. Ketika terjadi PHK, karyawan akan mengembalikan semua aset milik institusi dan hak akses karyawan pada sistem informasi akan dialihkan untuk menjaga keamanan informasi institusi.

5. A9 Keamanan Fisik dan Lingkungan

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul keamanan fisik dan lingkungan dengan nilai 3,40 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah di sosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan penilaian keamanan fisik dan lingkungan instansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul keamanan fisik dan lingkungan terdapat *gap* 0,6 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen. Diharapkan sistem informasi tidak dikelola oleh pihak luar instansi khususnya data-data yang bersifat sensitif dan perawatan terhadap perangkat keras agar menjadi fokus utama instansi.

6. A10 Pengelolaan Operasi dan Komunikasi

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan operasi dan komunikasi dengan nilai 3,47 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah di sosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan penilaian pengelolaan operasi dan komunikasi yang ada di instansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul pengelolaan operasi dan komunikasi terdapat *gap* 0,53 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen. Perlu diberlakukannya jam pemprosesan sistem informasi di institusi agar pengelolaan informasi dapat sepenuhnya diawasi ketika jam kerja sedang berlangsung.

7. A11 Pengendalian Akses

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengendalian akses dengan nilai 2,98 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan

E-ISSN 2460-9552
P-ISSN 2620-3227

penilaian pengendalian akses sistem informasi yang ada di instansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul pengendalian akses terdapat *gap* 1,02 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen. Setiap perangkat komputer perlu diberlakukan batasan pemprosesan data sehingga tidak semua karyawan dapat mengakses informasi yang memang bukan haknya.

8. A12 Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul akuisisi sistem informasi, pengembangan, dan pemeliharaan dengan nilai 3,27 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan penilaian akuisisi sistem informasi, pengembangan, dan pemeliharaan yang ada diinstansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul akuisisi sistem informasi, pengembangan, dan pemeliharaan terdapat *gap* 0,73 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen. Diperlukan *source code* program yang dapat membatasi akses pengguna sistem informasi, dan juga adanya pengendalian pergantian *software* pada instansi.

9. A13 Pengelolaan Peristiwa Keamanan Informasi

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan peristiwa keamanan informasi dengan nilai 3,25 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan penilaian pengelolaan peristiwa keamanan informasi yang ada diinstansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul pengelolaan peristiwa keamanan informasi terdapat *gap* 0,75 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen. Perlu diberlakukannya pelaporan kelemahan keamanan sistem informasi sehingga kelemahan tersebut dapat segera diatasi dan ditindaklanjuti untuk menjaga keamanan informasi institusi.

10. A14 Pengelolaan Bisnis yang Berkelanjutan

    Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan bisnis yang berkelanjutan dengan nilai 3,52 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 4 (*manage*), yang berarti bahwa perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan aplikasi teknologi informasi yang ada. Pada klausul pengelolaan bisnis yang berkelanjutan sudah memenuhi harapan pihak manajemen.

11. A15 Pemenuhan

    Pada proses perhitungan diperoleh nilai rata-rata pada klausul pemenuhan dengan nilai 3,48 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan tentang kegiatan *monitoring*, evaluasi, dan penilaian yang ada diinstansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul pemenuhan terdapat *gap* 0,52 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen. Perlu adanya prosedur keamanan informasi yang diterapkan untuk menjamin pemenuhan, perundangan, dan peraturan dalam pengelolaan informasi institusi.

4. PENUTUP

Berdasarkan hasil penelitian maka diperoleh simpulan dimana hasil analisis penyebaran kuesioner menghasilkan nilai rata-rata, yaitu 3,32 pada seluruh klausul ISO 27001 yang berarti

E-ISSN 2460-9552
P-ISSN 2620-3227

bahwa system keamanan informasi telah memiliki standard operasional prosedur yang baku dan tertulis yang telah disosialisasikan ke segenap jajaran dan staf untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari dan telah mencapai titik *defined process* dalam keamanan informasi.

Hasil evaluasi temuan yang bervariasi dari 11 klausul yang digunakan untuk menganalisis dan merekomendasikan perbaikan system keamanan informasi yang dikategorikan ke dalam level 4 (*manage and measurable*) yang berarti bahwa proses bisnis sudah dimonitor dan diukur dengan baik.

5. REFERENSI

Au, CH & Fung, WSL. (2016). *Knowledge Audit Model for Information Security.* Canberra: University of Sydney.

Ermana, F., Tanuwijaya, H., & Mastan, I. A. (2012). Audit Keamanan Sistem Informasi Berdasarkan Standar Iso 27001 Pada PT. BPR JATIM. *Jurnal JSIKA, 1*(1).

Gondodiyoto, S. (2007). Audit sistem informasi + pendekatan CobIT. *Jakarta: Mitra Wacana Media*.

Ramadhani, S. T. A., Hartanto, R., & Nugroho, E. (2018). RISK-MANAGEMENT BASED GOVERNMENT INFORMATION SYSTEM SECURITY USING OCTAVE ALLEGRO FRAMEWORK. In *Proceeding of International Seminar & Conference on Learning Organization*.

Syafrizal, M., & Kom, S. (2009). Information Security Management System (ISMS) MenggunakanStandar ISO/IEC 27001: 2005. *Jurnal DASI*, *10*(1), 92-117.

Utomo, M., Ali, A. H. N., & Affandi, I. (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001: 2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik ITS*, *1*(1), A288-A293.