Turnitin Originality Report

Processed on: 18-Jul-2021 08:37 WIB
ID: 1620840154
Word Count: 2574
Submitted: 1

Artikel TA By Yusuf Bahrudin Nizar

Similarity Index	Similarity by Source	
23%	Internet Sources:	22%
	Publications:	0%
	Student Papers:	6%

10% match (Internet from 02-Oct-2020)
http://repository.its.ac.id/2290/1/5212100178-Undergraduate_Theses.pdf

6% match (student papers from 15-Jan-2020)
Submitted to Forum Perpustakaan Perguruan Tinggi Indonesia Jawa Timur on 2020-01-15

3% match (Internet from 25-Nov-2020)
http://repository.its.ac.id/50822/1/09211450053024-Master_Thesis.pdf

3% match (Internet from 30-Apr-2021)
https://jurnal.dinamika.ac.id/index.php/jsika/article/download/3387/1502

JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X Sistem Manajemen Keamanan Informasi Berbasis ISO/IEC 27001:2013 Pada PT Angkasa Pura 1 (Persero) Surabaya Yusuf Bahrudin Nizar 1) Pantjawati Sudarmaningtyas 2) Slamet HASH(0x7f218310a3f8) security related to information assets is a critical aspect that must maintain by PT Angkasa Pura 1 (Persero) Surabaya, which handles the airport business sector includes services such as baggage control, aerodrome, and airport facilities. Information security systems that unwell manage can pose problems related to confidentiality, integrity, and availability. This study aims to improve security information systems thru risk assessment using the OCTAVE method to find the highest impact when the risk occurs and prioritization those risks. The objective and security controls build based on using ISO/IEC 27001:2013. The results of this study are the document of objective and security control, risk management documents, standard operational procedure (SOP) documents. The risk management documents related to information security, including risk assessment, risk identification, risk analysis, and evaluation at PT Angkasa Pura 1 (Persero) Surabaya. Standard Operational Procedure (SOP) documents include policy documents, work instructions, and work records that align with the selection of objective controls and security controls from risk management. Keywords: ISO27001, OCTAVE, Standard Operational Procedure PT Angkasa Pura I (Persero) Surabaya merupakan badan usaha milik negara dalam bidang usaha kebandarudaraan yang meliputi layanan pengendalian bagasi, layanan garbarata dan layanan fasilitas pengguna bandara. Salah satu misi PT Angkasa Pura 1 (Persero) Surabaya Yaitu mengusahakan jasa kebandaraudaraan melalui pelayanan prima yang memenuhi standar keamanan, kesalamatan, dan kenyamanan (PT Angkasa Pura 1, 2017). Untuk mengetahui proses yang ada pada layanan bisnis utama PT Angkasa Pura 1 (Persero) Surabaya dapat diperoleh dengan analisis value chain. Kondisi saat ini banyak ditemukan ancaman (Threat) dan kelemahan (Vurnerable) dari segi manajerial maupun teknis antara lain: Ancaman

(Threat) yang terjadi dari luar organisasi meliputi virus, worm, dan malware yang menyebabkan kerusakan, kehilangan, dan lambatnya akses data penerbangan pada aplikasi Flight Information Display System (FIDS) yang dibutuhkan untuk menjalankan salah satu layanan utama yaitu baggage handling. belum adanya kebijakan recovery server Ketika mengalami sebuah kegagalan sistem (down) yang menyebabkan informasi penerbangan tidak tersedia untuk pengunjung sehingga proses bisnis perusahaan terganggu. Berdasarkan Service Level Agreement (SLA) down time pada permasalahan tersebut paling lama terjadi selama 24 jam. Belum adanya kebijakan manajemen asset terkait keamanan informasi sehingga tidak ada yang bertanggung jawab dalam mengelola asset informasi. Selain itu belum adanya kebijakan autentikasi dan otorisasi terkait keamanan informasi untuk pengguna yang memiliki hak akses terhadap informasi terkait penentuan kualitas, perencanaan, pengendalian dan evaluasi proses bisnis utama, sehingga ketika terjadi kehilangan atau kesalahan informasi proses bisnis dapat terganggu dan pihak manajer tidak dapat menelusuri terkait kesalahan yang terjadi. Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi dari sisi CIA adalah dengan penyusunan dokumen Sistem Manajemen Keamanan Informasi dan pembuatan SOP (Standard Operational Procedure) dengan tujuan sebagai HASH(0x7f218310d1f8) PT JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 1 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X Angkasa Pura 1 (Persero) Surabaya agar HASH(0x7f218310d450) (Standard Operational Procedure) dipilih melalui pengendalian kontrol objektif dan kontrol keamanan menggunakan ISO/IEC 27001:2013 yang sesuai HASH(0x7f218310d870) dilakukan dalam 3 tahap yaitu tahap awal, tahap pengembangan, dan tahap akhir. Metodologi penelitian secara detil terdapat pada Gambar 1. A. Studi Literatur Studi literatur dilakukan dengan cara mempelajari dan mencari referensi, yang menjadi dasar keterkaitan topik penelitian yang berkaitan dengan keamanan informasi. Mengingat pentingnya keamanan informai bagi suatu organisasi, maka keamanan informasi sangat dibutuhkan untuk menjaga informasi dari seluruh ancaman yang mungkin terjadi, dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisasi risiko bisnis (Sarno & Iffano, 2009). B. Identifikasi Masalah Identifikasi masalah dilakukan dengan mengidentifikasi HASH(0x7f218310a218), permasalahan objek terkait dalam penelitian yakni pada PT Angkasa Pura 1 (Persero) Surabaya khususnya pada divisi ICT. Identifikasi dilakukan sesuai dengan hasil wawancara dan observasi terkait kondisi saat ini pada instansi. C. Identifikasi Aset dan HASH(0x7f218310d9c0), 2013). Proses ini memeliki empat langkah, yaitu: 1) Identifikasi aset dan klasifikasi aset dengan menggunakan tabel aset 2) Menghitung nilai aset berdasarkan aspek keamanan informasi (CIA) dengan memberikan nilai masing-masing, setelah ini dihitung nilai asetnya. 3) Menghitung nilai ancaman dan kelemahan aset 4) Identifikasi dampak kegagalan terhadap aspek keamanam informasi (CIA) yaitu dengan membuat tabel identifikasi dampak bisnis disertai level dampak yang terjadi. Gambar1.MetodologiPenelitian D. Penilaianrisiko Peniliaian terhadap risiko yang telah teridentifikasi dengan melakukan penerapan metodeOCTAVE(OperationallyCriticalThreat, Asset, and Vulnerability Evaluation) dengan hitungan matematis dalam analisa penilaian risikonya. OCTAVE adalah sebuah pendekatan terhadapevaluasirisikodaritigaaspekkeamanan informasi yaitu confidentiality, integrity, dan availability yang komprehensif, sistematik, terarah, dan dilakukan sendiri. (Suprandono, 2009) E.Identifikasidanevaluasipenangananrisiko Melakukan penanganan risiko langkah yangharusdilakukanyaitumengidentifikasiatau menentukan pilihan pengelolaan risikonya. Pilihan pengelolaan risiko: menerina risiko dengan menerapakan kontrol keamanan yang sesuai, menerima risiko dengan menggunakan kriteria risiko yang telah diterapkan, dan menerima risiko dengan men-transfer risiko kepadapihakketiga(asuransi,vendor,ataupihak

tertentu)(Sarno&Iffano,2009). F.PenentuanruanglingkupSMKI Penentuan ruang lingkup ini sangat dibutuhkan dengan tujuan dokumen yang JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 2 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X dihasilkan sesuai dengan kebutuhan permasalahan keamanan informasi pada divisi ICT. Dalam menentukan ruang lingkup Sistem Manajemen Keamanan Informasi (SMKI) dibutuhkan identifikasi masalah dari sisi eksternal dan internal di bagian ICT. HASIL DAN PEMBAHASAN A. Identifikasi Aset Kritis Daftar Aset kritis yang dimiliki divisi Information Communication and Technology Department Head (ICT) terdapat pada Tabel 1, dan secara lengkap disajikan pada lanjutan tabel 1 pada lampiran. B. Identifikasi Ancaman dan kelamahan Identifikasi ancaman dan kelemahan pada aset kritis dikategorikan ke dalam hardware, software, jaringan, data atau informasi dan SDM pada divisi Information Communication and Department Head (ICT). Daftar ancaman dan kelemahan terdapat pada Tabel 2 secara lengkap disajikan pada lanjutan tabel 2 pada lampiran. Tabel 1. Daftar Aset Kritis No Ketegori Aset 1. Hardware PC Server 2. Software FIDS Counter check-in 3. Jaringan Wifi Router Switch Kabel 4. Data Data Center Data Jadwal penerbangan Data Shift Kerja Pegawai Data Maskapai Tabel 2. Identifikasi Ancaman dan Kelemahan No Kategori Daftar aset Ancaman aset dan kelemahan 1. Hardware Server Bencana alam Kehilangan data Pencurian komponen Software Jaringan PC FIDS Wifi Router Switch Kerusakan server Server down Server mati Bencana alam PC rusak Kerusakan komponen PC Pencurian komponen PC Serangan virus,worm, mallware. Kesalahan konfigurasi Akses ilegal Pembobolan sistem Aplikasi tidak dapat diakses Monopoly bandwitch Kerusakan hardware Hilangnya komponen hardware Gangguan router C. Penilaian Risiko Penilaian Risiko sendiri adalah sebagai suatu HASH(0x7f218310eea0) (Siahaan 2007). Metode yang digunakan dalam penilaian risiko yaitu metode OCTAVE. Dengan menggunakan pendekatan terhadap evaluasi risiko dari tiga aspek keamanan informasi yaitu confidentiality, integrity, availability yang komprehensif, sistematik, terarah dan dilakukan sendiri dengan hitungan kuantitatif. D. Menentukan Kemungkinan (Probability) Tujuan menentukan kemungkinan ancaman yang timbul sesuai dengan identifikasi dan kelemahan. Penentuan kemungkinan (probability) berdasarkan histori kejadian ancaman sebelumnya, atau ditentukan berdasarkan JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 3 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X pengamatan kondisi yang dinilai. Dijabarkan pada tebel 3. E.HASH(0x7f218310f128) perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan risiko. Pilihan penanganan risiko pada ICT ditentukan sebagai berikut: 1) Menerima risiko dengan menetapkan kontrol keamanan yang sesuai 2) Menerima risiko dengan menggunakan kriteria penerimaan risiko yang ada F. Memilih Kontrol Objektif dan Kontrol Keamanan Pengelolaan Risiko Tujuan penentuan pemetaan kontrol obejektif ini HASH(0x7f218310f470). Berikut tabel pemetaan hasil rekomendasi pengendalian risiko dengan kebutuhan pada ISO 27001:2013. Pemetaan risiko dengan kebutuhan terdapat pada tabel 4 dan secara lengkap disajikan pada lanjutan tabel 4 pada lampiran. Tabel 3. Penilaian kemungkinan probalitas Nama aset Jenis aset Risiko Jenis Probability Rata-rata kejadian probability server Hardware Bencana alam Threat Low Kehilangan data Kerusakan server Pencurian komponen Kesalahan konfigurasi akses ilegal Server Down Serangan Virus Jumlah ancaman Nilai Threat Vulnerable Threat Threat Vulnerable Low Medium Medium Medium 0,2 0,2 0,4 0,6 0,4 Threat Medium 0,4 Threat Low 0,2 Vulnerable High 0,8 Jumlah rata-rata probabilitas 3,2 Jumlah rata-rata probabilitas/ jumlah ancaman 3,2 / 8 = 0,4 JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 4 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X Tabel 4. Memilih kontrol objektif dan kontrol keamanan pengelolaan risiko Kategori aset Aset potensi kegagalan Potensi Penyebab kegagalan Kontrol keamanan Hardware Kerusakan server Kerusakan PC Kesalahan konfigurasi server Kesalahan A.11.2.4 kontrol pemeliharaan

peralatan konfigurasi PC Data Data hilang Kelalaian teknisi HASH(0x7f218310f7a0).3.1 penggunaan informasi otentikasi rahasia A.12.4.3 Log administrasi dan operator Aset tidak dipelihara A.8.1.1 inventarisasi terhadap aset HASH(0x7f2183121080) Manipulasi data Rusaknya media A.12.3.1 backup informasi penyimpanan A.11.2.4 kontrol keamanan pemeliharaan peralatan Username password A.9.1.1 kebijakan pengendalian diketahui orang lain kontrol akses HASH(0x7f218310f5d8).4.3. prosedur log-on yang aman HASH(0x7f21831129c0) Informasi Kesalahan Adanya kesalahan HASH(0x7f218310f218) informasi informasi akibat kelalaian pegawai HASH(0x7f2183120a68) Manajemen HASH(0x7f2183120c78) Adanya kesalahan HASH(0x7f2183103000) dalam penyampaian informasi Software Aplikasi User dan password A.9.1.1 kebijakan pengendalian diakses oleh diketahui oleh kontol akses pihak yang pengguna lain HASH(0x7f218312d328).4.3 sistem manajemen password JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 5 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X Tabel 5. Perancangan dan struktur isi SOP Struktur Sub-Bab Pendahuluan Tujuan HASH(0x7f21831221b8) Ruang lingkup HASH(0x7f2183122320) ICT Rincian kebijakan Dokumen terkait Tujuan Ruang lingkup referensi Dokumen terkait Tujuan Konten Deskripsi umum dokumen Prosedur keamanan aset informasi Aspek keamanan HASH(0x7f2183122710) - HASH(0x7f2183112a08)HASH(0x7f218312d418)HASH(0x7f2183122290) - HASH(0x7f2183122e48) G. Perancangan struktur dan isi SOP Pada perancangan struktur dan isi SOP ini akan di sesuaikan dengan kebutuhan penelitian. Standar Operational Procedure (SOP) adalah pedoman yang berisi prosedur operasional standar yang berada di suatu organisasi yang digunakan untuk memastikan semua keputusan dan tindakan, serta penggunaan fasilitas-fasilitas proses yang dilakukan oleh orang-orang dalam organisasi dan merupakan anggota organisasi agar dapat berjalan dengan efektif,efisien, standar dan sistematis (Tambunan, 2013). HASH(0x7f2183125b28) tabel 5 dan secara lengkap disajikan pada lanjutan tabel 5 pada lampiran H. Dokumen yang dihasilkan membahas terkait dengan proses dan output dari penelitian ini, penjelasannya dapat dilihat pada tabel 6. Tabel 6. Hasil Proses dan Output Proses Output 1. Pemetaan klausul dengan kontrol objektif 2. Pemetaan risiko dengan kontrol keamanan 3. Pemetaan klausul dengan kebutuhan keamanan informasi 4. Pemetaan risiko dengan dokumen kebijakan 1. Kebijakan pengelolaan hardware 2. Kebijakan human resource security 3. Intruksi kerja pengelolaan hak akses 4. Intruksi kerja reset password 5. Intruksi kerja back- up data dan file 6. Intruksi kerja restore data JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 6 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X Proses Output 5. Pemetaan kebijakan, intruksi kerja, dan rekam kerja. 7. Intruksi kerja perawatan hardware 8. Intruksi kerja keamanaan informasi 9. Intruksi kerja perawatan kabel dan jaringan 10. HASH(0x7f2183125ff0) 14. formulir pengelolaan hak akses KESIMPULAN DAN SARAN A. KESIMPULAN Berdasarkan hasil pengerjaan penelitian yang telah dilakukan maka di dapat : a) Dokumen kontrol objektif dan kontrol keamanan Dokumen pengelolaan risiko terkait keamanan informasi, meliputi: penilaian risiko, identifikasi risiko, analisa dan evaluasi risiko, identifikasi dan evaluasi risiko penanganan risiko pada PT Angkasa Pura 1(Persero) Surabaya. b) Dokumen SOP (Standar Operational Procedure) meliputi: dokumen kebijakan, intruksi kerja, dan rekam kerja yang sesuai dengan pemilihan kontrol objektif dan kontrol keamanan dari hasil pengelolaan risiko terkait keamanan informasi B. Saran a) Pengembangan tugas akhir dapat dilakukan dengan menambahkan dampak biaya kerugian yang dialami oleh instansi b) HASH(0x7f21831265d8) c) HASH(0x7f218312ce60) DAFTAR PUSTAKA Iffano, Irsyad, Sarno, Riyanarto. (2009). Sistem Manajemen Keamanan Informasi : Berbasis ISO 27001 . Surabaya: ITS Press. ISO, (2013). HASH(0x7f218312d118) PT Angkasa Pura 1, (2017). Laporan Tahunan.

Surabaya. Siahaan, H. 2007. Manajemen Risiko. Jakarta: PT. Elex Media Computindo. Suprandono, B. (2009). Manajemen Resiko Keamanan Informasi dengan Menggunakan Metode OCTAVE. Semarang: Teknik Elektro Universitas Muhammadiyah Semarang Tambunan, R.M. (2013). Pedoman Penyusunan Standar Operating Procedures (SOP). Jakarta: Masitas Publishing. JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 7 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X LAMPIRAN Lanjutan tabel 1. Daftar Aset Kritis No Kategori Aset 4. Data Data perencanaan pengadaan fasilitas bandara Data pengendalian bagasi Data oeprator garbarata Data keuangan Data hasil evaluasi tiap layanan bisnis utama Data aset Data calon penumpang 5 Sumber Daya Manusia (SDM) Pegawai Satuan pengamanan Lanjutan tabel 2. Identifikasi ancaman dan Kelemahan No Kategori Aset Daftar Aset 4. Data Data center Data jadwal penerbangan Data shift kerja pegawai Data hasil evaluasi tiap layanan bisnis utama Data aset Data maskapai Data pengendalian bagasi Data keuangan 5. Sumber Daya Pegawai Manusia (SDM) Satuan pengamanan Ancaman dan kelemahan Kesalahan input data Pencurian data Data corrupt/rusak Data tidak dapat diakses Data hilang Password shared Penyalahgunaan data tidak sesuai Password shared Lanjutan Tabel 4. Memilih kontrol objektif dan kontrol keamanan pengelolaan risiko Ketegori Aset Aset Potensi Kegagalan Potensi penyebab Kegagalan Kontrol keamanan SDM HASH(0x7f218312d550) syarat dan ketentuan kerja akses A.7.2.2 kepedulian pendidikan dan pelatihan keamanan informasi A.9.1.1 kebijakan pengendalian kontrol akses Data tidak sesuai Kesalahan input data HASH(0x7f2183130458)-on JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 8 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X Lanjutan Tabel 5 Perancangan Struktur dan isi SOP Struktur Sub-Bab Kebijakan keamanan Ruang lingkup informasi Referensi Kebijakan pengelolaan hardware Kebijakan human resource security Prosedure pengelolaan hak akses Prosedur backup dan restore Intruksi kerja Dokumen terkait Tujuan Ruang lingkup Rincian kerja Dokumen terkait Tujuan Ruang lingkup referensi Rincian kebijakan Dokumen terkait tujuan tujuan Ruang lingkup definisi rincian prosedure Tujuan Ruang lingkup Referensi Rincian umum prosedur Bagan alur SOP Intruksi kerja perubahan hak kases Intruksi kerja perubahan password Konten Acuan kerja yang HASH(0x7f2183130818) backup dan restore informasi -HASH(0x7f2183130c38) -HASH(0x7f2183121188) -Prosedur pelatihan dan pengembangan SDM Deskripsi umum SOP HASH(0x7f2183130bf0)HASH(0x7f2183121248)JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 9 JSIKA Vol. ??, No. ??. Tahun 20?? ISSN 2338-137X Struktur Sub-bab Konten Intruksi kerja reset password Intruksi kerja backup file Intruksi kerja restore data Intruksi kerja perawatan hardware Intruksi kerja perawatan kabel jaringan telekomunikasi JSIKA Vol. ??, No. ??, Tahun 20??, ISSN 2338-137X Page 10