

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis keamanan sistem informasi pada PT. Asia Bandar Alam dapat disimpulkan bahwa:

1. ISO 27002 berperan sebagai standar dalam melaksanakan proses kontrol keamanan sistem informasi yang bertujuan untuk meminimalisir terjadinya risiko dalam perusahaan.
2. Penerapan ISO 27002 sebagai standarisasi keamanan sistem informasi pada PT. Asia Bandar Alam masih terbelang kurang karena rata – rata tingkat kematangan keamanan sistem informasi berada pada tingkat dua yaitu *initial/ad hoc*.
3. Terdapat beberapa kontrol dalam perusahaan yang berjalan secara spontanitas dikarenakan belum adanya aturan baku yang formal dan juga belum ada kebijakan maupun prosedur yang terdokumentasi.
4. Sebagian besar kontrol masih dijalankan secara informal. Dan banyak kontrol yang belum ada dokumentasi dan prosedur sehingga diperlukan membuat SOP supaya kontrol - kontrol dapat berjalan sesuai dengan landasan yang telah dibuat sehingga karyawan mempunyai prosedur tertulis yang dapat diikuti dan tidak hanya terbatas pada aturan aturan informal.

5.2 Saran

Berdasarkan hasil analisis keamanan sistem informasi pada PT. Asia Bandar Alam, diberikan saran untuk mencapai hasil yang diharapkan perusahaan dan saran bagi penelitian selanjutnya sebagai berikut:

1. Bagi perusahaan

- Diharapkan perusahaan dapat melakukan perbaikan manajemen keamanan sistem informasi sesuai dengan rekomendasi agar ancaman – ancaman yang berhubungan dengan keamanan sistem informasi dapat dikurangi.
- Diharapkan perusahaan dapat melakukan audit keamanan sistem informasi menggunakan ISO 27002 setelah memperbaiki manajemen keamanan sistem informasi.

2. Bagi penelitian selanjutnya

- Peneliti selanjutnya diharapkan untuk mengkaji lebih banyak referensi – referensi yang berkaitan dengan keamanan informasi sehingga hasil penelitian dapat lebih lengkap.

5.3 Justifikasi Penelitian

Berdasarkan hasil temuan dan rekomendasi yang didapat saat melakukan penelitian, perusahaan sudah mengikuti rekomendasi dari peneliti diantaranya :

1. Perbaikan tata letak kabel pada perusahaan dengan menggunakan penutup pada kabel – kabel yang terlihat oleh orang – orang, sehingga kabel menjadi lebih aman dan mengurangi terjadinya risiko keamanan.
2. Penggunaan antivirus terbaru untuk meminimalisir risiko sistem terinfeksi virus.
3. Adanya pengecekan dan pemeliharaan peralatan setiap 2 bulan sekali untuk memastikan semua peralatan pada perusahaan masih layak pakai.
4. Adanya peraturan untuk tidak boleh mengambil foto maupun video pada area ruangan perusahaan.

5. Terdapat peraturan untuk pembuatan dan penyimpanan kata sandi sehingga meminimalisir risiko keamanan sistem informasi.



DAFTAR PUSTAKA

- [1] Martin, "Managing Information Technology What Managers Need to Know. Pearson Educational International. New Jersey.," vol. 1, 1999.
- [2] G. Simson, "Pretty Good Privacy, O'Reilly & Associates," 1995.
- [3] H.S.W., "STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005," *Notes Queries*, vol. s6IX, no. 213, p. 52, 2015, doi: 10.1093/nq/s6-IX.213.77-d.
- [4] KOMINFO, *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*. 2011.
- [5] D. Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber," *J. Ilm. Saintikom, Univ. Sumatera Utara, Medan*, vol. 1978–6603, pp. 209–216, 2014.
- [6] G. Sharma, A. Kumar, and V. Sharma, "Windows operating system vulnerabilities," vol. 1, no. 3, p. 10, 2011.
- [7] E. Kurniawan and I. Riadi, "SECURITY LEVEL ANALYSIS OF ACADEMIC INFORMATION SYSTEMS BASED ON STANDARD ISO 27002: 2013 USING SSE-CMM," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)*, vol. 16, no. 1, 2018.
- [8] Nurul Fadhylah Octariza, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC27002 Pada Kantor Pusat PT. JASA MARGA," Universitas Islam Negeri Syarif Hidayatullah, 2019.
- [9] A. N. Fatimah, "PEMBUATAN DOKUMEN SOP (STADARD OPERATING PROCEDURE) KEAMANAN DATA YANG MENGACU PADA KONTROL KERANGKA KERJA COBIT 5 DAN ISO27002:2013 (STUDI KASUS : STIE PERBANAS)," *Keamanan Sist. Inf.*, 2016.
- [10] D. Anjani, "Identifikasi , Penilaian , dan Mitigasi Risiko Keamanan Informasi Pada Sistem Electronic Medical Record (Studi Kasus : Aplikasi Healthy Plus Modul Rekam Medis Di RSUD HAJI SURABAYA)," 2014.
- [11] A. P. Subriadi and N. F. Najwa, "The consistency analysis of failure mode

- and effect analysis (FMEA) in information technology risk assessment,” *Heliyon*, vol. 6, no. 1, p. e03161, 2020, doi: 10.1016/j.heliyon.2020.e03161.
- [12] V. Venkatesh, M. Morris, G. Davis, and F. Davis, “User acceptance of information technology: Toward a unified view,” vol. 27, no. 3, pp. 425–478, 2003.
- [13] P. Adler and P. Adler, *Teknik-Teknik Observas*. 2009.
- [14] H. Hasanah, “TEKNIK-TEKNIK OBSERVASI (Sebuah Alternatif Metode Pengumpulan Data Kualitatif Ilmu-ilmu Sosial),” *At-Taqaddum*, vol. 8, no. 1, p. 21, 2017, doi: 10.21580/at.v8i1.1163.
- [15] I. N. Rachmawati, “Pengumpulan Data Dalam Penelitian Kualitatif: Wawancara,” *J. Keperawatan Indones.*, vol. 11, no. 1, pp. 35–40, 2007, doi: 10.7454/jki.v11i1.184.
- [16] I. Pujihastuti, “PRINSIP PENULISAN KUESIONER PENELITIAN,” *J. Agribisnis dan Pengemb. Wil.*, vol. 2, no. 1, pp. 43–56, 2010.
- [17] T. Berners-Lee, *Weaving the Web: the past, present and future of the world wide web by its inventor*. Texere, 2000.
- [18] S. Garfinkel, *PGP: Pretty Good Privacy*. O’Reilly & Associates, Inc, 1995.
- [19] John D. Howard, “An Analysis Of Security Incidents On The Internet 1989 - 1995,” Carnegie Mellon University, 1997.
- [20] I. SO, “ISO/IEC 27002:2013(E),” 2013.
- [21] P. V. Handrianus, W. Widiatry, R. Priskila, and P. B. A. A. Putra, “Penerapan Skala Likert dan Skala Dikotomi Pada Kuesioner Online,” 2019.
- [22] Z. Luhua, “No Title,” in *Analysis of software capability maturity model (CMM)*. In *Proceedings of the 2012 National Conference on Information Technology and Computer Science*, 2012, pp. 830–833.
- [23] Ismail Ibnu, “Dokumentasi: Pengertian, Tujuan dan Fungsinya untuk Perusahaan,” *Mark. Manaj.*, vol. 1, pp. 2–3, 2020.
- [24] Maulina Rishna, “Cara Pembuatan dan Manfaat Standar Operasional Prosedur Perusahaan,” *Hum. Resour.*, vol. 1, 2019.

- [25] K. Nia, "HAK dan DISIPLIN KARYAWAN (Manajemen SDM Lanjut)," vol. 1, p. 5.
- [26] Nurichsan, "Managemen Password," *Password Manag.*, vol. 1, p. 4, 2011.
- [27] Kementrian Keuangan Republik Indonesia, "Meja Rapi dan Bersih, Ciptakan Lingkungan Kerja yang Aman dan Nyaman," 2020.
<https://www.djkn.kemenkeu.go.id/artikel/baca/13354/Meja-Rapi-dan-Bersih-Ciptakan-Lingkungan-Kerja-yang-Aman-dan-Nyaman.html>.
- [28] S. Sign-on, "OTENTIKASI (Authentication)," *Keamanan pada website*, pp. 1–19.
- [29] H. Badrul, Mohammad, "Segmentasi Jaringan Dengan Menggunakan Virtual Local Area Network," *J. Tek. Komput.*, vol. 2.2, pp. 7–16, 2016.
- [30] Mufadhol, "Strategi Dan Algoritma Routing Dalam Jaringan," *J. Transform.*, p. 3, 2007.
- [31] F. Nugraha, "Audit Kontrol Akses Sistem Informasi Berdasarkan Standar ISO 27002 Pada PT. Karya Karang Asem Indonesia," 2012.
- [32] Tashia, "Keamanan Jaringan Internet dan Firewall," *KOMINFO*, 2017.
<https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/>.
- [33] Mekari, "7 Jenis Pelatihan dan Pengembangan SDM Bagi Perusahaan," *J. Enterp.*, 2019.
- [34] and A. F. Susanto, Fredy, Muhammad Nur Rifai, "Internet of Things Pada sistem keamanan ruangan, studi kasus ruang server Perguruan Tinggi Raharja," *SEMNASTEKNOMEDIA ONLINE*, 2017.
- [35] Andani and Swelly, "Andani, Swelly. PENYUSUNAN STANDAR OPERASIONAL PROSEDUR PENGAMANAN FISIK KABEL BERDASARKAN SNI ISO/IEC 27001: 2009," 2017.
- [36] R. D. AJI, "EVALUASI RISIKO CELAH KEAMANAN MENGGUNAKAN METODOLOGI OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA APLIKASI WEB SISTEM INFORMASI MAHASISWA (STUDI KASUS: PERGURUAN TINGGI XYZ)," 2016.

- [37] T. Sinau, "Data Validation," 2020, p. 1.
- [38] T. A. Cahyanto and Y. Prayudi, "Investigasi Forensika Pada Log Web Server untuk Menemukan Bukti Digital Terkait dengan Serangan Menggunakan Metode Hidden Markov Models," *Snati*, pp. 15–19, 2014.

