BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian yang telah didapatkan pada bab 4, serta untuk menjawab rumusan masalah penelitian pada bab 1, maka dapat ditarik kesimpulan bahwa:

1. Penggunaan teknologi informasi dan penerapan sistem informasi kini mempunyai peranan yang besar bagi perusahaan untuk dapat memenuhi kebutuhan kompetitif (*competitive necessity*) / kualifikasi pasar dari perindustriannya. Perusahaan dapat dikatakan memiliki ketergantungan terhadap informasi dan pengolahan informasi, di mana ini terlihat jelas pada sistem informasi berbasis komputer yang dimilikinya dalam menjalankan aktivitas operasionalnya sehari-hari, menjadikan arus data dan informasi berharga bagi keberlangsungan hidup perusahaan ini. Dari analisis atas penggunaan teknologi informasi dan penerapan sistem informasi, telah diuraikan serta diselidiki setiap sumber daya sistem informasi yang meliputi: sumber daya perangkat lunak, keras, jaringan, data, dan manusia, lalu aktivitas sistem informasi yang meliputi: masukan data, pengolahan data menjadi informasi, keluaran produk informasi, penyimpanan sumber data, dan pengendalian kinerja sistem. Serta sarana pendukung operasional untuk teknologi informasi dan sistem informasi ini. Dari sini didapatkan gambaran pada aset informasi yang dimiliki oleh perusahaan.
2. Berdasarkan gambaran atas aset informasi yang telah diperoleh, berikutnya adalah mengidentifikasi dan mengukur pengendalian keamanan yang diterapkan padanya melalui *gap analysis* Standar ISO 27001:2013, pada domain penelitian yang telah ditetapkan sebelumnya, sekaligus menjelaskan bentuk serta keadaan pengendalian keamanan ini. Sehingga dapat diperoleh hasil atas *gap analysis* ini sebagai berikut:
   a. (A.7.) *Human Resource Security* yang memiliki nilai rata-rata *capability maturity level* 1,16 atau berada pada *level* 1 (*Performed Informally*).
   b. (A.9.) *Access Control* yang memiliki nilai rata-rata *capability maturity level* 1,64 atau berada pada *level* 1 (*Performed Informally*).
   c. (A.11.) *Human Resource Security* yang memiliki nilai rata-rata *capability maturity level* 1,89 atau berada pada *level* 1 (*Performed Informally*).

3. Berdasarkan nilai rata-rata *capability maturity level* dari setiap domain penelitian ini, maka diperolehlah nilai rata-rata untuk ketiga domainnya adalah 1,56 atau berada pada *level* 1 (*Performed Informally*). Dari sini dilakukan analisis lanjut ke pengendalian keamanan pada ketiga domain penelitian secara komprehensif, sehingga diperoleh temuan atau rekomendasi yang bisa dipertimbangkan atau dikembangkan menjadi materi pembahasan dalam pelatihan dan sosialisasi untuk meningkatkan kesadaran keamanan informasi bagi karyawan perusahaan sebagai pengguna sistem informasi. Namun, secara garis besar perusahaan perlu menutup kesenjangan nilai di dalam *capability maturity level* ini dengan memasuki proses penerapan sistem pengendalian intern atau manajemen risiko keamanan informasi, untuk mencapai keamanan informasi yang ideal bagi perusahaan ke masa depan.

5.2. Saran

Berdasarkan kesimpulan yang diperoleh, berikut ini merupakan saran bagi perusahaan untuk menjadi pertimbangan ke masa depan, yakni:

1. Pada jangka waktu yang pendek, perusahaan dirasakan perlu untuk memperhatikan temuan atau rekomendasi pada sub bab 4.5., terkait dengan evaluasi pengendalian keamanan yang terdapat di perusahaan, di mana ini bisa dirumuskan sebagai materi untuk pelatihan dan sosialisasi sehingga dapat meningkatkan kesadaran keamanan informasi, berikut pemaparan temuan / rekomendasi ketiga domain secara singkat:
   a. (A.7.) *Human Resource Security*
      1) Perusahaan perlu mempertimbangkan untuk merancang perjanjian kerja yang eksplisit menjelaskan tanggung jawab dari keamanan informasi.
      2) Perusahaan dapat membentuk perilaku dan persepsi yang mendukung keamanan informasi dengan penghargaan pada karyawan yang selalu taat dan saat ada pelanggaran keamanan informasi yang serius, perusahaan bisa mengumumkan proses pendisiplinan ini ke semua karyawan dengan tujuan untuk menghilangkan perilaku dan persepsi yang tidak diinginkan.
      3) Perlunya kesepakatan tanggung jawab keamanan informasi yang tetap berlaku sesudah penghentian kerja dalam mengantisipasi penyalahgunaan atau kebocoran informasi penting saat ada karyawan yang berhenti bekerja atau diberhentikan oleh perusahaan.

b. (A.9.) *Access Control*
    1) Hak Akses yang dimiliki *supervisor* teknologi informasi dapat dikatakan tidak terbatas dalam sistem informasi perusahaan (berbeda dengan konteks hak akses yang dipegang pemilik perusahaan), sehingga perlu pengawasan.
    2) Perusahaan dapat menambah fungsi pemblokiran username dalam *login interface* apabila salah memasukkan *password* selama beberapa kali dan untuk membukanya bisa melapor ke supervisor teknologi informasi dahulu.
    3) Supervisor teknologi informasi perlu untuk memeriksa hak akses karyawan secara berkala.
    4) Untuk penggunaan informasi otentikasi rahasia, perusahaan nantinya dapat menerapkan peraturan untuk penggunaan karakter unik (satu angka, huruf besar, huruf kecil, dan karakter simbol serta tidak boleh informasi umum).
c. (A.11.) *Human Resource Security*
    1) Sebagai bentuk pengendalian detektif, CCTV juga dapat bekerja sebagai pengendalian preventif dengan memasang tanda "Area ini diawasi CCTV".
    2) Perusahaan dirasakan perlu menggunakan mesin penghancur kertas (*paper shredder*) sebelum membuang arsip penting atau berharga.
    3) Perlunya pencatatan untuk memantau perpindahan peralatan seperti *laptop*.
    4) Dengan teknologi yang semakin canggih, kini ada program aplikasi yang dapat dipasang pada *laptop* perusahaan untuk memantaunya lewat internet.

2. Pada jangka waktu yang panjang, dengan lingkungan bisnis di era informasi yang semakin dinamis dan kompleks disertai risiko dan ancaman keamanan informasi yang semakin berkembang pesat, perusahaan dirasakan perlu untuk berpedoman terhadap standar yang dikhususkan untuk membentuk sistem pengendalian intern / sistem manajemen keamanan informasi / tata kelola teknologi informasi untuk beradaptasi, mempertahankan kelangsungan hidup. Di mana memenuhi kebutuhan kompetitif serta memperhatikan risiko dan ancaman keamanan. Dari penelitian ini, yang berfokus terhadap Standar ISO/IEC 27001:2013, perusahaan nantinya dapat mengembangkan analisis lebih lanjut pada semua domain yang ada dalam Standar ISO/IEC 27001:2013, di mana pendekatannya bisa disamakan dengan pembahasan dari penelitian ini. Di mana ini akan membantu perusahaan ketika terdapat rencana penerapan sistem manajemen keamanan informasi, Standar ISO/IEC 27001:2013.

DAFTAR PUSTAKA

Abdussalam, M. S. (2016, January 13). *Aksi Kawanan Pencuri Spesialis Perkantoran Berakhir di Penjara Polres Bandung*. Diambil kembali dari TribunJabar.id: http://jabar.tribunnews.com/2016/01/13/aksi-kawanan-pencuri-spesialis-perkantoran-berakhir-di-penjara-polres-bandung

Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model For Nist Cyber Security Framework. *CS & IT-CSCP*, 51-62.

Bélanger, F., & Slyke, C. V. (2012). *Information Systems for Business, An Experiential Approach.* New York: John Wiley & Sons , Inc.

Blakley, B., McDermott, E., & Geer, D. (2002). Information security is information risk management. *New Security Paradigms Workshop* (hal. 97-104). New York: Association for Computing Machinery.

Candiwan. (2014). Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia. *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security* (hal. 50-58). Bandung: Faculty of Economic & Business, Telkom University.

Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. *Organizational, Legal, and Technological Dimensions of Information System Administrator*, 1-48.

COSO. (2013). Internal Control — Integrated Framework, Executive Summary. Washington, D.C.: Committee of Sponsoring Organizations of the Treadway Commission.

Firlia, V. (2014). *Audit Human Resources Security, Access Control, dan Physical And Environmental Security Pada Sistem Informasi PT. Taspen (Persero) KCU Bandung Menggunakan ISO 27001*. Bandung: Program Studi S1 Manajemen Bisnis Telekomunikasi dan Informatika - Fakultas Ekonomi dan Bisnis - Universitas Telkom.

Hall, J. A. (2011). *Accounting Information Systems, Seventh Edition.* Ohio: Cengage Learning.

Harris, S. (2005). *CISSP All-in-One Exam Guide, Sixth Edition.* New York: McGraw-Hill, Inc.

Hitchings, J. (1996). A practical solution to the complex human issues of information security design. Dalam S. K. Katsikas, & D. Gritzalis, *Information systems security: facing the information society of the 21st century* (hal. 3-12). London: Chapman & Hall, Ltd.

ISACA. (2009). *An Introduction to the Business Model for Information Security.* New York: Information Systems Audit and Control Association.

ISO/IEC 21827. (2008). *Information Technology - Security Techniques - Systems Security Engineering - Capability Maturity Model (SSE-CMM).* Switzerland: International Organization for Standardization & International Electrotechnical Commission.

ISO/IEC 27000. (2014). *Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary.* Switzerland: International Organization for Standardization & International Electrotechnical Commission.

ISO/IEC 27001. (2013). *Information Technology - Security Techniques - Information Security Management Systems - Requirements.* Switzerland: International Organization for Standardization & International Electrotechnical Commission.

ISO/IEC 27005. (2011). *Information Security Risk Management.* Switzerland: International Organization for Standardization & International Electrotechnical Commission.

Jucan, M. (2016, June 14). *ISO 27001: Five tips for successful implementation*. Diambil kembali dari IT Governance: https://www.itgovernance.co.uk/blog/iso-27001-five-tips-for-successful-implementation/

Kiyuna, A., & Conyers, L. (2015). *Cyberwarfare Sourcebook.* Morrisville: Lulu.com.

Kosutic, D. (2015, June 23). *ISO 27001 gap analysis vs. risk assessment*. Diambil kembali dari 27001 Academy: https://advisera.com/27001academy/knowledgebase/iso-27001-gap-analysis-vs-risk-assessment/

Laudon, K. C., & Laudon, J. P. (2014). *Management Information Systems: Managing the Digital Firm, Thirteenth Edition.* New Jersey: Pearson Education Limited.

Lumy, G. D. (2017, May 16). *Waspada Serangan Virus 'Wannacry' Jilid 2*. Diambil kembali dari tribunnews.com: http://www.tribunnews.com/nasional/2017/05/16/waspada-serangan-virus-wannacry-jilid-2?page=4

Marco, D. (2003, October 1). *Capability Maturity Model Part 2: Overview of the Six Levels*. Diambil kembali dari The Data Administration Newsletter: http://tdan.com/capability-maturity-model-part-2-overview-of-the-six-levels/5146

Menteri BUMN Republik Indonesia. (2013, Februari 18). Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara. *Peraturan Menteri BUMN Republik Indonesia nomor PER-02/MBU/2013*. Jakarta: Menteri BUMN Republik Indonesia.

Noor, J. (2016). *Metodologi Penelitian: Skripsi, Tesis, Disertasi & Karya Ilmiah.* Jakarta: Prenada Media.

O'Brien, J. A., & Marakas, G. M. (2011). *Management information systems, Tenth Edition.* New York: McGraw-Hill Irwin.

Ribot, J. C., & Peluso, N. L. (2003). A theory of Access. *Rural Sociology*, 153-181.

Romney, M. B., & Steinbart, P. J. (2015). *Accounting Information Systems, Thirteenth Edition.* London: Pearson Education Limited.

Sekaran, U., & Bougie, R. (2013). *Research Method for Business: A Skill Building Approach, Sixth Edition.* West Sussex: John Wiley & Sons Ltd.

Shah, B. (2016, January 12). *Pivot Point Security*. Diambil kembali dari ISO 27001 Gap Assessment and Risk Assessment: What’s the Difference?:

https://www.pivotpointsecurity.com/blog/difference-between-iso-27001-gap-assessment-risk-assessment/

Simkin, M. G., Norman, C. S., & Rose, J. M. (2012). *Core Concepts of Accounting Information Systems, Twelfth Edition.* United States of America: John Wiley & Sons.

Stewart, J. M., Chapple, M., & Gibson, D. (2015). *Certified Information Systems Security Professional Study Guide, Seventh Edition.* Indianapolis: John Wiley & Sons, Inc.

Sukma, E. L. (2013). *Evaluasi Manajemen Risiko Keamanan Informasi Sistem Provisioning Gateway Telkom Flexi.* Jakarta: Program Studi S2 Teknologi Informasi - Fakultas Ilmu Komputer - Universitas Indonesia.

Titchener, J. (2013, November 20). *Is implementing ISO27001 in an SME possible?* Diambil kembali dari IT Governance: https://www.itgovernance.co.uk/blog/is-implementing-iso27001-in-an-sme-possible/

U.S. Department of Homeland Security. (2013). *National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat.* Washington, D.C.: U.S. Department of Homeland Security.

Wardani, A. S. (2018, January 4). *Hacker Makin Ganas di 2018, Apa Jurus Badan Siber?* Diambil kembali dari Tekno Liputan 6: http://tekno.liputan6.com/read/3214427/headline-hacker-makin-ganas-di-2018-apa-jurus-badan-siber

Yusuf, O. (2017, May 13). *Rumah Sakit di Jakarta Disandera "Ransomware", Minta Tebusan Rp 4 Juta*. Diambil kembali dari Tekno Kompas: http://tekno.kompas.com/read/2017/05/13/13360257/rumah.sakit.di.jakarta.disandera.ransomware.minta.tebusan.rp.4.juta

Zaenudin, A. (2017, August 25). *Mudahnya Data-data Pribadi Dijual di Dunia Maya*. Diambil kembali dari tirto.id: https://tirto.id/mudahnya-data-data-pribadi-dijual-di-dunia-maya-cviZ