

## **BAB V**

### **KESIMPULAN & SARAN**

#### **5.1. Kesimpulan**

Berdasarkan pada Laporan Kinerja Instansi Pemerintah (LKjIP) Dinas Komunikasi dan Informatika Provinsi XYZ tahun 2020, instansi memiliki tingkat ketergantungan yang tinggi terhadap penggunaan sistem elektronik dalam melakukan proses bisnis nya. Pada penilaian dengan metode Indeks KAMI menunjukkan untuk tingkat kematangan sebesar 482 dan termasuk “Cukup Baik” dengan tingkat kematangan secara keseluruhan berada pada III+, tingkat tersebut menunjukkan jika penilaian sudah sedikit melampaui standar minimal yang ditetapkan ISO 27001. Aspek yang memiliki persentase pemenuhan dan tingkat kematangan terendah rendah jika dibandingkan dengan aspek lainnya adalah Pengelolaan Risiko Keamanan Informasi dengan Tingkat Kematangan pada tingkat I+ dengan total skor yang diperoleh sebesar 26.

Dalam penelitian dilakukan pada Diskominfo Provinsi XYZ, maka diperoleh 86 proses bisnis beserta dengan asetnya yang dimiliki atau dijalankan oleh 7 *Risk Owner*. Berdasarkan hasil dari kuesioner yang disebar kepada pihak instansi, maka ancaman/risiko yang dapat terjadi berjumlah 841 ancaman/risiko dengan 203 penyebab/kerawanan beserta dengan 119 dampak dari ancaman/risiko berdasarkan pada 86 Standar Operasional Prosedur (SOP) pada Diskominfo XYZ beserta dengan tingkat terjadinya dari risiko tersebut pada setiap proses bisnis. Ancaman/risiko yang didapatkan dapat disimpulkan dari permasalahan yang sering muncul adalah *human error*, *server down*, penyalahgunaan hak akses, *virus* dan sejenisnya, dan kebocoran data. Hasil penilaian yang dilakukan dengan metode Indeks KAMI versi 4.1 pada aspek Pengelolaan Risiko Keamanan Informasi masih belum ada perubahan dengan nilai 26 dan tingkat kematangan I+. Hal ini dikarenakan pihak instansi belum melakukan penganggaran dana untuk perbaikan pada Pengelolaan Risiko Keamanan Informasi, pada tahun 2020 pihak instansi masih berfokus pada perbaikan Kerangka

Kerja Keamanan Informasi yang masih memiliki nilai 104 dengan Tingkat Kematangan II yang tergolong masih rendah.

Rekomendasi perbaikan diberikan pada setiap 86 proses bisnis dengan kontrol pada ISO/IEC 27001:2013 sebagai pedoman rekomendasi perbaikan. Dari kontrol pada ISO/IEC 27001:2013 akan disesuaikan sesuai dengan kondisi dalam Dinas Komunikasi dan Informatika Provinsi XYZ. Berdasarkan pada hasil identifikasi risiko, ancaman/risiko yang paling banyak disebabkan oleh *human error*. Oleh karena itu, sebagian besar rekomendasi perbaikan tertuju pada perlu diberikannya pemahaman kepada staff atau karyawan tentang tanggung jawab atas tugasnya dan kesadaran tentang keamanan informasi sesuai pada Annex A.6.1.2, Annex A.7.1.2 dan Annex A.7.2.3 pada ISO/IEC 27001:2013.

## 5.2. Saran

Berdasarkan pada hasil penelitian yang sudah diadaptkan. Maka akan dijabarkan beberapa saran untuk perbaikan antara lain:

1. Perlu diberikan pemahaman dan sosialisasi kepada staf dan karyawan terkait dengan kesadaran dan kedisiplinan terkait keamanan informasi
2. Dilakukan penjelasan terkait tugas dan tanggung jawab setiap bidang sesuai dengan *job desk* yang bertujuan meminimalisir penggunaan tidak sah, penyalahgunaan secara sengaja maupun tidak sengaja, dan penyalahgunaan aset dalam instansi.
3. Dilakukannya pengesahan terhadap dokumen Kebijakan dan Prosedur Manajemen Risiko SMKI.
4. Penelitian dapat dilakukan dengan menggunakan metode yang telah mengalami pembaruan baik Indeks KAMI atau ISO 27001.
5. Dapat direalisasikannya perbaikan pada aspek Pengelolaan Risiko Keamanan Informasi jika sudah dilakukan penganggaran perbaikan.



## DAFTAR PUSTAKA

- [1] Asmawi, Syafei, and M. Yamin, "PENDIDIKAN BERBASIS TEKNOLOGI INFORMASI DAN KOMUNIKASI," in *PROSIDING SEMINAR NASIONAL PENDIDIKAN PROGRAM PASCASARJANA UNIVERSITAS PGRI PALEMBANG 03 MEI 2019*, 2019.
- [2] I Putu Setyo Syahindra, Clara Hetty Primasari, and Aloysius Bagas Pradipta Irianto, "EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005 : 2011," *JURNAL TEKNOINFO*, vol. 16, pp. 165–182, 2022.
- [3] PRESIDEN REPUBLIK INDONESIA, *PERATURAN PRESIDEN REPUBLIK INDONESIA NOMOR 95 TAHUN 2018 TENTANG SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK*. 2018.
- [4] KEPALA LEMBAGA SANDI NEGARA, *PERATURAN KEPALA LEMBAGA SANDI NEGARA NOMOR 7 TAHUN 2017 TENTANG PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAHAN DAERAH PROVINSI DAN KABUPATEN/KOTA*. 2017.
- [5] GUBERNUR XYZ, *PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI XYZ*. 2018.
- [6] DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI XYZ, "PROFIL DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI XYZ," *Dinas Komunkasi dan Informatika Provinsi XYZ*. <https://diskominfo.xyz.go.id/2019/profil-dinas/> (accessed Nov. 04, 2022).
- [7] DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI XYZ, "LAPORAN KINERJA INSTANSI PEMERINTAH," 2020.
- [8] MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA, *PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA NOMOR 7 TAHUN 2018 TENTANG PELAYANAN PERIZINAN BERUSAHA TERINTEGRASI SECARA ELEKTRONIK BIDANG KOMUNIKASI DAN INFORMATIKA*. 2018.

- [9] S. Nurul, S. Anggrainy, and S. Aprelyani, “FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM),” *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.
- [10] D. Ciptaningrum, E. Nugroho, and D. Adhipta, “AUDIT KEAMANAN SISTEM INFORMASI PADA KANTOR PEMERINTAH KOTA YOGYAKARTA MENGGUNAKAN COBIT 5,” in *Seminar Nasional Teknologi Informasi dan Komunikasi*, 2015. [Online]. Available: [www.iso.org](http://www.iso.org).
- [11] P. Ferdiansyah, S. Subektiningsih, and R. Indrayani, “Evaluasi Tingkat Kesiapan Keamanan Informasi Pada Lembaga Pendidikan Menggunakan Indeks Kami 4.0,” *Mobile and Forensics*, vol. 1, no. 2, pp. 53–62, Sep. 2019, doi: 10.12928/mf.v1i2.1001.
- [12] M. Utomo, A. H. N. Ali, and I. Affandi, “Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I,” *JURNAL TEKNIK ITS*, vol. 1, no. 1, 2012.
- [13] M. Rizaldi Seputra, G. Ramadhan, T. Nur Hafizah Hersyaf, A. Nur Rokhman, J. H. Ir Juanda nomor, and K. Tangerang Selatan, “PENTINGNYA IMPLEMENTASI ISO 27001 DALAM MANAJEMEN KEAMANAN : SISTEMATIKA REVIEW,” 2017.
- [14] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” *Journal of Information Security*, vol. 04, no. 02, pp. 92–100, 2013, doi: 10.4236/jis.2013.42011.
- [15] Amazon, “ISO/IEC 27001:2013.” <https://aws.amazon.com/id/compliance/iso-27001-faqs/#:~:> (accessed Dec. 22, 2022).
- [16] N. Rochmania, “ANALISIS TREN PENGGUNAAN FRAMEWORK COBIT, ITIL, DAN ISO 27001 PADA PENELITIAN DI INDONESIA,” Surabaya, 2019.
- [17] M. I. Rosadi and L. Hakim, “PENGUKURAN DAN EVALUASI KEAMANAN SIAKAD UNIVERSITAS YUDHARTA MENGGUNAKAN INDEKS KAMI,” *Explore IT*, vol. 7, no. 1, 2015.
- [18] N. Diva Ramadhani, W. Hayuhardhika Nugraha Putra, and A. Dwi Herlambang, “Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi),” *Jurnal Pengembangan*

- Teknologi Informasi dan Ilmu Komputer*, vol. 4, no. 5, pp. 1490–1498, 2020, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [19] Administrator, “APA ITU INDEKS KAMI (KEAMANAN INFORMASI),” *Kawasan Pusat Pemerintahan Provinsi Banten (KP3B)*, Jun. 24, 2022. <https://csirt.bantenprov.go.id/portal/articles/read/apa-itu-indeks-kami-keamanan-informasi> (accessed Nov. 04, 2022).
- [20] Muh. Faturachman Husin, Hans F Wowor, and Stanley D.S. Karouw, “Implementasi Indeks KAMI di Universitas Sam Ratulangi,” *E-Journal Teknik Informatika*, vol. 12, no. 1, 2017.
- [21] F. Mahardika, “Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang),” *Jurnal Pengembangan IT (JPIT)*, vol. 02, no. 02, 2017.
- [22] T. A. Megawati, H. M. Astuti, and A. Herdiyanti, “PENGELOLAAN RISIKO ASET TEKNOLOGI INFORMASI PADA PERUSAHAAN PROPERTI PT XYZ, TANGERANG BERDASARKAN KERANGKA KERJA COBIT 4.1,” in *Seminar Nasional Sistem Informasi Indonesia*, 2014.
- [23] G. Setyadi and Y. Kusumawati, “Mitigasi Risiko Aset Dan Komponen Teknologi Informasi Berdasarkan Kerangka Kerja OCTAVE Dan FMEA Pada Universitas Dian Nuswantoro,” *Journal of Information System*, 2016.
- [24] M. Lenawati, W. Wahyu Winarno, and A. Amborowati, “Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5,” CDRUM, 2017.
- [25] Tami, “Apa yang Dimaksud dengan ISO 27001 Sistem Manajemen Keamanan Informasi,” *Mutu Institute*, Oct. 27, 2021. <https://mutuinstitute.com/post/iso-27001-sistem-manajemen-keamanan-informasi/> (accessed Dec. 22, 2022).
- [26] Firzah A Basyarahil, Hanim Maria Astuti, and Bekti Cahyo Hidayanto, “Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya,” *JURNAL TEKNIK ITS*, vol. 6, 2017.
- [27] S. Indah Dwi Octaviani and A. Dwi Herlambang, “Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Batu Dengan

- Menggunakan Indeks KAMI,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 3, pp. 2741–2745, 2019, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [28] N. Matondang, I. Nurlaili Isnainiyah, and A. Muliawati, “Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ),” *JURNAL RESTI*, vol. 2, no. 1, pp. 282–287, 2018, [Online]. Available: <http://jurnal.iaii.or.id>
- [29] E. Barlian, *METODOLOGI PENELITIAN KUALITATIF & KUANTITATIF*. Sukabina Press, 2016.
- [30] R. Bernardino, “ISO 27001 ver 2013,” *ResearchGate*, Feb. 2021. [https://www.researchgate.net/publication/349366608\\_ISO\\_27001\\_ver\\_2013](https://www.researchgate.net/publication/349366608_ISO_27001_ver_2013) (accessed Dec. 22, 2022).

