



Analisis Risiko dan Kontrol Perlindungan Data Pribadi pada Sistem Informasi Administrasi Kependudukan

Iqbal Santosa¹, Raras Yusvinindya²

^{1,2}Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

¹iqbals@telkomuniversity.ac.id, ²ayasnindya@student.telkomuniversity.ac.id

Abstract

Sistem Informasi Administrasi Kependudukan (SIK) is an application used in managing personal data of residents in all cities/districts in Indonesia. Personal data becomes the public attention because if it is not managed properly it will have an impact on one's legal protection and non-compliance with regulations, i.e. Permenkominfo Nomor 20 tahun 2016 about Protection of Personal Data in the Electronic System. Risk analysis and control of personal data protection on SIK applications are needed so that the personal data management can be carried out properly and comply with regulatory requirements. Data collected for this study are primary data, sourced from direct observations on the application, interview about assets related to SIK along with possible risks, and also internal organizations documents. Data analysis was performed with a risk analysis using the ISO 31000: 2018 risk management process approach, where the identification of relevant risks refers to the Generic Risk Scenarios COBIT 5 For Risk, and the determination of relevant controls refers to the Department of Defense Instruction 8500.2 and NIST 800-53. This research involves the Head of Department and employees of Disdukcapil XYZ City that are related to the strategic and operational aspects of SIK. The results of this study are the identification of 23 possible risks that are spread over 5 processes of personal data protection that classified into the medium-high risk level, and proposed risk control consisting of 19 preventive controls, 6 detective controls, and 2 corrective control.

Keywords: Data Protection, ISO 31000, Personal Data Protection, Sistem Informasi Administrasi Kependudukan, SIK

Abstrak

Sistem informasi Administrasi Kependudukan (SIK) merupakan aplikasi yang digunakan dalam mengelola data pribadi penduduk di seluruh kota/kabupaten di Indonesia. Data pribadi ini menjadi sorotan publik karena jika tidak dikelola dengan baik maka akan berdampak pada perlindungan hukum seseorang dan tidak terpenuhinya persyaratan dalam regulasi, yakni Permenkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Analisis risiko dan kontrol perlindungan data pribadi pada aplikasi SIK diperlukan sehingga pengelolaan data pribadi dapat dilakukan dengan baik dan sesuai dengan ketentuan regulasi. Data yang dikumpulkan untuk penelitian ini berupa data primer, yang bersumber dari pengamatan langsung pada aplikasi, wawancara mengenai aset terkait SIK beserta risiko yang mungkin terjadi, dan juga dokumen internal organisasi. Analisis data dilakukan dengan analisis risiko menggunakan pendekatan proses manajemen risiko ISO 31000:2018, dimana identifikasi risiko yang relevan mengacu pada *Generic Risk Scenarios COBIT 5 For Risk*, serta penentuan kontrol yang relevan mengacu pada *Department of Defense Instruction 8500.2* dan *NIST 800-53*. Penelitian ini melibatkan Kepala Dinas serta pegawai Disdukcapil Kota XYZ yang terkait dengan aspek strategis dan operasional dari SIK. Hasil dari penelitian ini ialah teridentifikasinya 23 kemungkinan risiko yang tersebar pada 5 proses perlindungan data pribadi yang tergolong dalam tingkat risiko sedang-tinggi, dan usulan kontrol risiko yang terdiri dari 19 kontrol preventif, 6 kontrol detektif, dan 2 kontrol korektif.

Kata kunci: Data Pribadi, ISO 31000, Perlindungan Data Pribadi, Sistem Informasi Administrasi Kependudukan, SIK

© 2019 Jurnal RESTI

1. Pendahuluan

Perkembangan teknologi memberikan dampak yang besar bagi kehidupan sosial. Terutama kontribusinya dalam kemudahan penyebaran informasi. Hal ini dapat menciptakan ancaman terhadap privasi dengan memberikan peluang besar bagi pihak yang memiliki akses ke informasi tersebut [1].

Data pribadi terbagi dalam dua jenis yaitu data pribadi biasa dan sensitif. Data pribadi umum adalah data yang berhubungan dengan kehidupan seseorang yang dapat diidentifikasi baik secara otomatis ataupun berdasarkan kombinasi dengan informasi lain seperti nama, nomor passport, foto, video, surat elektronik, sidik jari dan lain-lain. Sementara data pribadi sensitif diartikan sebagai data pribadi yang meliputi: agama/kepercayaan, kondisi kesehatan, kondisi fisik dan mental, kehidupan seksual, data keuangan pribadi, dan lain – lain [2].

Ancaman penyalahgunaan data pribadi di Indonesia menjadi kian mengemuka terutama sejak pemerintah menggulirkan program KTP elektronik (e-KTP) yang merupakan program perekaman data pribadi oleh pemerintah. Data pribadi yang terekam dalam e-KTP rawan disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab, terutama apabila pengamanannya kurang [3]. Kehadiran program e-KTP pada tahun 2011 ini serta integrasinya dengan beberapa instansi seperti perbankan dan lembaga keuangan, membuat semakin tingginya potensi dari pelanggaran data dan informasi pribadi [2].

Menanggapi hal ini, Pemerintah telah mengeluarkan beberapa regulasi terkait perlindungan data pribadi diantaranya pada UU No 23 Tahun 2006 tentang Administrasi Kependudukan pasal 84 ayat (1) dan Pasal 85 bahwa negara berkewajiban untuk memberi perlindungan data pribadi untuk setiap penduduk; UU No 19 Tahun 2016 tentang perubahan atas UU No 11 Tahun 2008 tentang Informasi Transaksi Elektronik Pasal 26 ayat (1) bahwa dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*); Permendagri No 25 Tahun 2011 tentang Pedoman Pengkajian, Pengembangan dan Pengelolaan Sistem Informasi Administrasi Kependudukan; Permenkominfo No 4 Tahun 2016 Pasal 1 ayat (7) tentang Sistem Manajemen Pengamanan Informasi data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiannya; serta Permenkominfo No 20 Tahun 2016 tentang Perlindungan Data Pribadi bahwa terdapat lima proses tentang perlindungan data pribadi yaitu Perolehan, pengolahan, penyimpanan dan penyebarluasan serta pemanfaatan data pribadi[4].

Penelitian terkait analisis risiko pada suatu aplikasi menggunakan ISO 31000 telah banyak dilakukan, diantaranya penelitian yang berjudul Analisis Risiko

Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS. Penelitian ini berfokus pada aplikasi untuk pengelolaan sumber daya manusia pada sebuah perusahaan [5].

Terdapat penelitian lain terkait analisis risiko pada suatu proses seperti pada penelitian yang berjudul Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan XYZ Melalui Kombinasi COBIT, PMBOK, dan ISO 31000. Sebelum pengelolaan risiko pada penelitian ini dilakukan, ditentukan standar maupun kerangka kerja yang akan digunakan pada setiap tahapan terlebih dahulu melalui proses komparasi. COBIT 5 dalam hal ini digunakan dalam tahapan identifikasi risiko dan pemilihan kontrol penanganan risiko. Sedangkan ISO 31000 digunakan dalam tahapan perencanaan manajemen risiko, analisis risiko, perencanaan penanganan risiko, serta pemantauan dan pengendalian risiko [6].

Berdasarkan ulasan tersebut, belum terdapat penelitian yang menggabungkan penggunaan ISO 31000:2018 sebagai tahapan proses analisis risiko, juga *Generic Risk Scenarios* COBIT 5 dalam identifikasi risiko, serta penggunaan standar tertentu dalam pemilihan kontrol penanganan risiko seperti Department of Defense Instruction 8500.2 dan NIST 800-5. Tahapan proses analisis risiko yang digunakan dalam penelitian sebelumnya belum sepenuhnya sesuai dengan tahapan yang ada pada ISO 31000. Selain itu, aplikasi maupun proses yang dipilih sebagai objek penelitian belum memiliki dampak yang cukup luas karena berfokus pada satu aplikasi atau proses di suatu perusahaan.

Penelitian yang dilakukan ini akan sangat membantu dalam pengelolaan data pribadi di Indonesia karena Sistem Informasi Administrasi Kependudukan (SIAK) tak hanya digunakan untuk mengelola data pribadi penduduk di suatu kota/kabupaten tertentu akan tetapi seluruh kota/kabupaten di Indonesia. Harapannya dengan diterapkannya kontrol yang dihasilkan dari penelitian ini maka pengelolaan data pribadi dapat dilakukan dengan baik dan sesuai dengan ketentuan regulasi.

2. Metode Penelitian

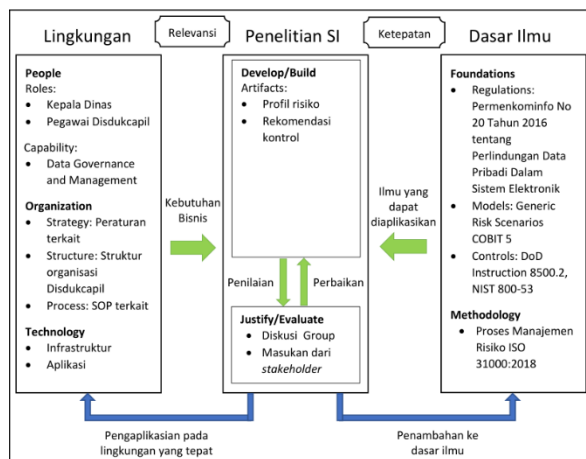
Untuk membantu dalam melakukan pemetaan kondisi lingkungan organisasi yang menjadi objek penelitian serta teori-teori relevan yang digunakan dalam penelitian maka digunakan model konseptual yang mengadopsi *Information System Research Framework*. Model konseptual ini dibagi menjadi 3 bagian yaitu lingkungan, penelitian SI dan dasar ilmu[7]. Model konseptual pada penelitian ini ada di Gambar 1.

Berikut penjelasan dari model konseptual tersebut.

1. Lingkungan penelitian terdiri dari orang, organisasi dan teknologi. Terkait orang, akan melibatkan Kepala Dinas dan pegawai. Terkait

organisasi akan mengacu pada dokumen strategi (peraturan terkait), struktur organisasi, dan proses-proses (SOP terkait). Terkait teknologi akan berhubungan dengan infrastruktur dan aplikasi yang ada pada organisasi.

2. Penelitian SI terdiri dari dua proses yaitu pengembangan/penyusunan dan justifikasi/evaluasi. Pengembangan/penyusunan dalam hal ini ialah artifak yang berbentuk profil risiko dan rekomendasi kontrol yang kemudian dilakukan justifikasi/evaluasi melalui diskusi grup dan masukan dari *stakeholder*.
3. Dasar ilmu terdiri dari dua, yaitu dasar dan metodologi penelitian. Hal yang menjadi dasar ialah regulasi yakni Permenkominfo No 20 Tahun 2016, model *Generic Risk Scenarios* pada COBIT 5 For Risk[8], serta kontrol pada Department of Defense Instruction 8500.2^[7] dan NIST 800-53[10]. Metodologi yang digunakan ialah proses manajemen risiko menggunakan standar ISO 31000:2018.



Gambar 1 Model Konseptual Penelitian

Data yang dikumpulkan untuk penelitian ini sepenuhnya berupa data primer, yang bersumber dari pengamatan langsung pada aplikasi SIAK, wawancara mengenai aset terkait SIAK beserta risiko yang mungkin terjadi, juga dokumen internal organisasi. Data kemudian dianalisis sesuai dengan proses manajemen risiko mengacu pada ISO 31000:2018 yang mencakup: pendefinisian ruang lingkup, konteks dan kriteria; penilaian risiko yang meliputi identifikasi risiko, analisis risiko dan evaluasi risiko; dan terakhir penanganan risiko[11]. Kriteria risiko yang digunakan dalam tahap penentuan kriteria risiko mengacu pada Keputusan Menteri Keuangan No. 845/KMK.01/2016 tentang Petunjuk Pelaksanaan Manajemen Risiko di Lingkungan Kementerian Keuangan [12]. Regulasi ini dipilih karena Kementerian Keuangan merupakan instansi pemerintah yang paling awal mengeluarkan aturan terkait manajemen risiko sekaligus paling awal dalam penerapannya. Dari 6 area dampak yang

disebutkan pada regulasi tersebut, area dampak yang dipilih hanya terkait gangguan terhadap layanan organisasi di level eselon II mengingat jabatan Kepala Dinas berada pada level eselon II. Penentuan nilai tingkat kejadian dan tingkat dampak pada tahap analisis risiko dilakukan dengan metode wawancara. Penanganan risiko yang dilakukan pada penelitian ini berhenti di tahap persiapan rencana penanganan risiko, dan tidak sampai ke tahap implementasi.

3. Hasil dan Pembahasan

3.1 Tahap Pendefinisian Ruang Lingkup, Konteks dan Kriteria

3.1.1 Pendefinisian Ruang Lingkup

Dilakukan pendefinisian ruang lingkup aset yang memiliki risiko dan/atau menjadi kontrol dalam proses perlindungan data pribadi pada aplikasi SIAK Kota XYZ sebagaimana pada Tabel 1.

Tabel 1. Identifikasi Aset

Komponen	Kode	Aset
Data dan Informasi	AS01	Rencana strategis organisasi
	AS02	Kebijakan organisasi
	AS03	Data pribadi pegawai
	AS04	Rekaman pelatihan pegawai
	AS05	Perjanjian kerja pegawai
	AS06	Kontrak kerja pihak ketiga
	AS07	Dokumentasi regulasi terkait
	AS08	Dokumentasi operasional
	AS09	Laporan bulanan
	AS10	Laporan triwulan
	AS11	Laporan tahunan
Perangkat Lunak	AS12	Aplikasi Sistem Informasi Administrasi Kependudukan (SIAK)
	AS13	Aplikasi Pemutakhiran
	AS14	Aplikasi Konsolidasi
	AS15	Aplikasi Dellica
	AS16	Aplikasi Pencarian Biometrik
	AS17	Situs Web Pemerintahan
	AS18	Intranet
	AS19	Mail server
	AS20	Windows 10 Operating System
	AS21	Microsoft Office Suite
Perangkat Keras	AS22	Server
	AS23	Laptop
	AS24	Desktop
	AS25	Printer
	AS26	CD-ROM
	AS27	Flash Disk
	AS28	Telepon

3.1.2 Identifikasi Konteks Organisasi

Diperlukan pemahaman yang memadai mengenai konteks organisasi yang menjadi objek penelitian. Gambaran umum mengenai konteks internal dan eksternal organisasi terdapat pada tabel 2.

3.1.3 Penentuan Kriteria Risiko

Sebelum risiko dapat dinilai, perlu ditentukan terlebih dahulu kriteria yang akan digunakan dalam penilaian

risiko. Diantaranya ialah tingkat kejadian risiko pada Tabel 3, tingkat dampak risiko pada Tabel 4, serta matriks risiko pada Tabel 5.

Tabel 2. Konteks Internal dan Eksternal

Konteks	Komponen	Dokumen Terkait
Internal	Visi, misi, strategi, sasaran, dan kebijakan	Rencana Pembangunan Jangka Menengah Daerah Kota XYZ Tahun 2017-2022
	Struktur organisasi, peran dan tanggung jawab	Perwal Kota XYZ Nomor 33 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Perangkat Daerah Kota XYZ
	Kemampuan (sumber daya & pengetahuan), hubungan dengan <i>stakeholder</i> internal	Laporan Kinerja Instansi Pemerintah (LKIP) Kota XYZ Tahun 2018, Peraturan Daerah Kota XYZ Nomor 8 Tahun 2014 tentang Penyelenggaraan Administrasi Kependudukan di Kota XYZ, SOP Pendaftaran Penduduk, SOP Pencatatan Sipil, SOP Sekretariat
	Komitmen kontraktual	Perjanjian Kerja Pegawai
Eksternal	Persyaratan hukum dan peraturan	UU No 23 Tahun 2006 tentang Administrasi Kependudukan, UU No 19 tahun 2016 tentang Perubahan atas UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pemendagri No 25 tahun 2011 tentang Pedoman Pengkajian, Pengembangan dan Pengelolaan Sistem Informasi Administrasi Kependudukan, Permenkominfo No 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, Permenkominfo No 20 Tahun 2016 tentang Perlindungan Data Pribadi
	Hubungan dengan <i>stakeholder</i> eksternal	Kontrak Kerja Pihak Ketiga

Tabel 3. Kriteria Tingkat Kejadian

Nilai	Kejadian	Frekuensi
1	Hampir tidak terjadi	< 2 kali dalam 1 tahun
2	Jarang terjadi	2-5 kali dalam 1 tahun
3	Kadang terjadi	6-9 kali dalam 1 tahun
4	Sering terjadi	10-12 kali dalam 1 tahun
5	Hampir pasti terjadi	> 12 kali dalam 1 tahun

Tabel 4. Kriteria Tingkat Dampak

Nilai	Dampak	Deskripsi
1	Tidak signifikan	$x < 10\%$ dari jam operasional layanan harian
2	Minor	$10\% \leq x < 25\%$ dari jam operasional layanan harian
3	Moderat	$25\% \leq x < 50\%$ dari jam operasional layanan harian
4	Signifikan	$50\% \leq x < 65\%$ dari jam operasional layanan harian
5	Sangat signifikan	$x \geq 65\%$ dari jam operasional layanan harian

Matriks risiko yang menjadi acuan organisasi dalam pengelolaan risiko terdapat pada Tabel 5 yakni matriks 5x5 dimana terdapat 5 tingkat kejadian (*likelihood*) dan 5 tingkat dampak (*impact*), serta dihasilkan 3 tingkat risiko yakni rendah (*low*), sedang (*medium*), dan tinggi (*high*).

Tabel 5. Matriks Risiko

Kejadian (Likelihood)	Dampak (Impact)				
	1 Tidak signifikan	2 Minor	3 Moderat	4 Signifikan	5 Sangat Signifikan
1 Hampir tidak terjadi	LOW	LOW	LOW	LOW	MED
2 Jarang terjadi	LOW	LOW	MED	MED	MED
3 Kadang terjadi	LOW	MED	MED	HIGH	HIGH
4 Sering terjadi	LOW	MED	HIGH	HIGH	HIGH
5 Hampir pasti terjadi	MED	MED	HIGH	HIGH	HIGH

3.2 Tahap Penilaian Risiko

3.2.1 Identifikasi Risiko

Tahapan identifikasi risiko dilakukan dengan melakukan identifikasi kemungkinan risiko dan dampaknya terhadap organisasi.

3.2.1.1 Identifikasi Kemungkinan Risiko

Kemungkinan risiko diidentifikasi pada setiap proses perlindungan data pribadi yang harus dilakukan oleh organisasi. Daftar kemungkinan risiko dijelaskan pada Tabel 6.

Tabel 6. Identifikasi Kemungkinan Risiko Pada Proses Perlindungan Data Pribadi

No	Proses	Kode	Kemungkinan Risiko
1	Perolehan dan Pengumpulan	0504	Adanya kesalahan input informasi oleh staf TI atau pengguna sistem TI
		1201	Adanya ketidakpatuhan dengan regulasi/ aturan yang ada
2	Pengolahan dan Penganalisisan	0601	Komponen perangkat keras rusak, menyebabkan kerusakan data secara parsial oleh staf internal
		0602	Database rusak, menyebabkan data tidak dapat diakses
		0606	Informasi sensitif sengaja terekspos karena kesalahan dalam mengikuti panduan penanganan informasi
		0802	Sistem tidak dapat menangani banyaknya transaksi saat volume pengguna meningkat
3	Penyimpanan	0902	Penggunaan perangkat lunak yang masih belum matang
		0603	Media <i>portable</i> yang berisi data sensitif hilang/ terekspos ke publik
		0604	Data sensitif hilang/ terekspos,

No	Proses	Kode	Kemungkinan Risiko
			karena <i>logical attack</i>
		0605	Media <i>backup</i> hilang
		0609	Informasi sensitif terungkap karena tidak efisien dalam mempertahankan/ mengarsip/ membuang informasi
		1602	Gangguan akibat serangan DoS
		1605	Adanya serangan virus
		1901	Adanya gempa bumi
		1903	Adanya badai besar
		1904	Adanya kebakaran
		1905	Adanya banjir
		1906	Batas air sungai meningkat
4	Penampilan, Pengumuman, Pengiriman, Penyebarluasan, dan/atau Pembukaan Akses	0902	Penggunaan perangkat lunak yang masih belum matang
		1601	Staf yang tidak berwenang mencoba masuk ke sistem
		1603	Adanya kerusakan pada <i>website</i>
5	Pemusnahan	0609	Informasi sensitif terungkap karena tidak efisien dalam mempertahankan/ mengarsip/ membuang informasi

3.2.1.2 Identifikasi Kemungkinan Dampak

Dilakukan identifikasi kemungkinan dampak yang mungkin ditimbulkan dari risiko yang mungkin terjadi. Daftar kemungkinan dampak terdapat pada Tabel 7.

Tabel 7. Identifikasi Kemungkinan Dampak Pada Proses Perlindungan Data Pribadi

No	Proses	Kode	Kemungkinan Dampak
1	Perolehan dan Pengumpulan	0504	Data pribadi masyarakat menjadi data anomali
		1201	Tidak sesuai dengan standar yang berlaku
2	Pengolahan dan Penganalisisan	0601	Tidak dapat mengolah data pribadi dengan baik
		0602	Terhambat dalam melakukan pengolahan data
		0606	Kurangnya kepercayaan masyarakat terhadap perlindungan data pribadi
		0802	Pengolahan data pribadi menjadi terhambat
		0902	Terhambat dalam melakukan pengolahan data
3	Penyimpanan	0603	Data dapat disalahgunakan untuk tindakan kejahatan
		0604	Kurangnya kepercayaan masyarakat terhadap perlindungan data pribadi
		0605	Data pribadi hilang
		0606	Data dapat disalahgunakan untuk tindakan kejahatan
		1602	Data pribadi tidak dapat diakses sehingga operasional terhambat
		1605	Data pribadi tidak dapat diakses sehingga operasional terhambat

No	Proses	Kode	Kemungkinan Dampak
		1901	Infrastruktur rusak atau hilang
		1903	Infrastruktur rusak atau hilang
		1901	Infrastruktur rusak atau hilang
		1905	Infrastruktur rusak atau hilang
		1906	Infrastruktur rusak atau hilang
4	Penampilan, Pengumuman, Pengiriman, Penyebarluasan, dan/atau Pembukaan Akses	0902	Terhambat dalam melakukan proses penampilan, pengumuman dan penyebarluasan data pribadi
		1601	Dapat terjadi tindakan kejahatan
		1603	Data pribadi tidak dapat diakses sehingga terhambatnya proses operasional
5	Pemusnahan	0609	Informasi dapat disalahgunakan sehingga tingkat reputasi menurun

3.2.2 Analisis Risiko

Dilakukan analisis penilaian terhadap kemungkinan risiko yang terjadi. Penilaian dilakukan dengan menentukan tingkat kejadian dan tingkat dampak pada risiko yang sudah diidentifikasi sebelumnya pada Tabel 7, dengan acuan kriteria pada Tabel 3. dan Tabel 4.

Tabel 8. Tabel Analisis Risiko

No	Proses	Kode	Likelihood	Impact
1	Perolehan dan Pengumpulan	0504	3	3
		1201	2	5
2	Pengolahan dan Penganalisisan	0601	1	5
		0602	3	5
		0606	5	4
		0802	2	3
		0902	1	5
3	Penyimpanan	0603	2	5
		0604	2	5
		0605	2	5
		0609	3	5
		1602	2	5
		1605	2	5
		1901	1	5
		1903	1	5
		1904	1	5
		1905	2	5
		1906	1	5
4	Penampilan, Pengumuman, Pengiriman, Penyebarluasan, dan/atau Pembukaan Akses	0902	2	5
		1601	3	5
		1603	1	5
5	Pemusnahan	0609	3	5

3.2.3 Evaluasi Risiko

Dilakukan evaluasi risiko dengan menentukan tingkat risiko yang terjadi pada organisasi mengacu pada matriks risiko di Tabel 5. Tabel 9 berikut menunjukkan tingkat risiko pada setiap kemungkinan risiko yang ada di organisasi, diurutkan berdasarkan tingkat risiko yang paling tinggi hingga paling rendah di setiap prosesnya.

Tabel 9. Tabel Evaluasi Risiko

No	Proses	Kode	Level of risk
1	Perolehan dan Pengumpulan	1201 0504	Medium Medium
2	Pengolahan dan Penganalisisan	0606 0602 0802 0601 0902	High High Medium Medium Medium
3	Penyimpanan	0609 0603 0604 0605 1602 1605 1905 1901 1903 1904 1906	High Medium Medium Medium Medium Medium Medium Medium Medium Medium Medium
4	Penampilan, Pengumuman, Pengiriman, Penyebarluasan, dan/atau Pembukaan Akses	1601 0902 1603	High Medium Medium
5	Pemusnahan	0609	High

3.3 Tahap Penanganan Risiko

Berdasarkan hasil evaluasi risiko diperoleh bahwa risiko terkait proses perlindungan data pribadi masuk dalam tingkat sedang-tinggi sehingga opsi penanganan risiko yang dipilih ialah *mitigate* dengan cara menghilangkan sumber risiko, mengubah tingkat kejadian, dan mengubah tingkat dampak. Usulan penanganan dalam hal ini berupa pemilihan kontrol yang perlu diterapkan dimana terbagi dalam tiga tipe yakni preventif, detektif, dan korektif seperti pada Tabel 10.

Tabel 10. Tabel Kontrol Penanganan Risiko

Kode	Kemungkinan Risiko	Nomor/ Judul Kontrol/ Kontrol
Proses Perolehan dan Pengumpulan		
1201	Adanya ketidakpatuhan dengan regulasi/ aturan yang ada	AT-1 Security Awareness and Training Policy and Procedures <u>Preventif</u> Menyusun, mendokumentasikan, dan menyebarluaskan: 1. Kebijakan mengenai kesadaran dan pelatihan keamanan 2. Prosedur untuk memfasilitasi implementasi kebijakan tersebut
0504	Adanya kesalahan input informasi oleh staf TI atau pengguna sistem TI	SI-10 Information input validation <u>Preventif</u> Mengecek validitas informasi yang dimasukkan, dengan bantuan sistem informasi
Proses Pengolahan dan Penganalisisan		
0606	Informasi sensitif sengaja terekspos karena kesalahan dalam mengikuti	PE-2 Physical Access Authorization <u>Preventif</u> 1. Menyusun, menyetujui, mengelola daftar individu yang diberikan
Proses Penyimpanan		
0602	Database rusak, menyebabkan data tidak dapat diakses	CODB-3 Data backup Procedures <u>Preventif</u> Pencadangan data dilakukan dengan memelihara sistem sekunder cadangan, tidak <i>co-located</i> (dalam satu lokasi yang sama), yang dapat diaktifkan (sewaktu-waktu) tanpa menyebabkan kehilangan data atau gangguan operasional.
0802	Sistem tidak dapat menangani banyaknya transaksi saat volume pengguna meningkat	AC-10 Concurrent Session Control <u>Preventif</u> Sistem informasi membatasi jumlah sesi bersamaan untuk setiap tipe akun tertentu
0601	Komponen perangkat keras rusak, menyebabkan kerusakan data secara parsial oleh staf internal	PE-3 Physical Access Control <u>Preventif</u> 1. Menyusun, menyetujui, mengelola daftar individu yang diberikan kewenangan akses fisik (terhadap fasilitas dimana sistem informasi berada) 2. Menerapkan otorisasi akses fisik dengan: a. Memverifikasi kewenangan akses fisik individu sebelum dibolehkan mengakses fasilitas b. Mengontrol keluar/masuk fasilitas dengan menggunakan sistem/perangkat 3. Memelihara catatan akses fisik (<i>audit log</i>) 4. Menyediakan penjaga untuk mengontrol akses fisik 5. Mendampingi pengunjung dan memantau aktivitasnya 6. Mengamankan kunci akses fisik 7. Mengubah kunci akses fisik jika hilang, disalahgunakan, atau individu dipindahkan atau diberhentikan
0902	Penggunaan perangkat lunak yang masih belum matang	SA-15 Development Process, Standards, and Tools <u>Preventif</u> 1. Mengharuskan pengembang perangkat lunak untuk menetapkan metrik kualitas di awal proses pengembangan 2. Meninjau kualitas proses pengembangan
0609	Informasi sensitif terungkap karena	AU-13 Monitoring for Information Disclosure

Kode	Kemungkinan Risiko	Nomor/ Judul Kontrol/ Kontrol	Kode	Kemungkinan Risiko	Nomor/ Judul Kontrol/ Kontrol
0603	Media <i>portable</i> yang berisi data sensitif hilang/ terekspos ke publik	<u>Detektif</u> Memantau bukti pengungkapan informasi organisasi tanpa izin pada situs atau media sosial tertentu MP-4 Media Storage <u>Preventif</u> 1. Mengontrol dan mengamankan fisik media penyimpanan digital maupun non-digital dalam area yang dikontrol 2. Melindungi media sistem informasi hingga ia dihancurkan atau dibersihkan menggunakan peralatan, teknik dan prosedur yang disepakati	1905	Adanya banjir	<i>malicious code</i> 2. Melakukan pemindaian <i>malicious code</i> secara berkala 3. Memblokir, mengkarantina atau menghapus <i>malicious code</i> yang ditemukan dan mengatasi dampak potensial terhadap ketersediaan (<i>availability</i>) dari sistem informasi <u>Preventif</u> Memperbarui (<i>update</i>) mekanisme perlindungan <i>malicious code</i> secara otomatis CODP-1 Disaster and Recovery Planning <u>Preventif</u> Menyediakan rencana bencana dan pemulihan yang memungkinkan dilanjutkannya kembali fungsi-fungsi bisnis utama setelah rencana tersebut diaktivasi.
0604	Data sensitif hilang/ terekspos, karena <i>logical attack</i>	RA-5 Vulnerability Scanning <u>Preventif</u> 1. Memindai kerentanan dalam sistem informasi pada frekuensi tertentu dan saat ditemukan kerentanan baru yang berpotensi mempengaruhi sistem 2. Menggunakan alat dan teknik pemindaian kerentanan yang mengotomasi proses manajemen kerentanan 3. Menganalisis laporan pemindaian kerentanan dan hasil dari penilaian kontrol keamanan 4. Memulihkan kerentanan sesuai dengan penilaian risiko organisasi	1901	Adanya gempa bumi	CODP-1 Disaster and Recovery Planning <u>Preventif</u> Menyediakan rencana bencana dan pemulihan yang memungkinkan dilanjutkannya kembali fungsi-fungsi bisnis utama setelah rencana tersebut diaktivasi.
0605	Media <i>backup</i> hilang	COBR-1 Protection of Backup and Restoration Assets <u>Preventif</u> Menyediakan prosedur untuk memastikan perlindungan fisik dan teknis yang tepat dalam pencadangan (<i>backup</i>) dan pemulihan (<i>restoration</i>) perangkat keras dan perangkat lunak	1903	Adanya badai besar	CODP-1 Disaster and Recovery Planning <u>Preventif</u> Menyediakan rencana bencana dan pemulihan yang memungkinkan dilanjutkannya kembali fungsi-fungsi bisnis utama setelah rencana tersebut diaktivasi.
1602	Gangguan akibat serangan DoS	SC-5 Denial of Service Protection <u>Detektif</u> Menggunakan perangkat pemantauan untuk mendeteksi terjadinya serangan DoS pada sistem informasi <u>Preventif</u> 1. Sistem informasi mengelola kelebihan bandwidth untuk membatasi efek dari serangan DoS 2. Memantau sumberdaya sistem informasi organisasi untuk memastikan memadai dalam mencegah serangan DoS	1904	Adanya kebakaran	PE-13 Fire Protection <u>Detektif</u> Menggunakan perangkat/sistem untuk mendeteksi kebakaran pada sistem informasi dan melaporkannya <u>Korektif</u> Menggunakan perangkat/sistem untuk memadamkan kebakaran pada sistem informasi dan melaporkannya
1605	Adanya serangan virus	SI-3 Malicious Code Protection <u>Detektif, Korektif</u> 1. Menerapkan mekanisme perlindungan <i>malicious code</i> (termasuk <i>virus</i>) di titik masuk dan keluar sistem informasi (termasuk <i>firewall</i>, <i>server</i>, komputer, perangkat <i>mobile</i>) untuk mendeteksi dan menghapus	1906	Batas air sungai meningkat	PE-15 Water Damage Protection <u>Preventif</u> Menggunakan mekanisme otomatis untuk mendeteksi keberadaan air di sekitar sistem informasi dan melaporkannya
				Proses Penampilan, Pengumuman, Pengiriman, Penyebarluasan, dan/atau Pembukaan Akses	
			1601	Staf yang tidak berwenang mencoba masuk ke sistem	SI-4 Information System Monitoring <u>Preventif</u> 1. Memantau sistem informasi untuk mendeteksi serangan dan indikasi serangan potensial dan mendeteksi koneksi lokal, jaringan, dan jarak jauh yang tidak sah. 2. Mengidentifikasi penggunaan

Kode	Kemungkinan Risiko	Nomor/ Judul Kontrol/ Kontrol
0902	Penggunaan perangkat lunak yang masih belum matang	sistem informasi yang tidak sah melalui teknik dan metode tertentu SA-15 Development Process, Standards, and Tools <u>Preventif</u> 1. Mengharuskan pengembang perangkat lunak untuk menetapkan metrik kualitas di awal proses pengembangan 2. Meninjau kualitas proses pengembangan
1603	Adanya kerusakan pada website	RA-5 Vulnerability Scanning <u>Preventif</u> 1. Memindai kerentanan dalam website pada frekuensi tertentu dan saat ditemukan kerentanan baru yang berpotensi mempengaruhi sistem 2. Menggunakan alat dan teknik pemindaian kerentanan yang mengotomasi proses manajemen kerentanan 3. Menganalisis laporan pemindaian kerentanan dan hasil dari penilaian kontrol keamanan 4. Memulihkan kerentanan sesuai dengan penilaian risiko organisasi
0609	Informasi sensitif terungkap karena tidak efisien dalam mempertahankan/ mengarsip/ membuang informasi	DM-2 Data Retention and Disposal <u>Preventif</u> Mempertahankan, mengarsip, dan membuang kumpulan informasi pengidentifikasi pribadi / <i>personally identifiable information</i> (PII) dengan teknik atau metode yang dapat mencegah kehilangan, pencurian, penyalahgunaan, atau akses tidak sah

Pada Tabel 10 dapat dilihat bahwa sebagian besar kontrol yang dipilih untuk penanganan risiko diambil dari NIST 800-53 yang nomor kontrolnya diawali dengan 2 karakter huruf, sebagian kecil lainnya diambil dari DoD Instruction 8500.2 yang nomor kontrolnya diawali dengan 4 karakter huruf.

Beberapa risiko ditangani dengan dua atau tiga tipe kontrol sekaligus, seperti halnya risiko serangan virus risiko yang ditangani dengan kontrol detektif, korektif maupun preventif, serta risiko kebakaran yang ditangani dengan kontrol detektif maupun korektif. Terdapat penggunaan kontrol yang sama untuk menangani beberapa risiko berbeda misalnya *vulnerability scanning* untuk menangani risiko data hilang (karena *logical attack*) dan kerusakan pada website, serta *disaster and recovery planning* untuk menangani risiko terjadinya banjir, gempa dan badai.

5. Kesimpulan

Berdasarkan hasil identifikasi risiko terkait perlindungan data pribadi pada aplikasi Sistem Informasi Administrasi Kependudukan (SIK) ditemukan 22 kemungkinan risiko yang tersebar pada 5 proses perlindungan data pribadi. Setelah dievaluasi, diperoleh bahwa risiko-risiko tersebut masuk ke dalam tingkat sedang-tinggi sehingga dipilihlah opsi penanganan *mitigate*. Usulan penanganan terhadap risiko terbagi dalam tiga tipe yakni kontrol preventif, kontrol detektif, dan kontrol korektif.

Implikasi dari penelitian ini ialah bahwa pemerintah kota/kabupaten sebagai pengelola aplikasi SIAK perlu memperhatikan setiap risiko yang mungkin terjadi terkait proses perlindungan data pribadi, dan menerapkan kontrol yang tepat untuk mitigasi risikonya. Implementasi kontrol yang dihasilkan dari penelitian ini diharapkan dapat mencegah, mendeteksi dan menyelesaikan risiko-risiko yang mungkin terjadi terkait proses perlindungan data pribadi.

Terdapat keterbatasan pada penelitian ini yakni proses manajemen risiko yang dilakukan berhenti pada tahap penanganan risiko atau lebih tepatnya tahap persiapan rencana penanganan risiko, tidak sampai pada implementasi rencana penanganan risiko atau bahkan hingga dilakukannya pemantauan dan peninjauan, juga pencatatan dan pelaporan. Sebelum usulan penanganan yang berupa kontrol ini diimplementasikan, pada penelitian selanjutnya perlu dilakukan pengkombinasian kontrol hasil dari penelitian ini dengan pasal-pasal yang terdapat di Permenkominfo No 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik maupun regulasi lainnya, serta dilakukan penyusunan peta jalan (*roadmap*) implementasinya.

Daftar Rujukan

- [1] S. Dewi, 2016, Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia, *Yustisia*, vol.5 no.1, hal. 22–30.
- [2] Anggara, 2015, Menyeimbangkan Hak : Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia, hal. 1–19.
- [3] Latumahina, R.E., 2014. Aspek Hukum Perlindungan Data Pribadi di Dunia Maya, *Jurnal GEMA AKTUALITA*, vol.3 no.2, hal. 14–25.
- [4] Menteri Komunikasi dan Informatika Republik Indonesia, 2016, Peraturan Menteri Komunikasi dan Informatika Nomor 20 tahun 2016 Tentang Perlindungan Data Pribadi, hal. 1-24.
- [5] Agustinus, Nugroho, Cahyono, 2017, Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS, *Jurnal RESTI*, vol.1 no.3, hal. 250-258.
- [6] Iin, Tjahyanto, 2017, Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan XYZ Melalui Kombinasi COBIT, PMBOK, dan ISO 31000, *DINAMIKA TEKNOLOGI*, vol.9 no.2, hal. 43-50.
- [7] Hevner, March, Park, Ram, 2004, Design Science in Information Systems Research, *MIS Quarterly*, vol. 28 no. 1, hal. 75.
- [8] ISACA, 2013, COBIT 5 for Risk, hal. 67-74.

- [9] US Department of Defense Instruction Number 8500.2, 2003. Information Assurance (IA) Implementation [online]. Available at: https://fas.org/irp/doddir/dod/d8500_2.pdf. [Accessed 20 July 2019]
- [10] NIST Special Publication 800-53 Revision 4, 2013. Security and Privacy Controls for Federal Information Systems and Organizations [online]. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. [Accessed 20 July 2019]
- [11] International Organization for Standardization, 2018, ISO 31000 Second Edition 2018-02. Risk Management – Guidelines.
- [12] Menteri Keuangan Republik Indonesia, 2016, Keputusan Menteri Keuangan Republik Indonesia Nomor 845/KMK.01/2016 tentang Petunjuk Pelaksanaan Manajemen Risiko di Lingkungan Kementerian Keuangan, hal. 1-34.