Rancangan Tata Kelola Organisasi Sistem Manajemen Keamanan Informasi Dinas Komunikasi dan Informatika Kabupaten Bekasi

Organization Governance Design of Information Security Management System Bekasi Communications and Information Technology Agency

Alhadi Saputra[1], Yudho Giri Sucahyo[2]
[1]Pusat Teknologi Informasi dan Standar Penerbangan dan Antariksa-LAPAN
Jalan Pemuda Persil No.1 Jakarta Timur
[2]Program Magister Teknologi Informasi Universitas Indonesia
Jalan Salemba Raya No.4 Jakarta

[1]alhadi.saputra@lapan.go.id, [2]yudho@cs.ui.ac.id,

Naskah diterima: 20 Oktober 2017, direvisi: 06 April 2018, disetujui: 16 Mei 2018

Abstract

Currently, Bekasi Communications and Information Technology Agency (Diskominfo Bekasi) is implementing information security management systems. To measure the implementation process, it conducts a compliance audit process using a framework of ISO / IEC 27001: 2013. Results of the compliance audit indicate that there is a nonconformity issue, in which one of the findings relates to information security organization clause. Information security organization established by Communications and Information Technology Agency has not incorporated the whole role and responsibilities specified in the framework. Therefore, Communications and Information Technology Agency has made some adjustments by developing organization governance design, which specifies the roles and responsibilities required by ISO / IEC 27001: 2013 and those that have been set by Communications and Information Technology Agency regulations. The result of organization governance design of information security management systems at Communications and Information Technology Agency suggests that Communications and Information Technology Agency Head plays a role in one objective control, Head of Division of Technology Standardisation and Communication and Information Technology Application plays a role in five objective controls, the Communication and Information Technolog Application Section plays a role in two objective controls, the Secretariate plays a role in two objective controls, the Information and Communication Technology Infrastructure Section plays a role in five objective controls, and the Information and Communication Technologies Application Section play a role in four objective controls.

Keywords: *Implementation, Information Security, ISO/IEC 27001:2013, Bekasi local Government.*

Abstrak

Saat ini Dinas Komunikasi dan Informatika Kabupaten Bekasi sedang mengimplementasikan sistem manajemen keamanan Informasi. Untuk mengukur proses pengimplementasiannya, Dinas Komunikasi dan Informatika (Diskominfo) melakukan proses audit kepatuhan menggunakan kerangka kerja ISO/IEC 27001:2013. Dari Hasil audit kepatuhan terdapat ketidaksesuaian dengan kerangka kerja ISO/IEC 27001:2013, salah satu temuannya terkait dengan klausul tentang organisasi keamanan informasi. Organisasi keamanan informasi yang ditetapkan oleh Dinas Komunikasi dan Informatika belum mencakup keseluruhan peran dan tanggung jawab yang disyaratkan pada kerangka kerja ISO 27001:2013. Oleh karena itu, Dinas Komunikasi dan Informatika melakukan penyesuaian dengan membuat rancangan tata kelola organisasi dengan memetakan peran dan tanggung jawab yang disyaratkan pada ISO/IEC 27001:2013 dengan yang ditetapkan oleh Dinas Komunikasi dan Informatika. Hasil rancangan tata kelola organisasi sistem manajemen keamanan informasi pada Dinas Komunikasi dan Informatika yaitu, Kepala Diskominfo berperan pada 1 kontrol objektif, Bidang Standarisasi teknologi dan Penerapan Teknologi Informasi dan Komunikasi berperan pada 5 kontrol objektif, Seksi penerapan teknologi informasi dan komunikasi berperan pada 2 kontrol objektif, Sekretariat berperan pada 2 kontrol objektif, Seksi Infrastruktur Teknologi Informasi dan Komunikasi berperan dalam 5 kontrol objektif, dan Seksi Aplikasi Teknologi Informasi dan Komunikasi berperan dalam 4 kontrol objektif.

Kata kunci: implementasi, keamanan informasi, ISO/IEC 27001:2013, Pemerintah Kabupaten Bekasi.

PENDAHULUAN

Keamanan informasi sudah menjadi kebutuhan dan syarat utama dalam menjaga keberlangsungan bisnis suatu organisasi. Suatu organisasi akan menghasilkan sejumlah data dan informasi. Data dan Informasi yang dihasilkan memiliki nilai yang sangat berharga karena banyaknya sumber daya yang telah dikeluarkan untuk menghasilkan data dan informasi tersebut. Beberapa dari data dan informasi biasanya merupakan produk yang memiliki nilai jual dan pada akhirnya dapat memengaruhi citra atau reputasi suatu organisasi.

Proses penciptaan data dan informasi pada organisasi sebagian besar didukung oleh pengoperasian layanan teknologi informasi dan layanan sistem informasi. Layanan-layanan ini selain harus memperhatikan ketersediaan layanannya setiap saat, perlu juga memperhatikan sisi keamanan informasinya agar tidak bisa diakses dan dicuri oleh orang yang tidak berhak. Area ancaman keamanan informasi di dalam organisasi berfokus pada sikap, niat, dan perilaku para pegawai (Safa, Maple, Watson, and Solms, 2017). Efektivitas manajemen keamanan informasi dapat dimaknai dari sejauh mana tujuan dan sasaran program manajemen keamanan informasi tercapai, informasi terlindungi, dan ukuran keamanan seperti metode, kebijakan atau prosedur keamanan informasi, pengendaliaan keamanan, dan *tools* terus diterapkan di dalam organisasi (Hwang dan Choi, 2017).

Bekasi adalah salah satu Kabupaten di Jawa Barat. Saat ini keamanan informasi sedang menjadi isu utama di Kabupaten Bekasi dengan diterbitkannya Peraturan Menteri

Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Dalam peraturan tersebut setiap penyelenggara sistem elektronik yang menyelenggarakan sistem elektronik strategis dan tinggi harus menerapkan standar SNI ISO/IEC 27001:2013 (Kemenkominfo, 2016). Dalam penerapan standar dan pedoman tersebut, penyelenggara sistem elektronik dapat menggunakan tenaga ahli internal dan/ atau eksternal yang berkewarganegaraan Indonesia atau tenaga ahli asing yang telah ditetapkan oleh Kementerian Komunikasi dan Informatika. Penyelenggaraan sistem manajemen pengamanan informasi pada penyelenggara sistem elektronik ditandai dengan diterimanya sertifikat dari lembaga sertifikasi pengamanan informasi yang telah ditetapkan oleh Kementerian Keamanan Informasi. Dengan adanya landasan hukum, sasaran strategi serta Permen Kominfo tersebut maka pemerintah Kabupaten Bekasi perlu melakukan sistem manajemen keamanan informasi.

Hal yang terkait dengan keamanan informasi, Pemerintah Kabupaten Bekasi menuangkan isu keamanan informasi pada Rencana Strategis Dinas Komunikasi dan Informatika Tahun 2015-2017. Pada rencana strategis disebutkan bahwa adanya tuntutan keamanan dan ketahanan informasi dan data milik pemerintah, sehingga perlu melakukan proteksi terhadap penyadapan informasi di lingkungan Pemerintah Kabupaten Bekasi, agar data dan informasi yang bersifat rahasia bagi negara tidak menjadi konsumsi publik (Diskominfo, 2015).

Selain itu, Pemerintah Kabupaten Bekasi juga sedang melakukan pengembangan *e-government* dengan sasaran dan strategi pengembangan yang jelas. Adapun sasaran yang terkait dengan pengamanan informasi yang ingin dicapai adalah perumusan kebijakan tentang pengamanan informasi serta pembakuan sistem otentikasi dan *public key infrastructure* untuk menjamin keamanan informasi dalam penyelenggaraan transaksi dengan pihak-pihak lain, terutama yang berkaitan dengan dengan kerahasiaan informasi dan transaksi finansial (Diskominfo, 2013).

Seiring dengan berjalannya waktu, berbagai kegiatan terkait implementasi keamanan informasi telah diselenggarakan oleh Pemerintah Kabupaten Bekasi. Pada tahun 2014, Pemerintah Kabupaten Bekasi telah melakukan evaluasi tingkat kematangan Indeks KAMI yang diselenggarakan oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika (Kemenkominfo, 2015). Salah satu kategori yang ada dalam penilaian Indeks KAMI adalah tingkat ketergantungan terhadap peran TIK. Hasil evaluasi pada kategori tingkat ketergantungan terhadap peran TIK adalah tinggi. Secara keseluruhan nilai status kesiapannya adalah 85 dari nilai maksimum 588, hal ini menunjukkan bahwa saat ini TIK merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan, tetapi kontrol pengamanan yang diterapkan masih belum memadai dan membutuhkan peningkatan di berbagai aspek sesuai dengan kebutuhan kontrol yang seharusnya diterapkan untuk peran TIK dengan tingkat ketergantungan yang tinggi.

Standar ISO/IEC 27001:2013 yang disyaratkan dalam peraturan penyelenggaraan system elektronik merupakan bagian dari rumpun standar ISO 27000 atau standar Sistem Manajemen Keamanan Informasi (SMKI). Rumpun standar tersebut dimaksudkan untuk membantu suatu organisasi dalam menerapkan dan menjalankan SMKI. Standar ISO/IEC 27001:2013 telah mengalami revisi dari ISO/IEC 27001:2005 menjadi ISO/IEC 27001:2013. ISO/IEC 27001:2013 menggunakan struktur penulisan sebagai berikut (ISO, 2013):

Foreword
Introduction
Scope
Normative references
Terms and definitions
Context of the organization
Understanding the organization and its context
Understanding the needs and expectations of interested parties
Determining the scope of the information security management sistem
Information security management sistem
Leadership
Leadership and commitment
Policy
Organizational roles, responsibilities and authorities
Planning
Actions to address risks and opportunities
Information security objectives and planning to achieve them
Support
Resources
Competence
Awareness
Communication
Documented Information
Operation
Operational planning and control
Information security risk assessment
Information security risk treatment
Performance evaluation
Monitoring, measurement, analysis and evaluation
Internal audit
Management review
Improvement
Nonconformity and corrective action
Continual improvement
Annex A (normative) Reference control objective and controls
Bibliography

Dari struktur penulisan di atas, inti dari standar ISO/IEC 27001:2013 terdapat pada klausul 4 sampai dengan 10. Klausul tersebut berisi ketentuan, proses dan aktivitas yang menjadi prasyarat yang harus dipenuhi oleh organisasi pada proses sertifikasi standar internasional. Sementara itu bagian lampiran A (Annex A) merupakan kontrol normatif yang terdiri dari 14 domain area, 35 tujuan kontrol dan 114 kontrol keamanan informasi. Area dan tujuan kontrol pada ISO/IEC 27001:2013 ini digunakan sepenuhnya untuk menilai sejauh mana penerapan sistem manajemen keamanan informasi yang telah dilakukan oleh Pemerintah Kabupaten Bekasi. Menurut Peraturan Menteri Komunikasi dan Informatika nomor 4 tahun 2016 Pasal 7 ayat (2), penyelenggara sistem elektronik yang menyelenggarakan sistem elektronik tinggi harus menerapkan standar SNI ISO/IEC 27001 (Kemenkominfo, 2016). Adapun area dan tujuan kontrol ISO/IEC 27001 terlihat pada Tabel 1.

Tabel 1. Area dan Tujuan Kontrol Pada ISO/IEC 27001:2013

Area	Sasaran Kontrol
Information Security Policies	*Management direction for information security*
Organization of information security	*Internal organization*
	Mobile devices and teleworking
Human resources security	*Prior to employment*
	During employment
	Termination and change of employment
Aset management	*Responsibility for asets*
	Information classification
	Media Handling
Access control	*Business requirements for access control*
	User access management
	User responsibilities
	Sistem and application access control
Cryptography	*Cryptographic controls*
Physical and environtmental security	*Secure areas*
	Equipment
Operations security	*Operational procedures and responsibilities*
	Protection from malware
	Backup
	Logging and monitoring
	Control of operational software
	Technical vulnerability management
	Information sistems audit considerations
Communications security	*Network security management*
	Information transfer
Sistem acquisitions, development and maintenance	*Security requirements of information sistems*
	Security in development and support process
	Test data
Supplier relationships	*Information security in supplier relationships*
	Supplier service delivery management
Information security incident management	*Management of infosec incidents and improvements*
Information security aspects of BCM	*Information security continuty*
	Redudancies
Compliance	*Compliance with legal & contractual requirement*
	Information security reviews

Manajemen keamanan informasi telah menjadi hal yang penting untuk menghindari ancaman keamanan terhadap aset informasi organisasi. Ancaman adalah upaya untuk mengeksploitasi kerentanan yang mengakibatkan hilangnya confidentiality (kerahasiaan), integrity (integritas), atau availability (ketersediaan) aset informasi organisasi (Gibson, 2011). Organisasi yang bersedia mencapai tingkat keamanan yang memadai harus dapat mengidentifikasi lubang keamanan dan mengembangkan mekanisme untuk mencegah penyalahgunaannya (Alsaif, Aljaafari, and Khan, 2015).

Keamanan informasi dipahami sebagai konsep yang mencakup faktor-faktor seperti teknologi keamanan informasi, hubungan sosial antara semua pihak di dalam organisasi, strategi keamanan informasi, dan kebijakan keamanan informasi (Moon, Choi, and Armstrong, 2018).

Manajer keamanan informasi ditugaskan untuk berbagai fungsi, termasuk perencanaan keamanan, kebijakan informasi, kepegawaian, manajemen risiko, pemilihan teknologi keamanan, penilaian ancaman, implementasi penanggulangan, pemantauan kinerja, dan pemeliharaan (Nazareth, and Choi, 2015). Manajemen Organisasi bertanggung jawab atas semua aktivitas sumber daya manusia, seperti perencanaan, akuisisi, motivasi, pelatihan, pemodelan perilaku dan pengendalian aktivitas manusia dalam organisasi, sehingga menjadi tanggung jawab manajemen untuk mengendalikan dan mengalihkan kegiatan ini menuju keamanan informasi (Soomro, Shah, and Ahmed, 2016). Oleh karena itu, peran dan tanggung jawab dari Kabupaten Bekasi perlu dikhususkan pada keamanan informasi sehingga penerapan sistem manajemen keamanan informasi menjadi efektif dan sukses.

Sebagai unit setingkat eselon II diberi wewenang untuk mengelola teknologi informasi dan komunikasi, selain keahlian di bidang teknologi informasi diharapkan juga memiliki keahlian dalam keamanan informasi. Petugas keamanan informasi yang berkualitas, memproses sejauh mana organisasi dan staf profesional dapat menentukan, melaksanakan, dan memelihara program keamanan informasi organisasi (Cavusoglu, Cavusoglu, Son, and Benbasat, 2015).

METODE

Penelitian diawali dengan melakukan audit kepatuhan keamanan informasi berdasarkan ISO/IEC 27001:2013 untuk mengetahui kondisi pengimplementasian keamanan informasi saat ini. Dari hasil audit tersebut terlihat kesenjangan sehingga sistem manajemen keamanan informasi perlu dilakukan perbaikan dan peningkatan.

Dalam rangka melakukan upaya perbaikan dan peningkatan sistem manajemen keamanan informasi dilakukan dengan beberapa tahapan. Tahapan pertama, yaitu melakukan tinjauan pemenuhan persyaratan dari setiap domain kontrol objektif pada ISO/IEC 27001:2013. Tahapan kedua, yaitu melakukan tinjauan terhadap peran dan tanggung jawab di setiap bidang tugas pada struktur organisasi Dinas Komunikasi dan Informatika khususnya terkait uraian tugas keamanan informasi. Tahapan ketiga adalah merancang tata kelola setiap domain kontrol objektif pada ISO/IEC 27001:2013 terhadap peran dan tanggung jawab di setiap bidang tugas pada struktur organisasi Dinas Komunikasi dan Informatika. Tujuan rancangan tata kelola tersebut agar proses perbaikan dan peningkatan sistem manajemen keamanan informasi dikerjakan secara efektif dan efisien sesuai dengan peran dan tanggung jawab terhadap bidang tugas yang ditetapkan dalam struktur organisasi Dinas Komunikasi dan Informatika Pemerintah Kabupaten Bekasi.

HASIL DAN PEMBAHASAN

Sebagaimana dijelaskan pada bagian metode, penelitian ini diawali dengan melakukan audit kepatuhan keamanan informasi berdasarkan ISO/IEC 27001:2013 untuk mengetahui kondisi pengimplementasian keamanan informasi saat ini. Analisis

kesenjangan dilakukan dengan mengkaji domain kontrol objektif dan pengendali yang ada pada ISO/IEC 27001:2013, setelah itu dilakukan perumusan pertanyaan untuk melakukan *assessment*. Setelah merumuskan pertanyaan, maka selanjutnya melakukan proses penilaian. Proses penilaian dilakukan dengan wawancara dan observasi dokumen. Wawancara dilakukan dengan sekretaris Dinas Komunikasi dan Informatika Pemerintahan Kabupaten Bekasi selaku eselon III, pengelola teknologi informasi dan sistem informasi, dan pengelola data center. Data hasil audit tersebut dapat dilihat pada tabel 2 (Saputra, 2016).

Tabel 2. Perhitungan Analisis Kesenjangan untuk Domain ISO/IEC 27001:2013

Domain Kontrol	A	B	C
Kebijakan Keamanan Informasi	0	6	0
Organisasi Keamanan Informasi	0,15	13	0,01
Keamanan Sumber Daya Manusia	0,4	15	0,03
Manajemen aset	0,65	17	0,04
Akses Kontrol	0,1	21	0,005
Kriptografi	0	3	0
Keamanan Fisik dan Lingkungan	0,47	32	0,01
Keamanan Operasi	0,48	27	0,02
Keamanan Komunikasi	0,29	14	0,02
Sistem Akuisisi, Pengembangan dan Pemeliharaan	0,42	19	0,02
Hubungan Pemasok	0,06	9	0,006
Manajemen Insiden Keamanan Informasi	0,15	13	0,01
Aspek-aspek Keamanan Informasi Pada Manajemen Keberlanjutan Bisnis	0,25	4	0,06
Kepatuhan	0,32	14	0,02

Sumber: Saputra, 2016 (telah diolah kembali)

A : Hasil wawancara dan observasi menggunakan panduan *assessment checklist*
B : Nilai Maksimum *Checklist*
C : Persentase penerapan (Hasil A dibagi dengan B)

Berdasarkan tabel 2, Perhitungan Analisis Kesenjangan untuk Domain ISO/IEC 27001:2013, hasil penilaian wawancara dan observasi menggunakan panduan *assessment checklist* berkisar antara 0 s.d 0,65 (Saputra, 2016). Terdapat dua domain kontrol yang bernilai 0, yaitu domain kebijakan informasi dan domain kriptografi, dan nilai tertinggi, yaitu 0,65 terdapat pada domain manajemen aset. Seluruh domain memiliki nilai persentase penerapan berkisar antara 0 s.d 0,06. Hasil penilaian ini merupakan acuan dalam pembuatan rancangan tata kelola organisasi sistem manajemen keamanan informasi sebelum adanya rencana restrukturisasi organisasi.

Dari analisis kesenjangan yang dilakukan terhadap domain kontrol objektif yang ada dapat terlihat bahwa Pemerintah Kabupaten Bekasi masih sangat jauh dari patuh terhadap Sistem Manajemen Keamanan Informasi yang disyaratkan oleh ISO/IEC 27001:2013. Beberapa permasalahan terkait keamanan informasi yang terjadi adalah adanya insiden *malware* yang menyerang beberapa halaman URL (*Uniform Resource Locator*) pada situs resmi pemerintahan kabupaten bekasi. Perbaikan terhadap insiden tersebut belum tertangani dikarenakan tidak adanya SDM yang memiliki kompetensi khusus untuk menangani insiden tersebut. Selain itu tidak adanya acuan kebijakan, standar, dan

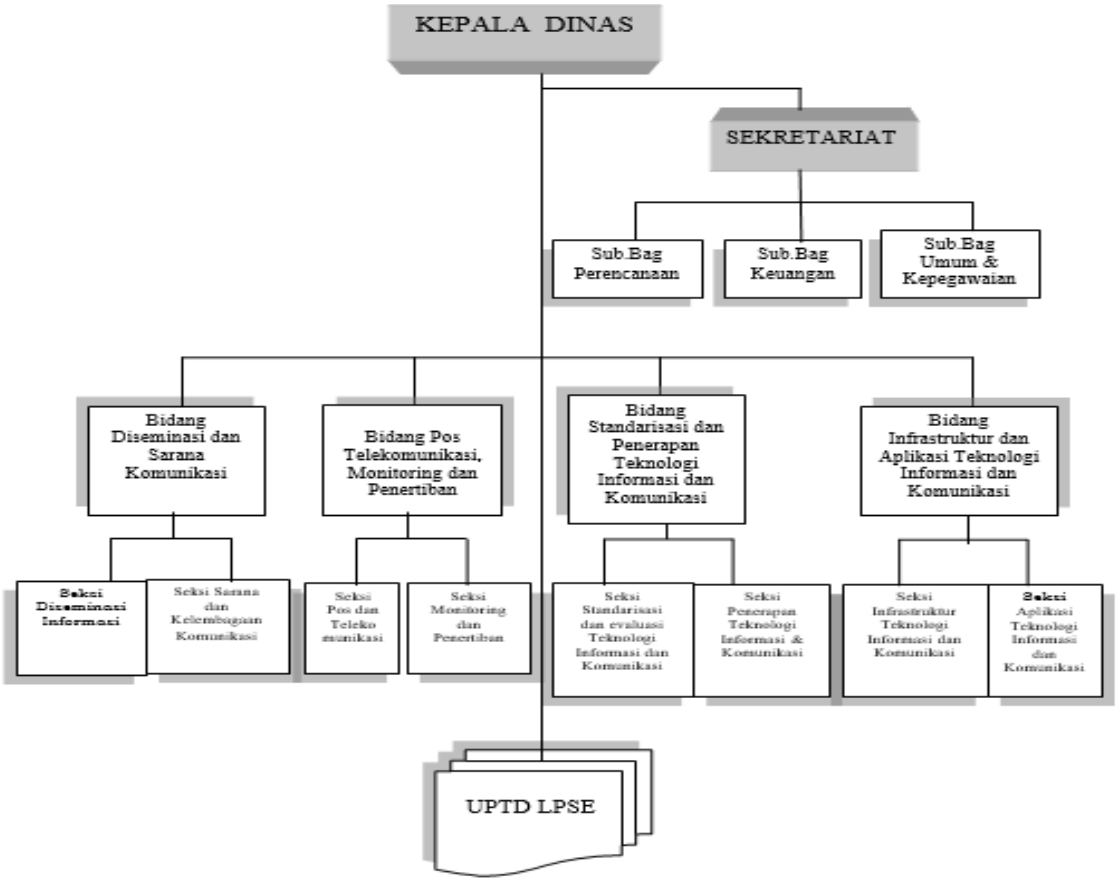
prosedur terkait penanganan keamanan informasi serta minimnya pengelolaan aset informasi yang terdokumentasi, hampir semua dilakukan secara informal dan penyelenggaraan pemerintahan lebih fokus kepada ketersediaan fasilitas TIK untuk membantu kelancaran kegiatan, belum disertai dengan fokus terhadap keamanan informasinya.

Struktur Organisasi Dinas Komunikasi dan Informatika

Untuk urusan kegiatan serta kebijakan terkait TIK, Pemerintah Kabupaten Bekasi memberikan wewenang tugas kepada Dinas Komunikasi dan Informatika (Diskominfo) yang merupakan unit kerja setingkat eselon II. Diskominfo dipimpin oleh seorang kepala dinas, dan kepala dinas membawahi beberapa kepala bidang, kepala bidang membawahi beberapa kepala seksi beserta staf pelaksana.

Sesuai dengan tugas pokok dan fungsi dari Diskominfo, Bidang yang terkait dengan TIK terdiri dari dua bidang, yaitu (1) Bidang Standarisasi dan Penerapan TIK dan (2) Bidang Infrastruktur dan Aplikasi TIK. Bidang Standarisasi dan Penerapan TIK membawahi dua seksi, yaitu (1) Seksi Standarisasi dan Evaluasi Teknologi Informasi dan Komunikasi dan (2) Seksi Penerapan Teknologi Informasi dan Komunikasi. Sementara itu Bidang Infrastruktur dan Aplikasi Teknologi Informasi dan Komunikasi membawahi dua seksi, yaitu (1) Seksi Infrastruktur Teknologi Informasi dan Komunikasi dan (2) Seksi AplikasiTeknologi Informasi dan Komunikasi.

Struktur organisasi Dinas Komunikasi dan Informatika berdasarkan Peraturan Bupati Bekasi No. 56 Tahun 2014 Tentang Struktur Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika terlihat pada gambar 1 (Pemerintah Kabupaten Bekasi, 2014).



Gambar 1. Struktur Organisasi Dinas Komunikasi dan Informatika Pemkab Bekasi

Dalam menjalankan seluruh proses bisnis yang ada, diskominfo didukung dengan Sumber Daya Manusia (SDM) yang terdiri dari berbagai macam kompetensi. Hal ini dapat dilihat pada Tabel 3 dan Tabel 4.

Tabel 3. Sumber Daya Manusia Berdasarkan Tingkat Pendidikan

Tingkat Pendidikan	Jumlah SDM
Strata-2	10
Strata-1	24
Diploma-3	4
Diploma-1	1
SMA	6
SMP	3
SD	1

Sumber: Bagian Kepegawaian Diskominfo (telah diolah kembali)

Tabel 4. Sumber Daya Manusia Berdasarkan Latar Belakang Pendidikan

Jurusan	Jumlah SDM
Administrasi	13
Manajemen SDM	3
Akuntansi	5
Komputer	9
Ilmu Pemerintahan	2
Lain-lain	7

Sumber: Bagian Kepegawaian Diskominfo (telah diolah kembali)

Bidang Standarisasi dan Penerapan TIK hanya memiliki satu pegawai berlatar pendidikan komputer. Bidang Infrastruktur dan Aplikasi TIK memiliki tiga pegawai berlatar belakang pendidikan komputer, dan pada UPTD LPSE terdapat lima pegawai berlatar belakang pendidikan komputer.

Hal ini menyimpulkan bahwa komposisi pegawai berlatar belakang pendidikan komputer dari tiap bidang tidak merata, jumlah pegawai berlatar belakang komputer yang seharusnya lebih banyak dibutuhkan pada dua bidang tersebut ternyata jumlahnya lebih sedikit dibanding UPTD LPSE yang justru memiliki lima pegawai berlatar belakang pendidikan komputer. Selain itu terdapat pegawai yang memiliki jabatan rangkap dan pekerjaan rangkap baik administrasi maupun tugas mengelola TIK.

Setiap bidang dan seksi memiliki peran dan tanggung jawab yang ditetapkan. Uraian tugas terkait keamanan informasi beserta pihak yang bertanggung jawab terlihat pada Tabel 5.

Tabel 5. Uraian Tugas Terkait Keamanan Informasi

Uraian Tugas	Pihak Penanggung Jawab
Menetapkan prosedur keamanan dan keandalan operasi perangkat lunak	Kepala Diskominfo
Menyelenggarakan perjanjian tingkat layanan (*Service Level Agreement*) dan perjanjian keamanan informasi dengan seluruh SKPD yang menyelenggarakan sistem elektronik untuk pelayanan publik	Kepala Diskominfo
Memantau dan mengawasi pendokumentasian dan memastikan setiap perangkat aplikasi memiliki Standar	Kepala Diskominfo

Uraian Tugas	Pihak Penanggung Jawab
Operasional Prosedur (SOP) dan Standar Operasional Prosedur (SOP) keamanan data	
Memantau penerapan aplikasi keamanan data pada *server* pusat data	Kepala Diskominfo
Memberikan masukkan dalam pembuatan perjanjian tingkat layanan/ *Service Level Agreement* dan perjanjian keamanan informasi di seluruh SKPD yang menyelenggarakan sistem elektronik untuk pelayanan publik	Bidang Standarisasi dan Penerapan Teknologi Informasi dan Komunikasi
Melaksanakan perjanjian tingkat layanan/ *Service Level Agreement* dan perjanjian keamanan informasi di seluruh SKPD yang menyelenggarakan sistem elektronik untuk pelayanan publik	Seksi Standarisasi dan Evaluasi Teknologi Informasi dan Komunikasi
Melakukan pengamanan dan pemeliharaan barang milik daerah di lingkup Bidang Infrastruktur dan Aplikasi Teknologi Informasi dan Komunikasi	Bidang Infrastruktur dan Aplikasi Teknologi Informasi dan Komunikasi
Melaksanakan inspeksi secara berkala terhadap perangkat di seluruh SKPD untuk mencegah kebocoran data melalui perangkat	Seksi Infrastruktur Teknologi Informasi dan Komunikasi
Mendokumentasikan dan memastikan setiap perangkat aplikasi memiliki SOP Operasional dan SOP Keamanan Data	Seksi AplikasiTeknologi Informasi dan Komunikasi

Sumber: Peraturan Bupati Bekasi No. 56 Tahun 2014 (telah diolah kembali)

Hasil Rancangan Tata Kelola Peran dan Tanggung Jawab Terhadap Kontrol Objektif ISO/IEC 27001:2013

Rancangan tata kelola peran dan tanggung jawab terhadap kontrol objektif ISO/IEC dikerjakan dengan melakukan tinjauan terhadap kontrol objektif ISO/IEC 27001:2013 dan uraian tugas terkait keamanan informasi yang telah ditetapkan berdasarkan Peraturan Bupati Bekasi No. 56 Tahun 2014 tentang Struktur Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika. Rancangan ini merupakan rekomendasi dalam peningkatan sistem manajemen keamanan informasi di Pemerintah kabupaten Bekasi. Hasil rancangan tata kelola Kontrol Objektif dalam Annex A pada ISO/IEC 27001:2013 terhadap struktur organisasi Dinas Komunikasi dan Informatika terlihat pada Tabel 6.

Tabel 6. Hasil Rancangan Tata Kelola Peran dan Tanggung Jawab Terhadap Kontrol Objektif ISO/IEC 27001:2013

Control Objectives *ISO/IEC 27001:2013*	***Objectives ISO/IEC 27001:2013***	**Pemilik Proses**
Information Security Policies	*To Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations*	Kepala Diskominfo
Organization of Information Security	*To establish a management framework to initiate and control the implementation and operation of information security within the organization*	Bidang Standarisasi teknologi dan Penerapan TIK dan /atau Seksi penerapan teknologi informasi dan komunikasi

Control Objectives *ISO/IEC 27001:2013*	***Objectives ISO/IEC 27001:2013***	**Pemilik Proses**
Human Resource Security	*To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered*	Sekretariat
Asset Management	*To identify organizational assets and define appropriate protection responsibilities*	Sekretariat
Access Control	*To limit access to information and information processing facilities*	Seksi Infrastruktur Teknologi Informasi dan Komunikasi dan/ atau Seksi AplikasiTeknologi Informasi dan Komunikasi
Cryptography	*To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information*	Seksi AplikasiTeknologi Informasi dan Komunikasi
Physical Security Perimeter	*To prevent unauthorized physical access, damage and interference to the organization's information and informatiom processing facilities*	Seksi Infrastruktur Teknologi Informasi dan Komunikasi
Operations Security	*To ensure correct and secure operations of information processing facilities*	Seksi Infrastruktur Teknologi Informasi dan Komunikasi
Communications Security	*To ensure the protection of information in networks and its supporting information processing facilities*	Bidang Standarisasi dan Penerapan Teknologi Informasi dan Komunikasi
System acquisition, development and maintenance	*To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks*	Seksi Infrastruktur Teknologi Informasi dan Komunikasi/ Seksi AplikasiTeknologi Informasi dan Komunikasi
Supplier Relationships	*To ensure protection of the organization's assets that is accesible by suppliers*	Bidang Standarisasi dan Penerapan Teknologi Informasi dan Komunikasi dan /atau Seksi penerapan teknologi informasi dan komunikasi
Information Security Incidents Management	*To ensure a concistent and effective approach to the management of information security incidents, including communication on security events and weaknesses*	Seksi Infrastruktur Teknologi Informasi dan Komunikasi/ Seksi AplikasiTeknologi Informasi dan Komunikasi
Information Security Aspects of Business Continuity Management	*Information security continuity shall be embedded in the organization's business continuity management systems*	Bidang Standarisasi dan Penerapan Teknologi Informasi dan Komunikasi

Control Objectives *ISO/IEC 27001:2013*	***Objectives ISO/IEC 27001:2013***	**Pemilik Proses**
Compliance	*To ensure that information security is implemented and operated in accordance with the organizational policies*	Bidang Standarisasi dan Penerapan Teknologi Informasi dan Komunikasi

PENUTUP

Pengimplementasian sistem manajemen keamanan informasi pada Pemerintah Kabupaten Bekasi perlu ditingkatkan dan diperbaiki, oleh karena itu dilakukan rancangan tata kelola peran dan tanggung jawab dari masing-masing 14 kontrol objektif ISO/IEC 27001:2013 terhadap struktur organisasi pada Diskominfo. Hasil rancangan tata kelola organisasi sistem manajemen keamanan informasi pada Dinas Komunikasi dan Informatika, yaitu Kepala Diskominfo berperan pada 1 kontrol objektif, Bidang Standarisasi teknologi dan Penerapan Teknologi Informasi dan Komunikasi berperan pada 5 kontrol objektif, Seksi penerapan teknologi informasi dan komunikasi berperan pada 2 kontrol objektif, Sekretariat berperan pada 2 kontrol objektif, Seksi Infrastruktur Teknologi Informasi dan Komunikasi berperan dalam 5 kontrol objektif, dan Seksi Aplikasi Teknologi Informasi dan Komunikasi berperan dalam 4 kontrol objektif. Penelitian ini masih perlu dikaji kembali dengan menambahkan daftar uraian tugas secara detail untuk pengimplementasian setiap kontrol objektif pada masing-masing Kepala bidang, Kepala Seksi dan staf yang ada pada Dinas Komunikasi dan Informatika.

DAFTAR PUSTAKA

Alsaif, M., Aljaafari, N., Khan, A.R., “Information Security Management in Saudi Arabian Organization”, Procedia Computer Science 56 (2015) 213-216, 2015

Cavusoglu, H., Cavusoglu. H, Son., J.Y., Benbasat., I, “Institutional Presures in security management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources”, Journal of Information & Management 52 (2015) 385-400”, 2015

Diskominfo. *Rencana Strategis Dinas Komunikasi dan Informatika Tahun 2015-2017”, Jawa Barat*, 2015

Diskominfo. *Laporan Akhir Penyusunan Masterplan Pengembangan E-Government Kabupaten Bekasi*, Jawa Barat, 2013

Gibson, D.. *Managing Risk in Information Systems.* Sudburry, Jones&Bartlett Learning, 2011

Hwang, K., and Choi., M.,”Effects of Innovation-Supportive and Organizational Citizenship behavior on E-Government information System Security Stemming from Mimetic Isomorphism”, International Journal of Information Technology Management, Policies, and Practices Government Information Quarterly 34 (2017) 183-198, 2017

ISO, *ISO/IEC 27001:2013, Information Technology-SecurityTechniques-Information Security Management Sistems-Requirements*, 2013

Kementerian Kominfo, *Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi*, Jakarta, 2016

Kementerian Kominfo, *Laporan Hasil Kajian Keamanan Informasi Desktop Assesment 2014*, Jakarta, 2014

Moon, Y.J., Choi, M., and Armstrong, D.J.,"The Impact of Relational Leadership and Social Alignment on Information Security System Effectiveness in Korean Governmental Organizations", International Journal of Information Management 40 (2018) 54-66, 2018

Nazareth, D.L. and Choi, J. "A System Dynamics Model For Information Security Management", Journal of Information Management 52 (2015) 123-134, 2015

Pemerintah Kabupaten Bekasi, *Peraturan Bupati Nomor 56 Tahun 2014 Tentang Struktur Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Bekasi*, Jawa Barat, 2014

Saputra, Alhadi. *Audit Kepatuhan Keamanan Informasi Berdasarkan Kerangka Kerja ISO/IEC 27001:2013, Studi Kasus: pemerintah kabupaten Bekasi*, Karya Akhir, Universitas Indonesia-Jakarta, 2016

Safa, N.S., Maple, C., Watson., T., Solms, R.V,"Motivation and Opportunity Base Model to Reduce Information Security Insider Threats in Organisations", Journal of Information Security and Applications 000 (2017) 1-11, 2017

Soomro, Z.A., Shah, M.A., Ahmed, J., "Information Security management Needs More Holistic Approach: A Literature Review", International Journal of Information Management 26 (2016) 215-225, 2016