Rekomendasi Pemodelan Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001:2013 dan DFD pada PT. XYZ

Gustiana A.P.[1], Yudi Priyadi[2]
Program Studi Manajemen Bisnis Telekomunikasi dan Informatika
Fakultas Ekonomi dan Bisnis, Universitas Telkom
Jl. Telekomunikasi No.1, Bandung, Jawa Barat 40257, Telp. (022)7564108
e-mail: [1]putri.gustiana@gmail.com, [2]whyphi@telkomuniversity.ac.id

Abstrak

PT. XYZ merupakan salah satu marketplace terbesar di Indonesia sebagai penyedia layanan transaksi jual beli secara online. Penelitian ini bertujuan untuk melakukan analisis sistem manajemen keamanan informasi yang diterapkan oleh PT. XYZ dalam ruang lingkup transaksi antara pelapak dan pelanggan menggunakan ISO/IEC 27001:2013 serta memberikan rekomendasi alur sistem manajemen keamanan informasi yang perlu diperbaiki. Perancangan model rekomendasi alur sistem manajemen keamanan informasi dijabarkan dengan menggunakan Data Flow Diagram. Penelitian ini menggunakan metode kualitatif deskriptif dengan teknik pengumpulan data triangulasi. Berdasarkan hasil penelitian dapat diketahui bahwa perusahaan tidak memenuhi kontrol ISO 27001:2013 pada kontrol Kriptografi (A.10). Selain itu perusahaan tidak memenuhi kontrol Organisasi Keamanan informasi (A.6) sebesar 21.4% dan Akusisi, Pengembangan, dan Peningkatan Sistem (A.14) sebesar 7.7%. Nilai Compliant terbesar yang dimiliki oleh sistem manajemen keamanan informasi perusahaan terdapat pada kontrol Keamanan Komunikasi (A.13) dan Aspek Keamanan Informasi pada Manajemen Keberlangsungan Bisnis (A.17) yaitu masing-masing memiliki nilai sebesar 100%. Dalam kontrol Kebijakan Keamanan Informasi (A.5), pemenuhan sistem keamanan informasi yang diterapkan oleh perusahaan hanya 50%. Pada kontrol Keamanan Sumber Daya Manusia (A.7) tingkat Compliant perusahaan terhadap persyaratan ISO 27001:2013 adalah sebesar 91.7% dan nilai Partially Compliant sebesar 8.3%. Pada kontrol Kontrol Akses (A.9) tingkat Compliant perusahaan terhadap persyaratan ISO 27001:2013 adalah sebesar 92.9% dan nilai Partially Compliant sebesar 7.1%. Rekomendasi Data Flow Diagram dibuat berdasarkan validasi hasil maturity level pada klausul A.10 yang memiliki nilai paling rendah, yaitu bernilai 1. Sehingga pemodelannya terdiri dari tiga entitas yaitu: Pemilik Akun, Database Engineer, dan DPPED. Selain itu, terdapat empat data store yaitu: Kebijakan Penggunaan Kendali Kriptografi, Manajemen Kunci, Data Center, dan Dashboard Big Data Platform. Proses tersebut dirinci hingga level 2 yang terfokus pada proses enkripsi.

Kata kunci: *ISO/IEC 27001:2013, Data Flow Diagram, Analisis keamanan informasi, Sistem manajemen keamanan informasi.*

Abstract

PT. XYZ is one of the biggest marketplace in Indonesia who provide online transaction service. This research has a purpose to analyze information security management system that applied by PT. XYZ in selling transaction area using ISO 27001:2013 and give a recommendation about information security management system that has to be fixed. The recommendation model of information security management system is defined by data flow diagram. This research use descriptive qualitative method with triangulation technic. According to the results, the company has not fulfill the ISO 27001:2013's control in Cryptography (A.10). Beside that, the company has not fulfill the Information Security Organization control (A.6) in the amount of 21.4% and System Acquisition, Development, and Maintenance (A.14) in the amount of 7.7%. The biggest Information Security Management System's compliant score lies in Communication Security (A.13) and Information Security Aspects of Business Continuity (A.17) control which both of them have 100% compliant score. In Information Security Policies (A.5), the information security management system fulfillness only 50%. In Human Resource Security (A.7), the compliant score against IDO 27001:2013 is 91.7% and the partially compliant score is 8.3%. In Access Control (A.9) control, the compliant score against ISO 27001:2013 is 92.9% and the partially compliant score is 7.1%. The Recommendation of Data

Flow Diagram made by maturity level's validation of clause A.10 which has the lowest score, that is 1. Then the modelling has three entities: Account's Owner, Database Engineer, and DPPED. Beside that, the modelling has four data store: Policy on The Use of Cryptographic Control, Key Management, Data Center, and Big Data Platform Dashboard. The process has been specified into two levels which has focused into cryptography.

***Keywords**: ISO/IEC 27001:2013, Data Flow Diagram, Information security analysis, Information security management system.*

1. Pendahuluan

PT. XYZ termasuk ke dalam *online marketplace* dengan tipe *Consumer-to-Consumer* (C2C) dan berperan sebagai sarana penunjang bisnis yang menyediakan berbagai fitur dan layanan untuk menjamin keamanan dan kenyamanan para penggunanya. PT. XYZ telah menjadi salah satu *e-commerce* terbesar yang berkembang di Asia Tenggara seiring dengan adanya masa penetrasi penggunaan *smartphone* di kalangan masyarakat. Sebagai penyedia layanan perantara antara penjual dan pembeli, PT. XYZ berhasil menempati posisi empat besar aplikasi yang banyak diunduh dengan total unduhan aplikasi sebanyak 10.000.000 kali pada tahun 2017. Terhitung mulai dari bulan Agustus 2017 hingga Januari 2018 rata-rata pengunjung web PT. XYZ adalah sebesar 91.900.000 *visitor* dengan rata-rata durasi kunjungan selama 5 menit 28 detik. Hal tersebut menjelaskan bahwa sering terjadinya transaksi jual beli di PT. XYZ. Sebagai salah satu *online marketplace* yang banyak digunakan oleh masyarakat, keamanan Sistem Informasi tentunya menjadi salah satu penyokong kelancaran aktivitas transaksi jual beli pada situs PT. XYZ.

Namun saat ini merupakan era di mana teknologi berkembang sangat cepat dan telah memunculkan ancaman baru untuk informasi bisnis serta informasi aset di setiap tahap *information life cycle* [1]. Ancaman keamanan informasi yang dialami oleh perusahaan merupakan serangan virus berupa penerobosan atau pelanggaran terhadap informasi aset sehingga tidak memiliki nilai jual yang tinggi [2]. Pengambilan data dari *web application* dapat mengakibatkan kebocoran data mengenai konsumen maupun kekayaan intelektual perusahaan regulasi yang mengatur tentang privasi data digital yang dimiliki mensyaratkan perusahaan untuk mampu meningkatkan kapabilitas organisasi dalam menjaga keamanan *web application.*

Merujuk pada hal tersebut, informasi transaksi jual beli merupakan hal yang penting untuk dijaga oleh PT. XYZ, dari kemungkinan gangguan dan risiko yang akan datang. Sebagai *online marketplace* yang ingin menjaga kelancaran aktivitas transaksi jual-beli, PT. XYZ perlu untuk melakukan kegiatan analisis proses bisnis pada transaksi jual beli yang berlangsung serta tata kelola keamanan informasi yang dimiliki. ISO/IEC 27001:2013 dapat digunakan sebagai standar sistem manajemen keamanan informasi untuk menganalisis keamanan sistem informasi transaksi jual beli antara pelapak dengan pelanggan yang berlangsung pada PT. XYZ. COBIT digunakan sebagai model penilaian *maturity level*, karena kerangka model ini secara spesifik berfokus menilai prosedur adaptasi dan *awareness* [3]. Sedangkan ISO 27001:2013, menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi yang diakui secara internasional, yaitu *Information Security Management System (ISMS) certification* [4]. Selain itu, analisis proses bisnis pada transaksi jual beli antara pelapak dan pelanggan yang berlangsung pada PT. XYZ dapat menggunakan *Data Flow Diagram* (DFD) sebagai pemodelannya.

2. Metodologi Penelitian

Pada metodologi penelitian untuk kegiatan ini, terdapat beberapa konsep yang menjadi acuan semua tahapan dalam pelaksanaannya, yaitu: ISO/IEC 27001:2013, COBIT, Data Flow Diagram, dan tahapan penelitiannya.

2.1. *International Standarization for Organization* (ISO) 27001:2013

Penelitian ini menggunakan ISO 27001:2013 sebagai standardisasi dalam menilai tingkat kematangan pada sistem manajemen keamanan informasi milik PT. XYZ. ISO / IEC 27001:2013 menspesifikasikan persyaratan untuk membangun, menerapkan, memelihara dan terus meningkatkan sistem manajemen keamanan informasi serta menyediakan persyaratan untuk penilaian atas penanggulangan risiko keamanan informasi dalam konteks organisasi [5].

2.2. *Control Objective for Information Technology*

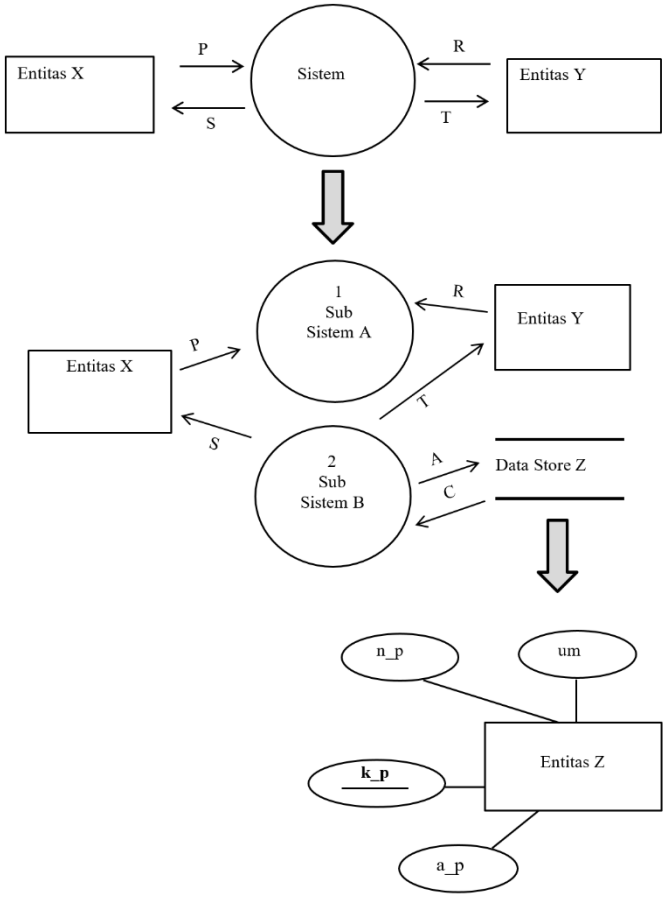
COBIT model dipilih karena kerangka model ini secara spesifik berfokus menilai prosedur adaptasi dan *awareness*. COBIT model merupakan alat informasi teknologi yang digunakan untuk

mengukur seberapa baik proses manajemen berkembang di dalam kontrol internal yang dapat diterapkan untuk mengukur dengan landasan standar tertentu dan dapat digunakan untuk menemukan peningkatan praktikal tentang kontrol internal sistem teknologi informasi [3].

2.3. *Data Flow Diagram*

DFD dipilih sebagai metode untuk mengilustrasikan fungsi-fungsi yang harus dijalankan oleh sistem. DFD dibuat mulai dari *Context Diagram* (CD), DFD level 1, DFD level 2, dan seterusnya sesuai dengan kompleksitas informasi dan kebutuhan [6].

Dalam pemodelan sistem yang menggunakan DFD, terdapat penggunaan teknik *Balanced Fragment*, sebagai proses konsistensi dalam melakukan *breakdown* setiap proses. Mulai dari CD menuju DFD, hingga *Entity Relationship Diagram* (ERD). Untuk mempertegas hal tersebut, ilustrasi aturannya dapat dicermati pada Gambar 1 [7], [8].

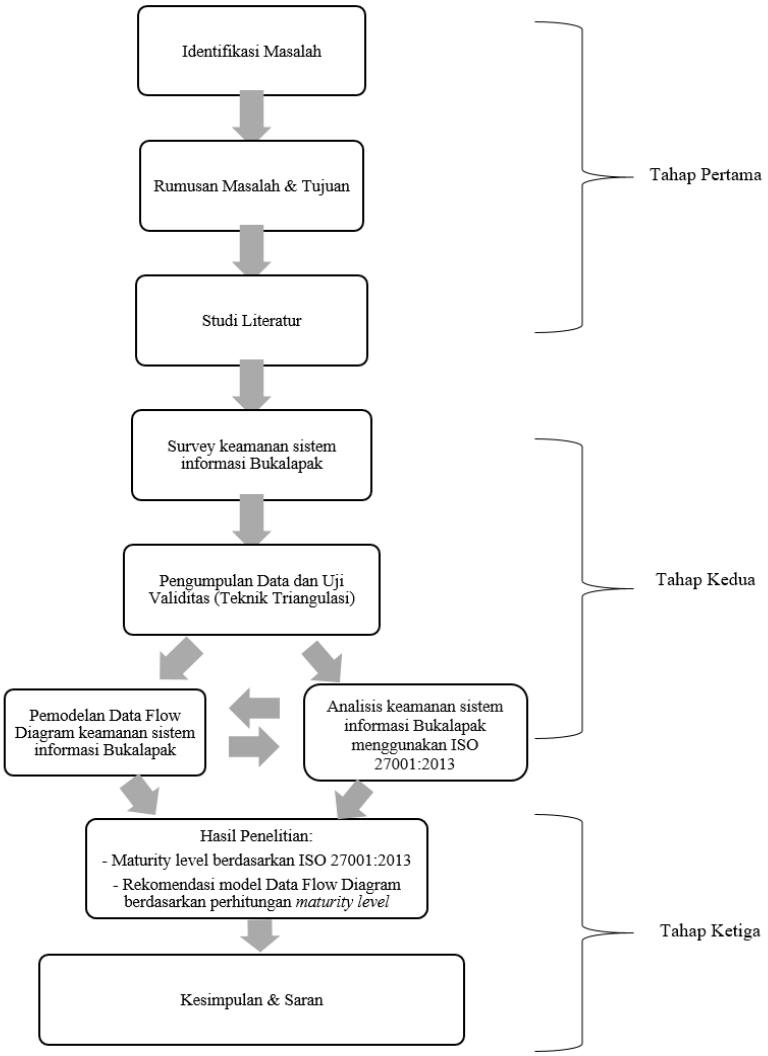


Gambar 1. Konsistensi CD-DFD-ERD [7], [8].

2.4. Tahapan Penelitian

Penelitian ini merupakan penelitian kualitatif deskriptif dengan metode pengumpulan data menggunakan teknik triangulasi. Triangulasi teknik merupakan penggunaan teknik pengumpulan data yang berbeda-beda untuk mendapatkan data dari sumber yang sama dengan menggunakan wawancara, observasi, serta dokumentasi secara serempak [9]. Lingkup penelitian yang ditetapkan ialah pada sistem manajemen keamanan informasi transaksi jual-beli antara penjual dan pelanggan.

Tahapan penelitian ini diawali dengan melakukan wawancara, observasi, sekaligus studi dokumen tentang sistem manajemen keamanan informasi di PT. XYZ dalam lingkup transaksi jual-beli antara penjual dan pelanggan yang mengacu pada ISO/IEC 27001:2013 klausul A.5 Kebijakan Keamanan, A.6 Organisasi Keamanan Informasi, A.7 Keamanan Sumber Daya Manusia, A.9 Kendali Akses, A.10 Kriptografi, A.13 Keamanan Komunikasi, A.14 Akuisisi, Pengembangan, dan Peningkatan Sistem, A.16 Manajemen Insiden Keamanan Informasi, dan A.17 Manajemen Aspek Keamanan Informasi dari Keberlangsungan Bisnis.



Gambar 2. Tahapan penelitian.

Daftar klausul tersebut dipilih berdasarkan keperluan penilaian sistem manajemen keamanan informasi yang berlaku di PT. XYZ serta berkaitan dengan keberlangsungan keamanan informasi transaksi jual-beli antara penjual dan pelanggan. Kemudian observasi dilakukan guna untuk mengetahui kondisi lapangan secara langsung mengenai sistem manajemen keamanan informasi yang telah diterapkan oleh PT. XYZ serta membantu pemberian nilai *maturity level* pada kontrol objektif tersebut. Sedangkan studi dokumen merupakan alat pelengkap yang digunakan dalam penelitian kualitatif untuk menjamin keabsahan penelitian. Hasil dari penilaian *maturity* level sistem manajemen keamanan informasi perusahaan terhadap ISO 27001:2013 yang diperoleh akan dibandingkan dengan *benchmark* yang telah ditentukan pada Tabel 1 [3].

Tabel 1. *Benchmark score*.

Maturity level di bawah 1.65	Organisasi harus mulai menerapkan langkah-langkah keamanan secara keseluruhan
Maturity level antara 1.66 dan 3.25	Organisasi telah mengambil langkah signifikan untuk meningkatkan keamanan.
Maturity level di atas 3.26	Organisasi memenuhi langkah-langkah yang ditetapkan, sehingga probabilitas risiko tinggi adalah marginal

Hasil wawancara, observasi, dan studi dokumen akan diolah ke dalam *work paper gap analysis* untuk melihat kesesuaian antara sistem yang berlaku di PT. XYZ dengan ISO 27001:2013 melalui metode *Gap Analysis* dengan menggunakan kategori yang dijabarkan pada Tabel 2 [3].

Tabel 2. *Compliance*.

Item	Definisi
Compliant	Organisasi sepenuhnya patuh dengan standar ISO 27001:2013
Partially Compliant	Organisasi telah melakukan beberapa cara untuk patuh namun tetap membutuhkan pekerjaan tambahan untuk dilakukan
Noncompliant	Organisasi tidak mematuhi kontrol dari persyaratan ISO 27001:2013

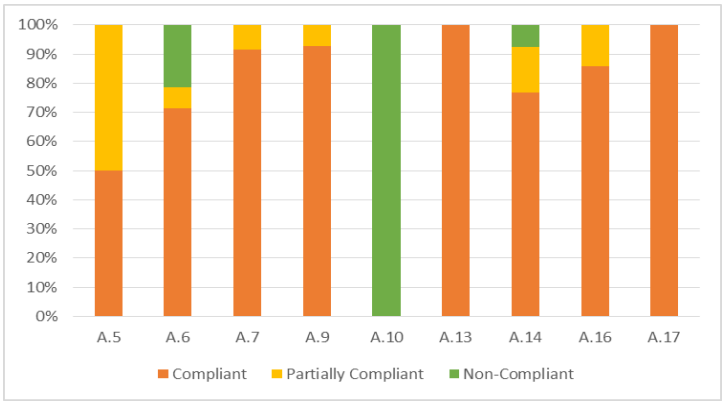
Selanjutnya dilakukan penilaian tingkat kematangannya (*Maturity level*) menggunakan COBIT model. Kemudian aliran data yang telah dikumpulkan tentang sistem manajemen keamanan informasi dalam lingkup transaksi antara pelapak dengan pelanggan dibentuk ke dalam pemodelan *Data Flow Diagram*.

Hasil penelitian akan berbentuk pemodelan aliran data informasi transaksi jual-beli antara pelapak dan pelanggan dalam bentuk *Data Flow Diagram* dan *maturity level* sistem manajemen keamanan informasi PT. XYZ dalam lingkup transaksi jual-beli antara pelapak dan pelanggan yang mengacu pada ISO 27001:2013. Hasil penelitian tersebut kemudian dijadikan landasan untuk mengetahui kekurangan pada sistem manajemen keamanan informasi pada PT. XYZ. Tahap terakhir adalah membuat kesimpulan dan saran dari analisis yang didapat dari hasil penelitian. Bentuk saran yang diberikan merupakan rekomendasi sebagai solusi dalam kekurangan sistem manajemen keamanan informasi PT. XYZ dalam transaksi jual beli antara pelapak dan pelanggan serta rekomendasi perbaikan sistem manajemen keamanan informasi dengan menggunakan kolaborasi antara pemodelan *Data Flow Diagram* dengan hasil *maturity level* sistem manajemen keamanan informasi PT. XYZ dalam transaksi jual beli antara pelapak dan pelanggan yang mengacu pada ISO 27001:2013.

3. Hasil dan Pembahasan

3.1. *Gap Analysis*

Berdasarkan domain tingkat pemenuhan oleh perusahaan di atas, dapat diketahui bahwa perusahaan tidak memenuhi kontrol ISO 27001:2013 pada kontrol Kriptografi (A.10). Hal tersebut disebabkan perusahaan tidak memiliki kebijakan terhadap penggunaan kendali kriptografi maupun siklus hidup kriptografi terkait transaksi jual-beli antara pelapak dan pelanggan meskipun perusahaan telah melakukan enkripsi sebagai metode perlindungan informasi. Sedangkan menurut persyaratan ISO 27001:2013 kebijakan terhadap penggunaan kendali kriptografi untuk melindungi informasi haruslah diimplementasikan dan dikembangkan dan kebijakan, perlindungan, serta siklus hidup kunci kriptografi harus dikembangkan dan diimplementasikan dalam seluruh siklus hidupnya.



Gambar 3. Persentase *compliance.*

Selain itu, perusahaan tidak memenuhi kontrol Organisasi Keamanan informasi (A.6) sebesar 21.4% dan Akuisisi, Pengembangan, dan Peningkatan Sistem (A.14) sebesar 7.7%. Hal tersebut dikarenakan pada kontrol Organisasi Keamanan informasi (A.6) perusahaan diketahui tidak menjalankan kontak dengan kelompok minat khusus dan tidak adanya dokumentasi ketika perusahaan menjalin kontak dengan pihak berwenang terkait transaksi jual-beli antara pelapak dan pelanggan. Sementara menurut persyaratan ISO 27001:2013, Perusahaan harus menjalani kontak yang baik dengan kelompok minat khusus seperti kelompok spesialis keamanan dan asosiasi profesional harus ditingkatkan. Sedangkan pada Akuisisi, Pengembangan, dan Peningkatan Sistem (A.14) perusahaan tidak memenuhi kontrol tersebut sebesar 7.7% dikarenakan perusahaan tidak melakukan pengembangan sistem terkait transaksi jual-beli antara pelapak

dan pelanggan oleh pihak ketiga atau dialihdayakan sehingga perusahaan tidak menetapkan kebijakan yang membahas tentang hal tersebut.

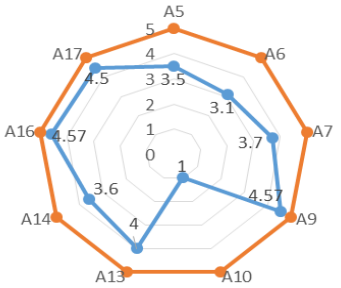
Sementara itu, nilai *Compliant* terbesar yang dimiliki oleh sistem manajemen keamanan informasi perusahaan terdapat pada kontrol Keamanan Komunikasi (A.13) dan Aspek Keamanan Informasi pada Manajemen Keberlangsungan Bisnis (A.17) yaitu masing-masing memiliki nilai sebesar 100%. Pada kedua kontrol objektif tersebut, perusahaan telah memenuhi sepenuhnya persyaratan yang dijabarkan oleh ISO 27001:2013. Hal tersebut menjelaskan bahwa perusahaan lebih terfokus pada kepentingan keamanan komunikasi di dalam perusahaan dan keamanan informasi dalam keberlangsungan bisnis jangka panjang dalam kondisi apa pun terkait transaksi jual-beli antara pelapak dan pelanggan.

Dalam kontrol yang lainnya, perusahaan sudah memenuhi persyaratan yang dijabarkan oleh ISO 27001:2013 namun belum sepenuhnya. Dalam kontrol Kebijakan Keamanan Informasi (A.5), pemenuhan sistem keamanan informasi yang diterapkan oleh perusahaan hanya 50%. Hal tersebut disebabkan perusahaan masih belum mengembangkan beberapa kebijakan keamanan informasi, salah satunya adalah kebijakan penggunaan kriptografi. Pada kontrol Keamanan Sumber Daya Manusia (A.7) tingkat *Compliant* perusahaan terhadap persyaratan ISO 27001:2013 adalah sebesar 91.7% dan nilai *Partially Compliant* sebesar 8.3%. Hal tersebut dikarenakan tidak adanya kontrol oleh perusahaan setelah pegawai perusahaan berhenti bekerja 1 minggu dari tanggal pemberhentian kerja. Pada kontrol *Kontrol* Akses (A.9) tingkat *Compliant* perusahaan terhadap persyaratan ISO 27001:2013 adalah sebesar 92.9% dan nilai *Partially Compliant* sebesar 7.1%. Hal tersebut disebabkan tidak adanya dokumentasi yang menjabarkan kebijakan kontrol akses perusahaan secara spesifik. Sementara pada kontrol Manajemen Insiden di Keamanan Informasi (A.16), perusahaan memiliki nilai *Compliant* sebesar 85.7% dan *Partially Compliant* sebesar 14.3%. Hal tersebut dikarenakan tidak adanya dokumentasi yang menjelaskan prosedur penilaian dan keputusan kejadian saat terjadi insiden.

Dari hasil analisis tersebut dapat disimpulkan bahwa perusahaan sudah hampir memenuhi kontrol Kebijakan Keamanan Informasi, Keamanan Sumber Daya Manusia, Kontrol Akses, dan Manajemen Insiden di Keamanan Informasi terkait dengan transaksi jual-beli antara pelapak dan pelanggan namun masih ada upaya yang harus dilakukan agar perusahaan sepenuhnya mematuhi persyaratan ISO 27001:2013.

3.2. *Maturity Level*

Berdasarkan Gambar 3, dapat diketahui bahwa Klausul Kebijakan Keamanan Informasi (A.5) memiliki nilai tingkat kematangan sebesar 3.5, Klausul Organisasi Keamanan Informasi (A.6) memiliki nilai tingkat kematangan sebesar 3.1, Klausul Keamanan Sumber Daya Manusia (A.7) memiliki nilai tingkat kematangan sebesar 3.7, Klausul Kontrol Akses (A.9) memiliki nilai tingkat kematangan sebesar 4.57, Klausul Kriptografi (A.10) memiliki nilai tingkat kematangan sebesar 1, Klausul Keamanan Komunikasi (A.13) memiliki nilai tingkat kematangan sebesar 4, Klausul Akuisisi, Pengembangan, dan Peningkatan Sistem (A.14) memiliki nilai tingkat kematangan sebesar 3.6, Klausul Manajemen Insiden Keamanan Informasi (A.16) memiliki nilai tingkat kematangan sebesar 4.57, dan Klausul Aspek Keamanan Informasi dalam Manajemen Keberlangsungan Bisnis (A.17) memiliki nilai tingkat kematangan sebesar 4.5.



Gambar 4. *Maturity level*.

Masih merujuk Gambar 4, diketahui Sistem manajemen keamanan informasi PT. XYZ dalam konteks Kebijakan Keamanan Informasi (A.5), Keamanan Sumber Daya Manusia (A.7), Kontrol Akses (A.9), Keamanan Komunikasi (A.13), Akuisisi, Pengembangan, dan Peningkatan Sistem (A.14), dan Aspek Keamanan Informasi dalam Manajemen Keberlangsungan Bisnis (A.17) memiliki nilai tingkat kematangan di atas 3.26. Hal tersebut menggambarkan bahwa perusahaan sudah memenuhi kebijakan keamanan informasi sesuai dengan ISO 27001:2013, telah memenuhi pengendalian keamanan sumber daya manusia

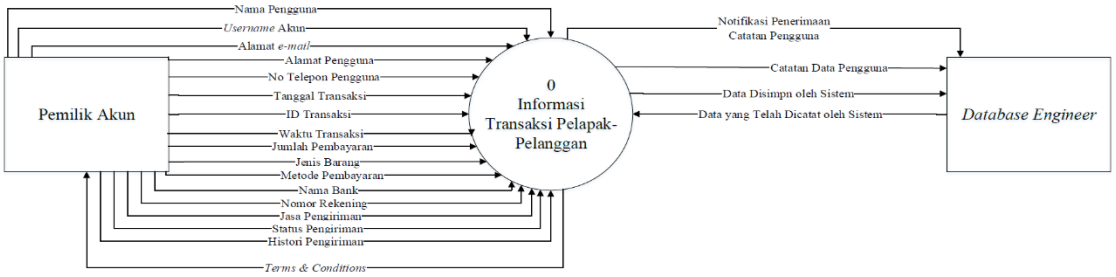
serta keamanan komunikasi dengan baik, telah menerapkan prosedur akuisisi, pengembangan, dan peningkatan sistem perusahaan sesuai dengan standar yang digunakan, serta telah menerapkan manajemen keberlangsungan bisnis dalam aspek keamanan informasi. Perusahaan dinilai telah memenuhi kontrol yang telah dilakukan sehingga meningkatkan kesiapan perusahaan terhadap probabilitas risiko yang akan dihadapi.

Kemudian klausul Manajemen Insiden Keamanan Informasi (A.16) memiliki nilai tingkat kematangan tertinggi yaitu sebesar 4.57. Hal tersebut menggambarkan bahwa sistem manajemen keamanan informasi perusahaan sudah sepenuhnya memenuhi persyaratan ISO 27001:2013. Perusahaan dinilai paling baik dalam menangani manajemen insiden keamanan informasi bila dibandingkan dengan kontrol lainnya. Hal tersebut dapat menandakan bahwa perusahaan paling siap untuk menghadapi risiko yang akan muncul terkait manajemen insiden keamanan informasi.

Selanjutnya Sistem manajemen keamanan informasi PT. XYZ dalam konteks Organisasi Keamanan Informasi (A.6) memiliki nilai yang terketak di antara 1.66-3.25. Hal tersebut menggambarkan bahwa perusahaan masih belum sepenuhnya memenuhi persyaratan ISO 27001:2013 dalam organisasi keamanan informasi meskipun sudah menerapkan langkah yang signifikan untuk meningkatkan organisasi keamanan informasi terkait transaksi jual-beli antara pelapak dan pelanggan. Penyebabnya ialah dikarenakan tidak adanya kontak antara perusahaan dengan kelompok minat khusus serta tidak terdapat dokumentasi kebijakan ketika perusahaan menjalin kontak dengan pihak berwenang terkait transaksi jual-beli antara pelapak dan pelanggan.

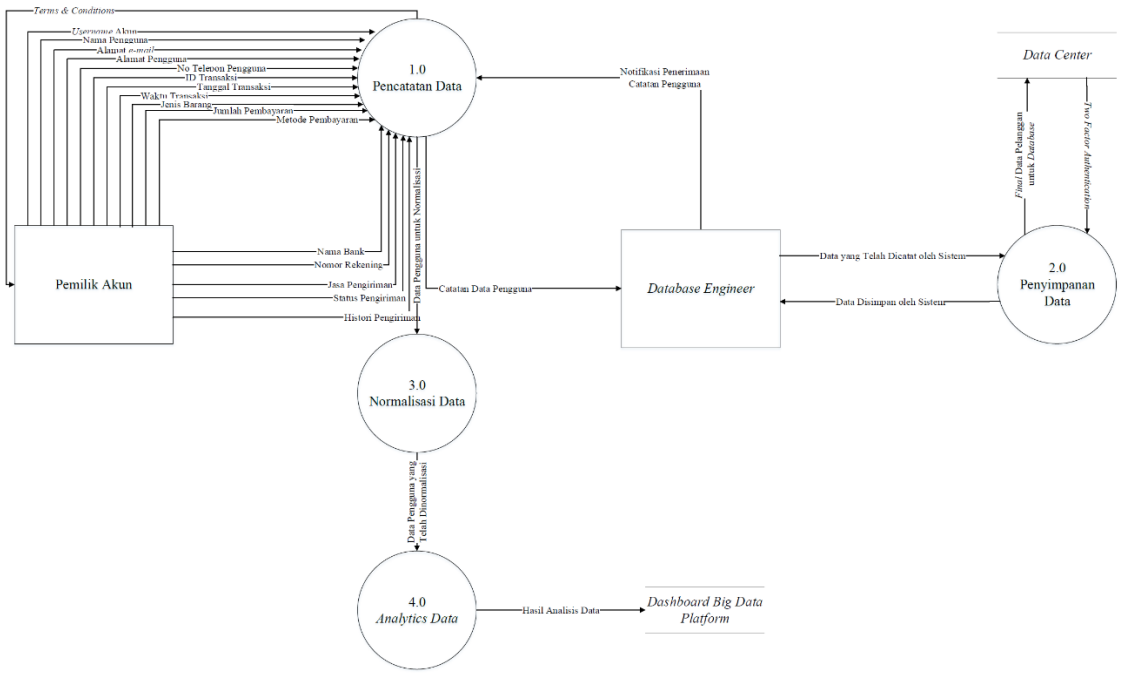
Sistem manajemen keamanan informasi PT. XYZ dalam konteks Kriptografi (A.10) memiliki nilai terkecil yaitu berada di bawah 1.65. Hal tersebut menggambarkan bahwa perusahaan masih sangat jauh untuk memenuhi persyaratan ISO 27001:2013 dalam kontrol kriptografi yang menandakan perusahaan belum memberikan perhatian khusus pada kendali kriptografi untuk informasi transaksi jual-beli antara pelapak dan pelanggan dikarenakan tidak adanya kebijakan atas kendali kriptografi di dalam perusahaan. Maka organisasi harus mulai untuk mengimplementasikan kendali kriptografi agar memenuhi persyaratan keamanan informasi.

3.3. *Existing* CD/DFD



Gambar 5. *Existing context diagram.*

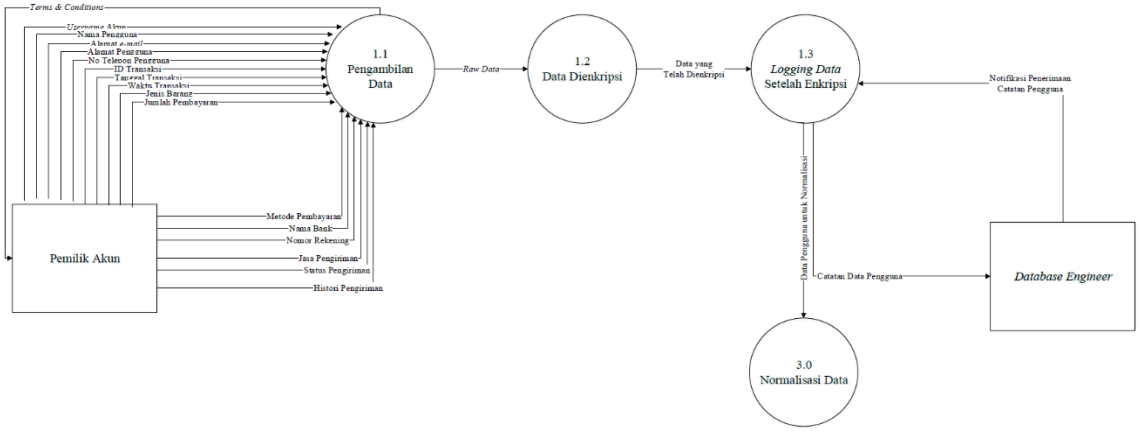
Pada *Context Diagram*, aliran data informasi transaksi jual-beli antara pelapak dan pelanggan di dalam Sistem Manajemen Keamanan Informasi yang diterapkan oleh PT. XYZ digambarkan secara umum. Terdapat dua entitas yang terlibat di dalam aliran data di sistem manajemen keamanan informasi tersebut. Entitas pertama adalah Pemilik Akun yang merupakan pengguna aplikasi PT. XYZ. Entitas kedua adalah *Database Engineer* yang terlibat di dalam sistem manajemen keamanan informasi perusahaan. Aliran data yang digambarkan merupakan data yang terlibat di dalam sistem manajemen keamanan informasi pada transaksi jual-beli antara pelapak dan pelanggan di PT. XYZ. Data yang berasal dari entitas Pemilik Akun menuju proses sistem keamanan informasi perusahaan berupa Nama Pengguna, *Username* Akun, Alamat *e-mail*, Alamat Pengguna, No. Telepon Pengguna, Tanggal Transaksi, ID Transaksi, Waktu Transaksi, Jumlah Pembayaran, Jenis Barang, Metode Pembayaran, Nama Bank, Nomor Rekening, Jasa Pengiriman, Status Pengiriman, Histori Pengiriman. Sedangkan data yang berasal dari sistem menuju entitas Pemilik Akun berupa *Terms & Conditions*. Data yang berasal dari entitas *Database Engineer* menuju proses sistem keamanan informasi perusahaan berupa Data yang Telah Dicatat oleh Sistem. Sedangkan data yang berasal dari proses sistem keamanan informasi perusahaan menuju entitas sistem berupa Notifikasi Penerimaan Catatan Pengguna, Catatan Data Pengguna, serta Data disimpan oleh sistem.



Gambar 6. DFD *Level* 1

Data Flow Diagram level 1 menjabarkan aliran data informasi transaksi jual beli antara pelapak dan pelanggan pada sistem manajemen keamanan informasi di PT. XYZ. Data yang berasal dari entitas Pemilik Akun menuju proses Pencatatan Data berupa Nama Pengguna, *Username* Akun, Alamat *e-mail*, Alamat Pengguna, No. Telepon Pengguna, Tanggal Transaksi, ID Transaksi, Waktu Transaksi, Jumlah Pembayaran, Jenis Barang, Metode Pembayaran, Nama Bank, Nomor Rekening, Jasa Pengiriman, Status Pengiriman, dan Histori Pengiriman. Pada saat yang bersamaan *Terms & Conditions* akan dikirimkan kepada Pemilik Akun sebagai persyaratan dan persetujuan atas data yang telah terlibat dalam transaksi tersebut. Kemudian data yang berasal dari proses Pencatatan Data tersebut akan dikirimkan menuju entitas *Database Engineer* dengan nama Catatan Data Pengguna. Selanjutnya *Database Engineer* akan memberikan Notifikasi Penerimaan Catatan Data Pengguna sebagai isyarat bahwa *Database Engineer* telah menerima seluruh data informasi transaksi dari Pemilik Akun. Data yang telah dicatat oleh *Database Engineer* kemudian diproses dengan nama proses Penyimpanan Data di mana data tersebut akan disimpan di data store bernama Data Center. Ketika data akan disimpan di Data Center, Data Center akan mengirimkan *Two Factor Authentication* berupa *password* dan kode OTP. Setelah data berhasil disimpan di Data Center, maka sistem akan menerima notifikasi bahwa data telah disimpan oleh sistem.

Sementara itu data yang telah dicatat oleh sistem pada proses Pencatatan Data berubah menjadi Data Pengguna untuk Normalisasi dan dikirimkan menuju proses selanjutnya yaitu Normalisasi Data di mana dalam proses tersebut data yang telah diperoleh dari Pemilik Akun akan dinormalisasi untuk dianalisis. Setelah normalisasi data dilakukan, maka data tersebut akan menuju proses *Analytics Data* di mana data tersebut akan dianalisis. Hasil analisis data kemudian akan disimpan di data *store* bernama *Dashboard Big Data Platform* sebagai referensi bagi manajemen.



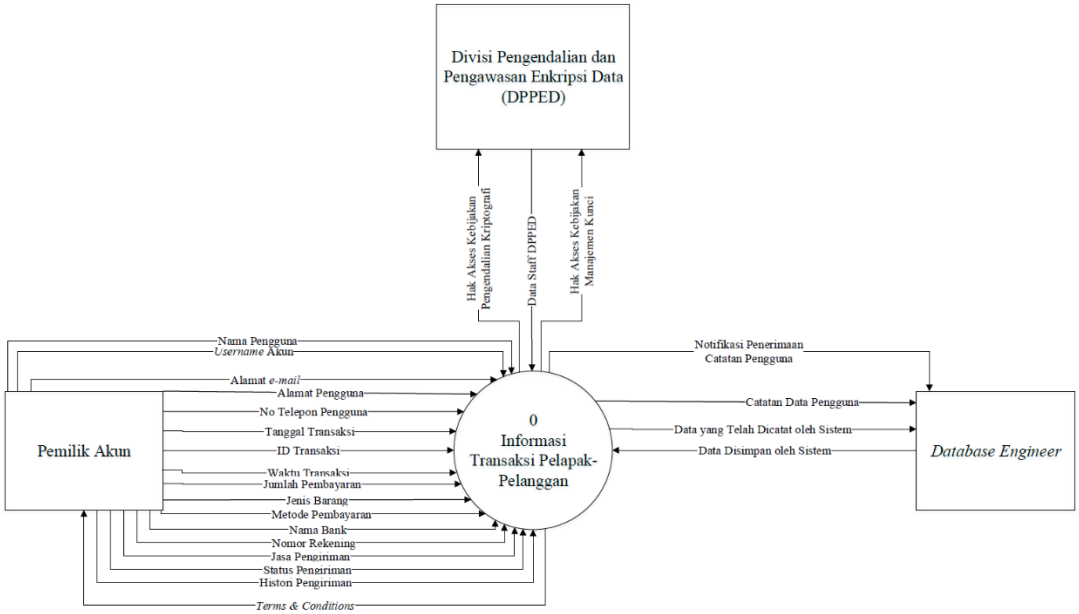
Gambar 7. DFD *level 2*.

Proses yang akan dijabarkan lebih rinci pada level 2 adalah Proses 1 yaitu proses Pencatatan Data. Perincian tersebut didasari oleh penilaian *maturity level* Sistem Manajemen Keamanan Informasi pada transaksi jual-beli antara pelapak dan pelanggan di PT. XYZ. Pada proses Pencatatan Data oleh Sistem terdapat proses Enkripsi Data, di mana pada penilaian *maturity level* yang telah dilakukan klausul Kriptografi memiliki *maturity level* terendah yaitu sebesar senilai 1.

Data yang berasal dari entitas Pemilik Akun menuju proses Pengambilan Data berupa Nama Pengguna, *Username* Akun, Alamat *e-mail*, Alamat Pengguna, No. Telepon Pengguna, Tanggal Transaksi, ID Transaksi, Waktu Transaksi, Jumlah Pembayaran, Jenis Barang, Metode Pembayaran, Nama Bank, Nomor Rekening, Jasa Pengiriman, Status Pengiriman, dan Histori Pengiriman. Sedangkan data yang diberikan kepada Pemilik Akun berupa *Terms & Conditions*. Data yang telah diambil oleh sistem berbentuk *raw data* atau data mentah yang kemudian dilanjutkan ke proses berikutnya yaitu Data Dienkripsi. Pada proses enkripsi data ini, ditemukan temuan bahwa tidak adanya pengawasan, pengendalian, serta manajemen kunci maupun dokumentasi dan kontrol kebijakan yang disyaratkan oleh ISO 27001:2013 sehingga PT. XYZ hanya sekedar melakukan enkripsi data saja. Data yang telah dienkripsi kemudian akan diproses dalam proses *Logging Data* Setelah Enkripsi. Proses tersebut merupakan proses terakhir dalam proses Pencatatan Data dan dilanjutkan menuju proses berikutnya yaitu pengiriman data kepada entitas *Database Engineer* dalam bentuk Catatan Data Pengguna dan dilanjutkan menuju proses berikutnya yaitu Normalisasi Data.

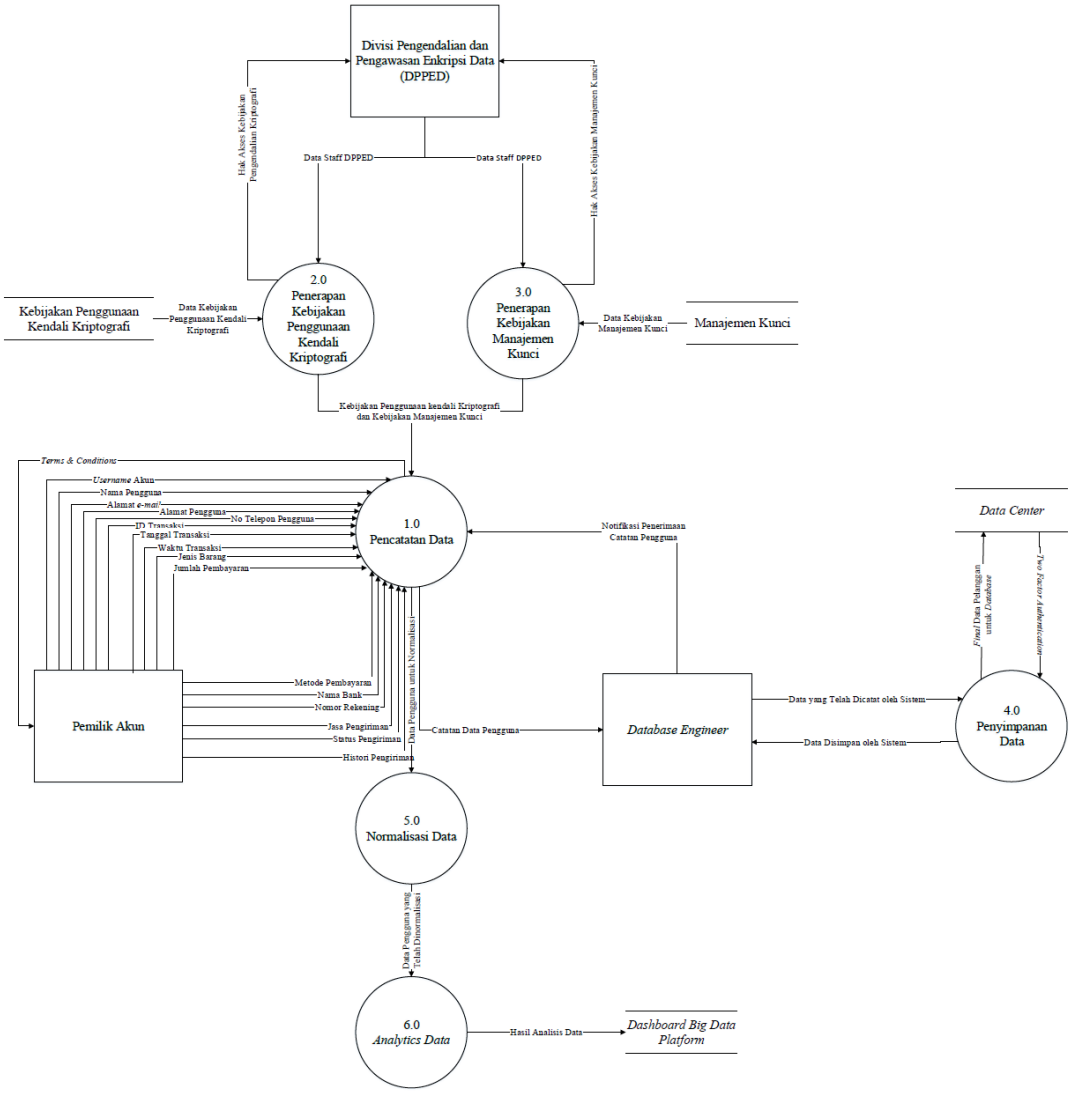
3.4. *Recommendation* CD/DFD

Maturity level pada sistem manajemen keamanan informasi di PT. XYZ terkait transaksi jual-beli antara pelapak dan pelanggan masing-masing klausul menunjukkan bahwa pada beberapa kebijakan PT. XYZ sudah mendekati standar sertifikasi ISO 27001:2013 namun dalam beberapa kebijakan lainnya PT. XYZ masih dinilai jauh untuk memenuhi standar sertifikasi ISO 27001:2013 terutama dalam kebijakan Kriptografi (A.10). Hal ini dapat mengancam keamanan informasi transaksi jual-beli antara pelapak dan pelanggan ketika dicatat oleh sistem mengingat tidak adanya kebijakan yang mengendalikan penggunaan enkripsi beserta kontrol terhadap penggunaan enkripsi tersebut. ISO 27001:2013 mensyaratkan kebijakan terhadap penggunaan kendali kriptografi untuk melindungi informasi serta siklus hidup kunci kriptografi haruslah diimplementasikan dan dikembangkan dalam seluruh siklus hidupnya sementara PT. XYZ belum menerapkan kebijakan tersebut dalam keamanan informasi transaksi jual-beli antara pelapak dan pelanggan. Oleh karena itu, pemodelan sistem dengan menggunakan *Data Flow Diagram* difokuskan pada Kendali Kriptografi dalam sistem manajemen keamanan informasi di PT. XYZ dalam lingkup aliran data informasi transaksi jual-beli antara pelapak dan pelanggan.



Gambar 8. Rekomendasi pemodelan *context diagram.*

Pada pemodelan *Context Diagram* yang direkomendasikan, aliran data informasi transaksi jual-beli antara pelapak dan pelanggan di dalam Sistem Manajemen Keamanan Informasi untuk PT. XYZ digambarkan secara umum. Terdapat tiga entitas yang terlibat di dalam pemodelan aliran data di sistem manajemen keamanan informasi tersebut. Entitas pertama adalah Pemilik Akun yang merupakan pengguna aplikasi PT. XYZ. Entitas kedua merupakan Divisi Pengendalian dan Pengawasan Enkripsi Data (DPPED) yang merupakan pengawas dan pengendali dari proses enkripsi yang akan dilakukan. Entitas ketiga adalah *Database Engineer* yang terlibat di dalam sistem manajemen keamanan informasi perusahaan. Aliran data yang digambarkan merupakan data yang terlibat di dalam sistem manajemen keamanan informasi pada transaksi jual-beli antara pelapak dan pelanggan di PT. XYZ. Data yang berasal dari entitas Pemilik Akun menuju proses sistem keamanan informasi perusahaan berupa Nama Pengguna, *Username* Akun, Alamat *e-mail*, Alamat Pengguna, No. Telepon Pengguna, Tanggal Transaksi, ID Transaksi, Waktu Transaksi, Jumlah Pembayaran, Jenis Barang, Metode Pembayaran, Nama Bank, Nomor Rekening, Jasa Pengiriman, Status Pengiriman, Histori Pengiriman. Sedangkan data yang berasal dari sistem menuju entitas Pemilik Akun merupakan *Terms & Conditions*. Data yang berasal dari entitas Divisi Pengendalian dan Pengawasan Enkripsi Data (DPPED) menuju proses sistem keamanan informasi perusahaan yaitu data staf DPPED. Sedangkan data yang berasal dari proses sistem keamanan informasi perusahaan menuju entitas Divisi Pengendalian dan Pengawasan Enkripsi Data (DPPED) adalah Hak Akses Kebijakan Pengendalian Kriptografi dan Hak Akses Kebijakan Manajemen Kunci. Data yang berasal dari entitas *Database Engineer* menuju proses sistem keamanan informasi perusahaan berupa Data yang Disimpan oleh Sistem. Sedangkan data yang berasal dari proses sistem keamanan informasi perusahaan menuju entitas *Database Engineer* berupa Notifikasi Penerimaan Catatan Pengguna, Catatan Data Pengguna, dan Data yang Telah Dicatat oleh Sistem.



Gambar 9. Rekomendasi pemodelan DFD *level 1*.

Data yang berasal dari entitas Pemilik Akun menuju proses sistem keamanan informasi perusahaan berupa Nama Pengguna, *Username* Akun, Alamat *e-mail*, Alamat Pengguna, No. Telepon Pengguna, Tanggal Transaksi, ID Transaksi, Waktu Transaksi, Jumlah Pembayaran, Jenis Barang, Metode Pembayaran, Nama Bank, Nomor Rekening, Jasa Pengiriman, Status Pengiriman, dan Histori Pengiriman akan menuju pada proses pertama yaitu Pencatatan Data. Pada saat yang bersamaan, entitas Pemilik Akun akan menerima data berupa *Terms & Conditions* yang merupakan persyaratan serta persetujuan penyimpanan data yang terlibat dalam transaksi tersebut. Selanjutnya Divisi Pengendalian dan Pengawasan Enkripsi Data (DPEED) akan melakukan Penerapan Kebijakan Penggunaan Kendali Kriptografi yang didasari oleh Kebijakan Penggunaan Kendali Kriptografi serta melakukan Penerapan Manajemen Kunci yang didasari oleh Manajemen Kunci pada proses Pencatatan Data. Kemudian Catatan Data Pengguna akan dikirimkan menuju entitas *Database Engineer* dan *Database Engineer* akan memberikan Notifikasi Penerimaan Catatan Pengguna. Data yang Telah Dicatat oleh Sistem kemudian akan dilanjutkan menuju proses Penyimpanan Data untuk kemudian disimpan di *Data Center*. Saat data akan disimpan di *Data Center*, *Data Center* akan mengirimkan *two factor authentication* sebagai persyaratan akses penyimpanan data dalam bentuk *password* dan OTP. Kemudian data berhasil disimpan oleh sistem. Selain itu data yang telah dicatat oleh sistem pada proses Pencatatan Data berubah menjadi Data Pengguna untuk Normalisasi dan dikirimkan menuju proses selanjutnya yaitu Normalisasi Data di mana dalam proses tersebut data yang telah diperoleh dari Pemilik Akun akan dinormalisasi untuk dianalisis. Setelah normalisasi data dilakukan, maka data tersebut akan menuju proses *Analytics Data* di mana data tersebut akan dianalisis. Hasil analisis

data kemudian akan disimpan di *data store* bernama *Dashboard Big Data Platform* sebagai referensi bagi manajemen.

Merujuk Gambar 9, maka rekomendasi pemodelan yang akan dijabarkan lebih rinci untuk *level* 2, yaitu Proses 1 Pencatatan Data. Pada *level* 2, Proses ini menjadi tiga sub proses yang terdiri dari Pengambilan Data, Data Dienkripsi, dan *Logging Data* Setelah Enkripsi. Perincian tersebut didasari oleh penilaian *maturity level* Sistem Manajemen Keamanan Informasi pada transaksi jual-beli antara pelapak dan pelanggan di PT. XYZ. Pada proses Pencatatan Data oleh Sistem terdapat proses Enkripsi Data, di mana pada penilaian *maturity level* yang telah dilakukan klausul Kriptografi memiliki *maturity level* terendah yaitu senilai 1. Sehingga solusi untuk meningkatkan nilai *maturity level* pada klausul Kriptografi tersebut dijabarkan dengan merincikan proses 1. Data yang berasal dari entitas Pemilik Akun menuju proses Pengambilan Data berupa Nama Pengguna, *Username* Akun, Alamat *e-mail*, Alamat Pengguna, No. Telepon Pengguna, Tanggal Transaksi, ID Transaksi, Waktu Transaksi, Jumlah Pembayaran, Jenis Barang, Metode Pembayaran, Nama Bank, Nomor Rekening, Jasa Pengiriman, Status Pengiriman, dan Histori Pengiriman. Sedangkan data yang diterima oleh Pemilik Akun berupa *Terms & Conditions*. Data yang telah diambil oleh sistem berbentuk *raw data* atau data mentah yang kemudian dilanjutkan ke proses berikutnya yaitu Data Dienkripsi. Saat Data Dienkripsi, dilakukan Penerapan Kebijakan Penggunaan Kendali Kriptografi serta Penerapan Manajemen Kunci. Setelah Data Dienkripsi proses selanjutnya adalah *Logging Data* Setelah Enkripsi. Lalu entitas *Database Engineer* akan menerima Catatan Data Pengguna dan akan mengirimkan Notifikasi Penerimaan Catatan Pengguna. Proses tersebut merupakan proses terakhir dalam proses Pencatatan Data dan dilanjutkan menuju proses berikutnya yaitu pengiriman data kepada entitas *Database Engineer* dalam bentuk Catatan Data Pengguna dan dilanjutkan menuju proses berikutnya yaitu Normalisasi Data.

4. Simpulan

Maturity level pada sistem manajemen keamanan informasi di PT.XYZ, yang terkait transaksi jual-beli antara pelapak dan pelanggan masing-masing klausul menunjukkan bahwa pada beberapa kebijakan, PT.XYZ sudah mendekati standar sertifikasi ISO 27001:2013. Namun, dalam beberapa kebijakan lainnya PT.XYZ masih dinilai tidak memenuhi standar sertifikasi ISO 27001:2013 terutama dalam kebijakan Kriptografi (A.10). Hal ini dapat mengancam keamanan informasi transaksi jual-beli antara pelapak dan pelanggan ketika dicatat oleh sistem mengingat tidak adanya kebijakan yang mengendalikan penggunaan enkripsi beserta kontrol terhadap penggunaan enkripsi tersebut.

Berdasarkan hasil penilaian *maturity level* pada sistem yang sedang terjadi, ditemukan ketidaksesuaian antara kebijakan Kriptografi yang disyaratkan oleh ISO 27001:2013 dengan penerapan kriptografi pada sistem manajemen keamanan informasi di PT.XYZ. Hal tersebut dapat dicermati dari pemodelan Data Flow Diagram yang terdiri dari dua entitas yaitu: Pemilik Akun dan *Database Engineer*. Selain itu, terdapat dua *data store* yang terlibat, yaitu *Data Center* dan *Dashboard* Big Data Platform. Proses tersebut dirinci hingga *level* 2 yang terfokus pada proses enkripsi.

Berdasarkan perhitungan *maturity level* yang telah dilakukan, rekomendasi pemodelan sistem dengan menggunakan *Data Flow Diagram* difokuskan pada Enkripsi Data dalam sistem manajemen keamanan informasi di PT.XYZ dalam lingkup aliran data informasi transaksi jual-beli antara pelapak dan pelanggan. Rekomendasi *Data Flow Diagram* dibuat berdasarkan validasi hasil *maturity level* pada klausul A.10 yang memiliki nilai paling rendah, yaitu bernilai 1. Sehingga pemodelannya terdiri dari tiga entitas yaitu: Pemilik Akun, *Database Engineer*, dan DPPED. Selain itu, terdapat empat *data store* yaitu: Kebijakan Penggunaan Kendali Kriptografi, Manajemen Kunci, *Data Center*, dan *Dashboard Big Data Platform*. Proses tersebut dirinci hingga level 2 yang terfokus pada proses enkripsi.

Daftar Pustaka

[1] A. N. Singh and M. P. Gupta, "I*dentifying factors of ' organizational information security management* ,'" *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 644–667, 2014.

[2] Yuze, Y., Priyadi, Y., & Candiwan, C. Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 : 2013 Serta Rekomendasi Model Sistem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi. JSINBIS (Jurnal Sistem Informasi Bisnis), 2016, 6(1), 38-45. doi:http://dx.doi.org/10.21456/vol6iss1pp38-45.

[3] Al-mayahi and S. P. Mansoor, "*ISO 27001 Gap Analysis - Case Study*" *Int. Conf. Secur. Manag. (SAM' 12), Las Vegas*, 2012.

[4] Sarno, R. dan Iffano, I. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press. 2009.

[5] International Standard Organization. *ISO/IEC 27001 Information Technology, Security Techniques - Information Security Management System-Requierements.* Switzerland : International Standard

Organization. 2013.
[6] Yourdon. *Just Enough Structured Analysis*. Website : www.yourdon.com. 2006. Diakses tanggal 14 Oktober 2018.
[7] Y. Priyadi. Kolaborasi SQL & ERD Dalam Implementasi Database (Edisi I). Yogyalarta: Andi. 2014.
[8] Hapsari, K., & Priyadi, Y. Perancangan Model Data Flow Diagram Untuk Mengukur Kualitas Website Menggunakan Webqual 4.0. JSINBIS (Jurnal Sistem Informasi Bisnis), 2017, 7(1), 66-72. doi:http://dx.doi.org/10.21456/vol7iss1pp66-72.
[9] Sugiyono. Metode Penelitian Kuantitatif Kualitatif dan R&D. Penerbit Alfabeta. 2017.