Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 : 2013 Serta Rekomendasi Model Sistem Menggunakan *Data Flow Diagram* pada Direktorat Sistem Informasi Perguruan Tinggi

Yuni Cintia Yuze[a*], Yudi Priyadi[b], Candiwan[c]

[abc]Program Studi Manajemen Bisnis Telekomunikasi dan Informatika,
Fakultas Ekonomi dan Bisnis, Universitas Telkom

Naskah Diterima : 14 Januari 2016; Diterima Publikasi : 15 Maret 2016

DOI: 10.21456/vol6iss1pp38-45

Abstract

The importance of information and the possible risk of disruption, therefore the universities need to designed and implemented of the information security. One of the standards that can be used to analyze the *level* of information security in the organization is ISO/IEC 27001 : 2013 and this standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The objective of this research is to measure the *level* of information security based on standard ISO/IEC 27001: 2013 and modeling systems for information security management. This research uses descriptive qualitative approach, data collection and validation techniques with tringulasi (interview, observation and documentation). Data was analyzed using gap analysis and to measure the *level* of maturity this research uses SSE-CMM (Systems Security Engineering Capability Maturity Model). Based on the research results, Maturity *level* clause Information Security Policy reaches *level* 1 (Performed-Informally), clause Asset Management reaches *level* 3 (Well-Defined), clause Access Control reaches *level* 3 (Well-Defined), clause Physical and Environmental Security reaches *level* 3 (Well-Defined), clause Operational Security reaches *level* 3 (Well-Defined), Communication Security clause reaches the *level* 2 (Planned and Tracked). Based on the results of maturity *level* discovery of some weakness in asset management in implementing the policy. Therefore, the modeling system using the flow map and CD / DFD focused on Asset Management System.

Keywords : Analysis Information Security*;* ISO/IEC 27001 : 2013; Maturity *Level;* SSE-CMM; CD/DFD

Abstrak

Pentingnya informasi dan adanya kemungkinan risiko terjadi gangguan, oleh karena itu perguruan tinggi perlu untuk merancang dan mengimplementasikan keamanan informasi. Salah satu standar yang dapat digunakan untuk menganalisa tingkat keamanan informasi di organisasi adalah ISO/IEC 27001 dan standar ini telah disiapkan untuk menyediakan persyaratan untuk membuat, mengimplemetasikan dan meningkatkan secara berkelanjutan sistem manajemen keamanan informasi. Tujuan dari penelitian ini adalah untuk mengukur tingkat keamanan informasi berdasarkan standar ISO/IEC 27001 : 2013 dan pemodelan sistem manajemen keamanan informasi. Penelitian ini menggunakan jenis pendekatan kualitatif deskriptif, teknik pengumpulan dan validasi data dengan teknik tringulasi (wawancara, observasi dan dokumentasi). Analisis data dilakukan dengan *gap analysis* dan untuk mengukur tingkat kematangan penelitian ini mengunakan SSE-CMM *(Systems Security Engineering Capability Maturity Model*). Berdasarkan hasil penelitian, *maturity level* pada klausul kebijakan keamanan informasi mencapai *level* 1 (*Performed-Informally*), klausul manajemen aset mencapai *level* 3 (*Well-Defined*), klausul kontrol akses mencapai *level* 3 (*Well-Defined*), klausul keamanan fisik dan lingkungan mencapai *level* 3 (*Well-Defined*), klausul keamanan operasional mencapai *level* 3 (*Well-Defined*), klausul keamanan komunikasi mencapai *level* 2 (*Planned and Tracked*). Berdasarkan hasil penilaian *maturity level* ditemukan beberapa kekurangan pada manajemen aset dalam mengimplementasikan kebijakan. Oleh karena itu, pemodelan sistem dengan menggunakan *flow map* dan CD/DFD difokuskan pada sistem manajemen aset.

Kata Kunci : Analisis Keamanan Informasi; ISO/IEC 27001 : 2013; *Maturity Level*; SSE-CMM; CD/DFD

1. Pendahuluan

Perguruan tinggi merupakan salah satu instansi penyelenggaraan pelayanan publik, dimana perguruan tinggi dituntut memberikan pelayanan terbaik untuk pihak yang membutuhkan informasi, seperti mahasiswa, karyawan, ataupun pihak lainnya. Oleh karena itu, perguruan tinggi membentuk divisi

*) Penulis korespondensi: chintyayuze@gmail.com

khusus yang melayani sistem manajemen informasi dan layanan interkoneksi universitas. Seiring dengan perkembangan teknologi informasi, menurut Darmawan dan Fauzi (2013) menjadikan informasi menjadi aset penting karena selain bersifat rahasia, informasi juga memiliki risiko dari akses tidak sah, modifikasi data, pencurian data, *human error*, kerusakan *hardware & software*, maupun risiko dari bencana alam.

Berdasarkan data dari *Data Loss DB* (2015) sampai dengan bulan Oktober 2015 tercatat telah terjadi 1.416 insiden terkait dengan keamanan informasi pada organisasi swasta maupun pemerintah, 12% dari insiden tersebut terjadi pada sektor pendidikan. Berdasarkan survei yang dilakukan oleh *Verizon* (2014) selama sepuluh tahun terakhir menyimpulkan bahwa tiga jenis insiden yang terjadi dalam bidang pendidikan yaitu *miscellaneous errors* (20%), *web app attacks* (20%), dan *physical theft/loss* (19%).

Mengingat pentingnya informasi dan tingginya kemungkinan risiko terjadi gangguan, perguruan tinggi perlu untuk melakukan kegiatan tata kelola keamanan informasi dilingkungannya. Salah satu standar yang dapat digunakan untuk menganalisa tingkat keamanan informasi di organisasi adalah standar ISO/IEC 27001 sesuai dengan insiden yang banyak terjadi berkaitan dengan bidang pendidikan. Penelitian ini melakukan pengukuran tingkat keamanan informasi yang dilakukan untuk menganalisa sejauh mana perguruan tinggi telah mengamankan informasi dilingkungannya. Dari analisa tingkat keamanan, perguruan tinggi dapat melakukan evaluasi dan perancangan ataupun pembaharuan sistem manajemen keamanan informasi di perguruan tinggi tersebut. Dalam jurnal internasional *Information Security Management System Standards : A Comparative Study of Big Five* Susanto et al (2011), menjelaskan bahwa ISO/IEC 27001 menjadi *framework* yang paling banyak digunakan oleh organisasi oleh karena itu pengukuran tingkat kematangan akan dilakukan dengan mengacu pada ISO/IEC 27001 dan mengacu pada kriteria penilaian kematangan dengan menggunakan SSE-CMM. Tujuan penelitian ini yaitu untuk menganalisis tingkat keamanan informasi mengacu pada ISO/IEC 27001 terkait dengan manajemen aset, kontrol akses, keamanan fisik dan lingkungan, dan keamanan operasional serta keamanan komunikasi serta menganalisis alur kegiatan dan merancang aliran data sistem manajemen keamanan informasi akademik dengan menggunakan CD/DFD (*Context Diagram/Data Flow Diagram*) dari penilaian tingkat kematangan klausul tersebut. Perancangan aliran data sistem manajemen keamanan informasi diutamakan kepada kaulus/kontrol yang dinilai memiliki nilai kematangan dan hasil observasi yang kurang.

2. Kerangka Teori

Menurut Darmawan (2013) informasi merupakan hasil dari pengolahan data yang dapat memberikan makna atau arti serta bermanfaat bagi seseorang. Menurut Laudon (2007) sistem informasi didefinisikan secara teknis sebagai serangkaian komponen yang saling berhubungan yang mengumpulkan, mengolah, menyimpan, dan mendistribusikan informasi untuk mendukung pengambilan keputusan dan kontrol di dalam sebuah organisasi. Menurut Weber (dalam Sutabri, 2012) audit sistem informasi merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem yang digunakan telah dapat melindungi aset, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien.

Menurut ISO/IEC 27002 (2005) keamanan informasi adalah perlindungan informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis, meminimalkan risiko bisnis, dan memaksimalkan laba atas investasi dan peluang bisnis. Dalam ISO/IEC 27001 (2013) sistem manajemen keamanan informasi menjaga kerahasiaan, integritas dan ketersediaan informasi dengan menerapkan proses manajemen risiko dan meyakinkan pihak yang berkepentingan bahwa risiko dikelola dengan baik. Sistem manajemen keamanan informasi merupakan bagian dari dan terintegrasi dengan proses organisasi dan struktur manajemen secara keseluruhan.

Context *Diagram* (CD) adalah *top level* atau sering dikenal *level* 0 dari DFD. Pada CD, sistem digambarkan dengan sebuah proses, kemudian entitas luar yang berinteraksi dengan proses tunggal tadi diidentifikasi. *Data Flow Diagram* (DFD) adalah penyajian grafis dari sebuah sistem yang mempergunakan empat bentuk simbol untuk mengilustrasikan bagaimana data mengalir melalui proses-proses yang saling tersambung. Pengembangan DFD biasanya menggunakanan cara berjenjang. Dimulai dari *Context Diagram*, DFD *level 1, level 2* dan seterusnya sesuai dengan kompleksitas dari sistem yang dikembangkan. *Balancing* dalam DFD digunakan dalam menyimpan aliran input dan output dari *level* yang berbeda.

3. Metodologi

Penelitian ini menggunakan jenis pendekatan kualitatif deskriptif dan mengumpulkan data menggunakan teknik tringulasi. Dimana menurut Sugiyono (2014) tringulasi diartikan sebagai teknik pengumpulan data dengan dengan menggunakan teknik wawancara, observasi dan dokumentasi untuk sumber data yang sama secara serempak. Serta dilakukan analisis sistem informasi akademik yang

sedang berjalan yang dijelaskan dalam bentuk *flow map*, analisis dilakukan ketika sedang melakukan wawancara dan observasi. Dengan mengacu pada ISO/IEC 27001 untuk menentukan ruang lingkup penelitian dengan memilih klausul yang sesuai berdasarkan fakta yang telah dijelaskan dalam latar belakang penelitian, maka dengan klausul yang dipilih akan dilakukan pengukuran tingkat kematangan pada setiap aset pada objek penelitian, dan pengukuran tingkat kematangan mengacu pada kriteria penilaian dari SSE-CMM.

Hasil penelitian dapat berupa 2 *output*, yaitu rekomendasi model CD/DFD dari sistem informasi akademik dan tingkat kematangan dari setiap kontrol yang diteliti. Analisis data dilakukan dengan *gap analysis* untuk membandingkan sejauh mana klusul-klausul ISO/IEC 27001 yang sudah dilakukan, baik dalam aspek dokumentasi kebijakan/prosedur, implementasi, maupun evaluasi. Sebelum data dilakukan analisis dengan *gap analisis*, terlebih dahulu data dari hasil wawancara, observasi dan dokumentasi dikumpulkan, hasil wawancara dikembangkan menjadi verbaltim, kemudian dikelompokkan sesuai dengan kategori pertanyaan masing-masing variabel penelitian, dan juga hasil observasi digunakan untuk pembuatan catatan lapangan serta dokumentasi digunakan sebagai bukti implementasi oleh organisasi. Hasil akhir data berupa tabel penilaian pengukuran tingkat kematangan. Dan kondisi akhir yang ditemukan dari penelitian akan dianalisa dampak dan memberikan rekomendasi agar sistem manajemen keamanan informasi dapat ditingkatkan sesuai dengan target yang ingin dicapai.

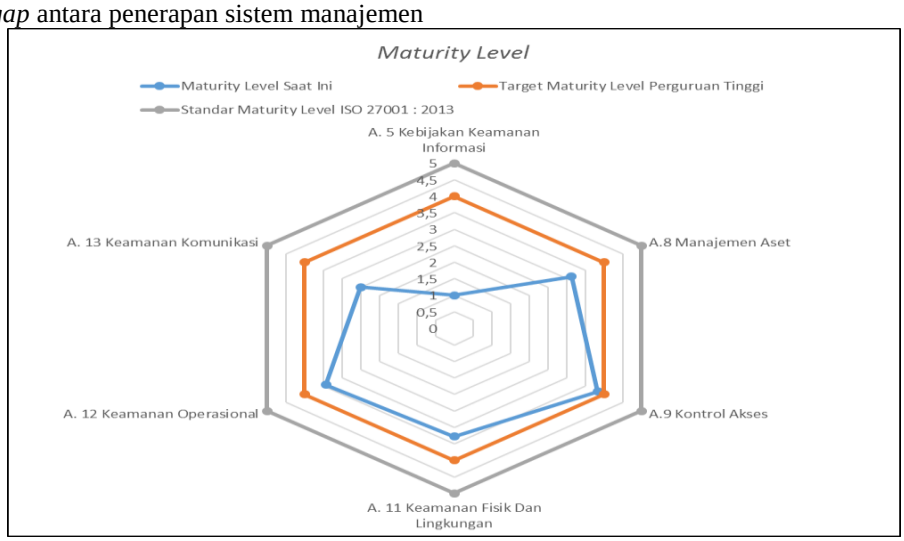
4. Hasil dan Pembahasan

Analisis *maturity level* diawali dengan analisis *gap* dimana analisis ini akan menunjukkan bukti hasil observasi dan studi dokumen dilapangan yang mendukung pernyataan informan. Temuan lapangan menjelaskan *gap* antara penerapan sistem manajemen keamanan informasi dengan standar ISO/IEC 27001: 2013. Dalam penelitian ini didapatkan nilai temuan sebesar 0,6% pada klausul A. 5 Kebijakan Keamanan Informasi, 3,97% pada klausul A. 8 Manajemen Aset, 5,4% pada klausul A. 9 kontrol akses, 6,53% pada klausul A. 11 keamanan fisik dan lingkungan, 6,97% pada klausul A. 12 keamanan operasional dan 3,7% pada klausul A. 13 keamanan komunikasi. Berdasarkan pertanyaan yang ada pada kontrol Annex ISO/IEC 27001 sesuai dengan klausul yang diteliti maka didapatkan hasil *maturity level* untuk setiap kontrol objektif sesuai klausul. Nilai yang didapatkan dari setiap kontrol akan dirangkum dalam Tabel 1 Ringkasan *Maturity Level*.

Tabel 1. Ringkasan *maturity level* tiap klausul

Klausul	*Level*	
A. 5 Kebijakan Keamanan Informasi	1	*Performed-Informally*
A. 8 Manajemen Aset	3	*Well-Defined*
A. 9 Kontrol Akses	3	*Well-Defined*
A. 11 Keamanan Fisik dan Lingkungan	3	*Well-Defined*
A. 12 Keamanan Operasional	3	*Well-Defined*
A. 13 Keamanan Komunikasi	2	*Planned and Tracked*
Rata-rata	2	*Planned and Tracked*

Dari hasil penilaian akhir *Maturity Level* menunjukkan pencapaian praktik sistem manajemen keamanan informasi yang telah dimiliki berdasarkan pada standar ISO/IEC 27001 : 2013. Hasil dari tingkatan *Maturity Level* tersebut akan digambarkan dan dianalisis dengan grafik pada Gambar 1 yang akan dibandingkan dengan standar tingkat *Maturity Level* yang baik dari ISO/IEC 27001 : 2013 (nilai 5) dan juga tingkat *Maturity Level* yang diharapkan dan ditargetkan oleh Direktorat Sistem Informasi Perguruan tinggi (nilai 4).



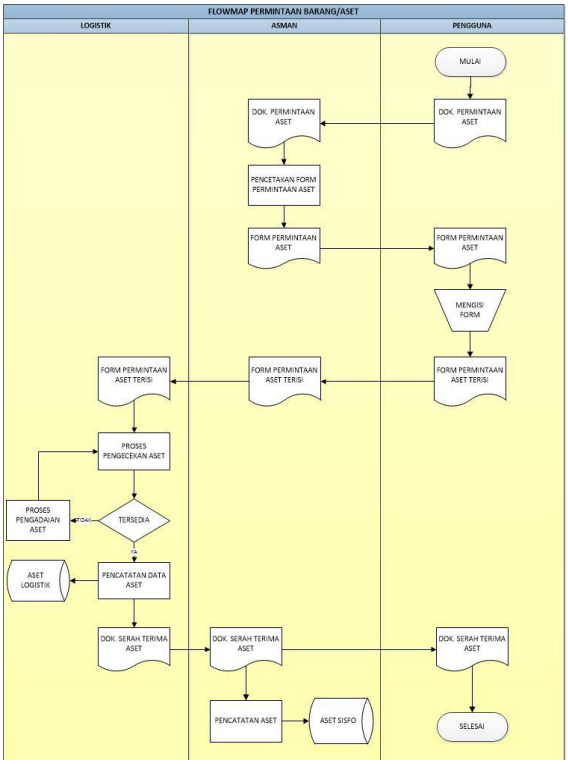
Gambar 1. Grafik analisi *maturity level*

Dari grafik tersebut menunjukkan bahwa hasil dari tingkatan *maturity level* yang didapatkan sebagai berikut :

1. Keamanan sistem informasi terkait kebijakan keamanan informasi berada pada *level* 1 (*Performed-Informally*). Hal ini menunjukkan bahwa kebijakan keamanan informasi hanya dilakukan secara informal, tanpa pendokumentasian dokumen kebijakan secara formal. Dan hasil tersebut masih jauh dari harapan Direktorat Sistem Informasi dan standar ISO/IEC 27001 : 2013. Namun, Direktorat Sistem Informasi sudah sadar akan pentingnya penetapan kebijakan keamanan informasi secara formal.
2. Keamanan sistem informasi terkait manajemen aset berada pada *level* 3 (*Well-Defined*). Hal ini menunjukkan bahwa sebagian besar dari setiap kontrol telah ada dan terdokumentasi, namun masih ditemukan seperti kontrol pengembalian aset, dan kontrol penanganan fisik media *transfer* belum dilakukan pendokumentasian kebijakan secara formal.
3. Keamanan sistem informasi terkait kontrol akses berada pada *level* 3 (*Well-Defined*). Kebijakan untuk kontrol akses telah terdokumentasikan dengan baik, namun beberapa kontrol belum memenuhi harapan organisasi seperti kontrol registrasi pengguna, manajemen otentikasi pengguna, penghapusan hak akses, manajemen *password* belum dilakukan secara maksimal dan masih ditemukan beberapa temuan. Namun, organisasi telah memiliki solusi yang cukup baik untuk mengatasi hal tersebut hanya belum diterapkan secara berkelanjutan.
4. Keamanan sistem informasi terkait keamanan fisik dan lingkungan berada pada *level* 3 (*Well-Defined*). Kontrol pada klausul ini masih ditemukan yang belum terdokumentasi dengan baik seperti perimeter keamanan fisik, keamanan untuk daerah pemuatan dan pegiriman barang, perlindungan dan penempatan barang, dan keamanan barang dilingkungan kerja.
5. Keamanan sistem informasi terkait keamanan operasional berada pada *level* 3 (*Well-Defined*). Hal ini menunjukkan bahwa masih ditemukan beberapa kontrol belum dilakukan pendokumentasian seperti kontrol manajemen kapasitas, pemisahan lingkungan operasional, testing dan pengembangan, dan pembatasan instalasi *software*. Oleh karena itu, keamanan operasional belum memenuhi harapan organisasi.
6. Keamanan sistem informasi terkait keamanan komunikasi berada pada *level* 2 (*Planned and Tracked).* Hal ini menunjukkan bahwa kebijakan keamanan komunikasi hanya dilakukan secara nonformal dan belum dilakukan pendokumentasian secara formal, belum dilakukan evaluasi dan perbaikan secara berkala pada dokumen kebijakan. Terutama pada kebijakan dan prosedur *transfer* informasi dan dokumen kerahasiaan.

Dari hasil analisis *maturity level* dan observasi yang telah dilakukan, maka didefinisikan spesifikasi rancangan sistem yang akan dibuat. Merujuk pada Gambar 1 mengenai grafik analisis *maturity level*, terdapat hasil bahwa klausul kebijakan keamanan informasi, kontrol akses, keamanan fisik dan lingkungan, keamanan operasional dan keamanan komunikasi sudah pernah diterapkan namun belum secara berkelanjutan, sedangkan untuk klausul manajemen aset belum dilakukan secara menyeluruh dan masih dilaksanakan secara konvensional. Hal ini terlihat pada *maturity level* sebesar 3,14 sedangkan target nilai *maturity level* sebesar 4. Oleh karena itu, untuk pemodelan sistemnya terfokus pada sistem manajemen aset.

Pemodelan analisis sistem dilakukan berdasarkan alur dokumen yang telah dilakukan selama ini yang dijelaskan dalam bentuk *Flow Map*, sedangkan untuk pemodelan perancangan sistem akan dijelaskan dalam bentuk *Data Flow Digram* (DFD). Analisis proses dan dokumen (*Flow Map*) digunakan untuk menggambarkan aliran dokumen pada sistem yang berjalan disuatu organisasi. Sistem yang berjalan ditunjukkan pada Gambar 2 dan Gambar 3. Gambar 2 menggambarkan aliran dokumen permintaan aset yang terdiri dari 3 pelaku, yaitu Logistik, Asman (Asisten Manajer) dan pengguna aset.

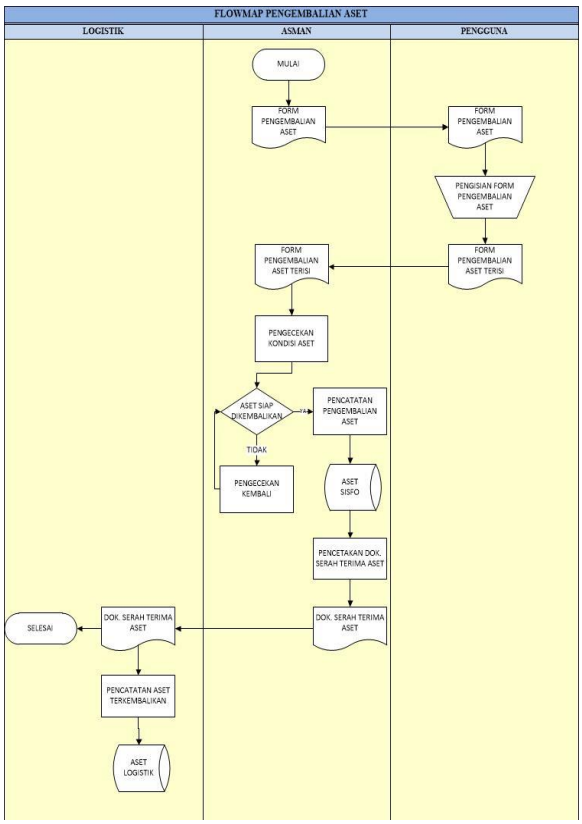


Gambar 2. *Flow map* permintaan aset

Proses permintaan barang/aset tersebut dapat dijabarkan sebagai berikut :

1. Pertama, calon pengguna mengajukan permohonan permintaan barang kepada asman, kemudian akan dicetak *form* permintaan aset yang diisi secara manual oleh calon pengguna sendiri dan diserahkan kembali kepada asman. Asman menyerahkan form permintaan aset yang telah terisi kepada pihak logistik.
2. Pihak logistik setelah menerima *form* permintaan aset akan melakukan pengecekan stok barang, jika stok barang tidak tersedia makan akan dilakukan proses pengadaan barang, namun jika stok tersedia maka akan langsung diproses pencatatan di data aset logistik untuk penyerahan kepada asman.
3. Asman, yang telah menerima aset akan mencatat data aset tersebut di data aset sisfo, kemudian menyerahkan kepada calon pengguna dengan pengisian dokumen serah terima aset.

Gambar 3 menggambarkan aliran dokumen pengembalian aset yang terdiri dari 3 pelaku, yaitu Logistik, Asman (Asistem Manajer) dan Pengguna Aset.



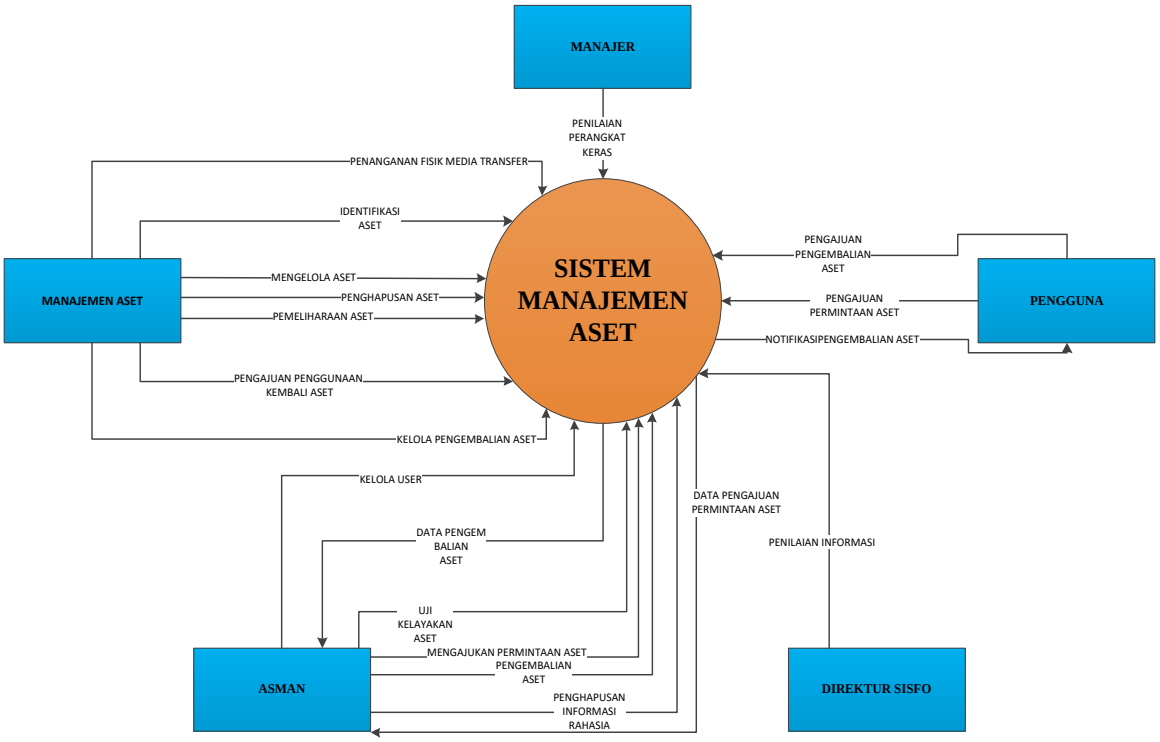
Gambar 3. *Flow Map* Pengembalian Aset

Proses pengembalian barang/aset tersebut dapat dijabarkan sebagai berikut :

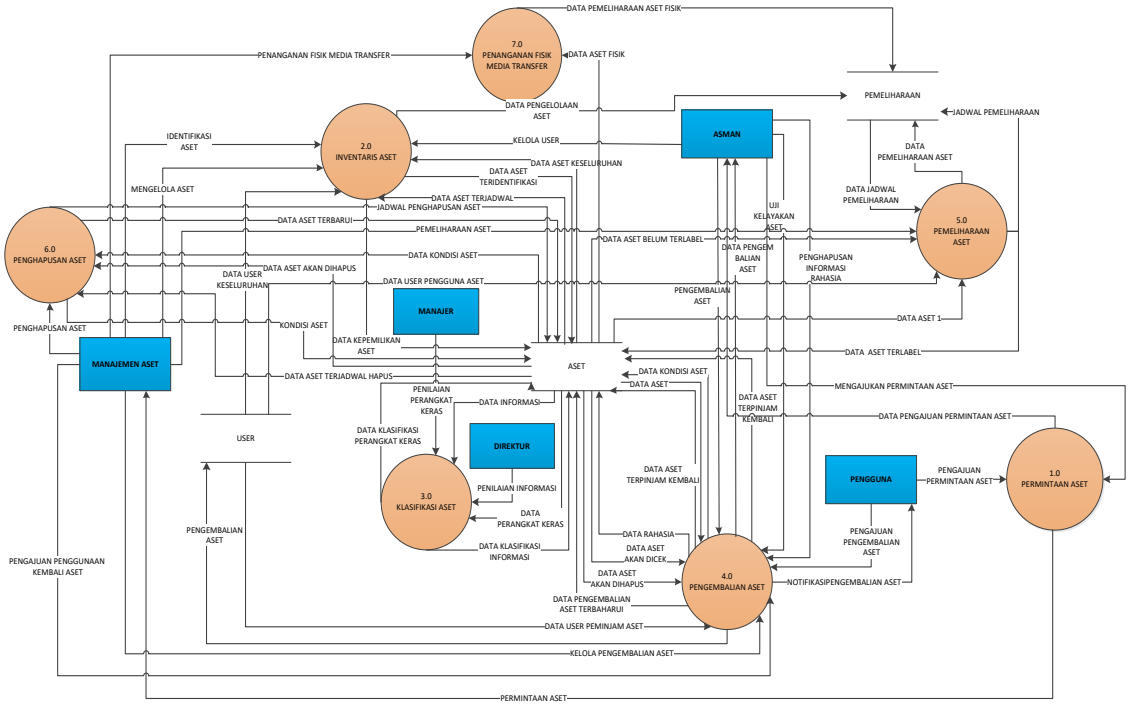
1. Pengembalian aset diawali dengan pengisian form pengembalian aset oleh pengguna yang didapatkan dari asman. Pengisian secara manual dan kemudian diserahkan kembali kepada asman form pengembalian yang telah terisi.
2. Asman menerima form pengembalian yang telah terisi akan melakukan pengecekan kondisi aset, apakah aset dalam kondisi siap untuk dikembalikan atau tidak. Jika aset ditemukan dalam kondisi masih menyimpan informasi rahasia maka akan dilakukan pengecekan kembali. Dimana pada tahap ini informasi rahasia akan dibackup dan dihapuskan secara permanen dari aset yang akan dikembalikan. Aset yang siap untuk dikembalikan akan dicatat dalam data aset sisfo sebelum dikembalikan akan dilakukan pencetakan dokumen serah terima aset.
3. Dokumen serah terima aset diserahkan bersama dengan aset yang akan dikembalikan oleh asman kepada pihak logistik. Pihak logistik akan melakukan mencatatan pada data aset logistik sebelum menggudangkan aset tersebut.

Pemodelan sistem dilakukan pada sistem manajemen aset yang selama ini dilakukan secara konvensional. Rekomendasi sistem di rancang dalam bentuk CD/DFD. Berikut merupakan gambaran CD/DFD model sistem manajemen aset.

Pada Gambar 4 menggambarkan sistem secara garis besar menggambarkan hubungan masukan dan keluaran antara sistem dengan entitas diluar sistem meliputi Manajemen Aset, Manajer, Asisten Manajer, Pengguna dan Direktur Sisfo pada Sistem Manajemen Aset. Dari *Context Diagram* dapat dijelaskan bagaimana tujuan tujuan data, pemrosesan data tersebut yang akan menghasilkan bentuk entitas yang dapat dipakai sebagai dasar pembentukan data base pada *Data Flow Diagram level* 1.



Gambar 4. *Context Diagram*



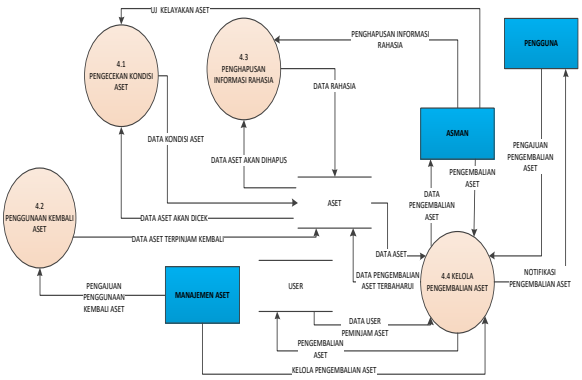
Gambar 5. DFD *Level* 1

Gambar 5 menggambarkan aliran data yang terjadi dalam sistem yang terdiri dari 6 proses, sebagai berikut :

1. Inventaris Aset, dilakukan oleh manajemen aset, diawali dengan melakukan identifikasi aset dari data aset yang didapatkan dari *data store*, data identifikasi aset akan disimpan kembali di *data store* aset.
2. Klasifikasi Aset, dilakukan oleh manajer dan direktur, dimana manajer melakukan penilaian terhadap nilai aset fisik dan direktur melakukan penilaian terhadap informasi. Data klasifikasi aset disimpan dalam *data store* aset.

3. Pengembalian Aset, kelola pengembalian aset dilakukan oleh manajemen aset dan pengembalian aset sendiri dilakukan oleh asman masing-masing divisi. Data *user* dan data aset didapatkan dari *data store* dan data pengembalian aset sendiri akan disimpan di *data store* aset. Pengguna akan mendapatkan notifikasi untuk pengembalian aset dan melakukan pengajuan pengembalian aset melalui sistem.
4. Pemeliharaan Aset, manajemen aset bertanggung jawab atas pemeliharaan aset. Dan data pemeliharaan aset akan disimpan di *data store* pemeliharaan.
5. Penghapusan Aset, dilakukan oleh manajemen aset dan data penghapusan aset akan disimpan di *data store* aset. Penghapusan aset akan menilai kelayakan aset untuk dihapus dan akan dapat diajukan untuk penggunaan kembali.
6. Penanganan fisik media *transfer*, dilakukan oleh manajemen aset, dengan data aset dari *data store* maka akan dilakukan penanganan fisik media *transfer* dan akan diperbaharui data pemeliharaan di *data store* pemeliharaan.

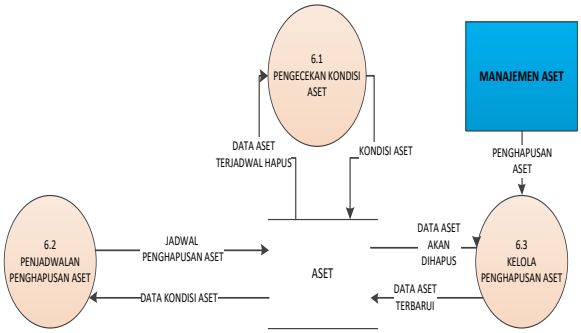
Pengembangan DFD biasanya menggunakanan cara berjenjang. Dimulai dari *Context Diagram*, DFD *level 1*, *level 2* dan seterusnya sesuai dengan kompleksitas dari sistem yang dikembangkan. Dalam pengembangan sistem manajemen aset ini, dikembangkan sampai pada *level* 2. Beberapa aktivitas yang dikembangkan sampai dengan *level* 2 yaitu, pengembalian aset dan penghapusan aset yang terkait langsung dengan keamanan informasi. Salah stu bentuk pengembangan sistem DFD *level* 2 ditunjukkan pada Gambar 6 dan Gambar 7.



Gambar 6. DFD *Level* 2 pengembalian aset

Pengembalian Aset dilakukan dengan beberapa tahap sebagai berikut

1. Pertama, pengecekan kondisi aset yang dilakukan oleh asistem manajer. Data kondisi aset masuk ke proses penggunaan kembali aset.
2. Kedua, penggunaan kembali dilakukan asisten manajer. Data aset yang dapat dan tidak dapat digunakan kembali masuk ke dalam proses pengembalian aset.
3. Ketiga, proses penghapusan informasi rahasia dilakukan oleh asistem manajer. Data rahasia disimpan dalam *data store* aset.



Gambar 7. DFD *level* 2 penghapusan aset

Penghapusan Aset Gambar 7. penghapusan aset dilakukan dengan beberapa tahap, yaitu :

1. Pertama, proses pengecekan kondisi aset dilakukan oleh manajemen aset. Proses ini menghasilkan data kondisi aset terbaru yang disimpan dalam *data store aset*.
2. Kedua, penjadwalan penghapusan aset dilakukan untuk menghasilkan jadwal penghapusan setiap aset yang dimiliki.
3. Ketiga, pencatatan terhapus dilakukan manajemen aset yang mencatat setiap aset yang telah terhapus dan menyimpan data aset yang terbaru di *data store* aset.

5. Kesimpulan

Berdasarkan penelitian yang telah dilakukan *Maturity level* pada yang didapatkan yaitu, *Maturity level* pada klausul kebijakan keamanan informasi telah mencapai *level* 1 (*Performed-Informally*), keamanan informasi hanya dilakukan secara nonformal. Perguruan tinggi belum memiliki dokumen resmi mengenai kebijakan keamanan informasi, yang berarti belum sesuai dengan target Perguruan tinggi. *Maturity level* pada klausul manajemen Aset telah mencapai *level* 3 (*Well-Defined*), Perguruan tinggi telah melakukan pendokumentasian terhadap beberapa dokumen kebijakan mengenai manajemen aset, namun belum melakukan implementasi secara menyeluruh, evaluasi dan perbaikan secara berkala belum sesuai dengan target Perguruan tinggi. Penanganan media khususnya fisik media *transfer* belum dilakukan oleh Perguruan Tinggi. *Maturity level* pada klausul kontrol akses telah mencapai *level* 3 (*Well-Defined*), dokumentasi pada kebijakan telah dilakukan, hanya ditemukan beberapa dokumen kebijkan belum dilakukan evaluasi dan perbaikan secara berkala. *Maturity level* pada klausul keamanan fisik dan lingkungan telah mencapai *level* 3 (*Well-Defined*), temuan pada klausul ini yaitu mencapai 6,53 %. *Maturity level* pada klausul keamanan operasional

telah mencapai *level* 3 (*Well-Defined*), paling banyak temuan pada kalusul ini yaitu mencapai 6,97%. Ditemukan kontrol tidak dilakukan dan belum terdokumentasikan secara formal. *Maturity level* pada klausul keamanan komunikasi telah mencapai *level* 2 (*Planned and Tracked*), beberapa kebijakan belum dilakukan namun belum ditemukan temuan yang berarti di kalusul ini atau gangguan yang terjadi masih dapat diatasi oleh Perguruan Tinggi.

Dan berdasarkan hasil penilaian *maturity level* ditemukannya beberapa kekurangan pada manajemen aset dalam mengimplementasikan kebijakan. Oleh karena itu, pemodelan sistem dengan menggunakan *flow map* dan CD/DFD difokuskan untuk Sistem Manajemen Aset. Dalam perancangan alur bisnis proses terlibat beberapa entitas dalam sistem seperti Manajemen Aset, Manajer, Direktur, Pengguna, dan Asman (Asisten Manajer). Pembuatan sistem bagian manajemen aset berhubungan langsung dengan Direktorat Sisfo melalui sistem. Beberapa aktivitas atau proses kerja sistem yang dapat dilakukan yaitu, Inventaris Aset, Klasifikasi Aset, Pengembalian Aset, Pemeliharaan Aset, Penghapusan Aset, dan Penanganan Fisik Media Transfer. Semua aktivitas telah disesuaikan dengan standar ISO/IEC 27001 : 2013. Terdapat beberapa *data store* yang digunakan untuk mengambil dan menyimpan data olahan seperti *data store* Aset, *User* dan Pemeliharaan yang berhubungan langsung dengan aktivitas sistem. Dalam perancangan sistem beberapa aktivitas dipilah sampai pada *level* 2.

Daftar Pustaka

Darmawan, Deni dan Fauzi, Kunkun Nur, 2013. Sistem Informasi Manajemen. Remaja Rosdakarya, Bandung.

DataLossDB, 2015. *Stastistics.* Website : http://datalossdb.org/ statistics. Diakses tanggal 14 Oktober 2015.

Fatta, Hanif Al, 2007. Analisis dan Perancangan Sitem Informasi untuk Keunggulan Bersaing Perusahaan dan Organisasi Modern. Andi, Yogyakarta.

International Standard Organization, 2005. ISO/IEC 27002 Information Technology, Code of prectice for information security management. International Standard Organization, Switzerland.

International Standard Organization. 2013. ISO/IEC 27001 Information Technology, Security Techniques - Information Security Management System-Requierements. International Standard Organization, Switzerland.

Laudon, Kenneth C., and Laudon, Jane P., 2007. Sistem Informasi Manajemen Mengelola Perusahaan Digital. Salemba Empat, Jakarta.

Sugiyono, 2014. Metode Penelitian Kuantitatif Kualitatif dan R&D. Alfabeta, Bandung.

Susanto, H., Almunawar, Mohammad, N., dan Tuan, Yong Chee. 2011. Information Security Management System Standards : A Comparative Study of The Big Five. Retrieved from International Journal of Electrical & Computer Sciences IJECS-IJENS, 11(5), 21-27.

Sutabri, Tata. 2012. Konsep Sistem Informasi. Andi, Yogyakarta.

Verizon. 2014. 2014 Data Breach Invetigations Report. Verizon, United States.