ANALISIS KEAMANAN INFORMASI DATA CENTER MENGGUNAKAN COBIT 5

Iik Muhamad Malik Matin, Arini, Luh Kesuma Wardhani

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi
Universitas Islam Negeri Syarif Hidayatullah Jakarta
iikmuhamadmalikmatin@mhs.uinjkt.ac.id, arini@uinjkt.ac.id; luhkesuma@uinjkt.ac.id

ABSTRAK

Data center pada sebuah institusi telah diamati dan dianalisa untuk mendapatkan deskripsi mengenai keamamanan informasinya. *Data center* pernah mengalami insiden keamanan informasi berupa *Shell Injection*. Akibatnya, beberapa situs web tidak dapat diakses beberapa saat. Insiden ini dapat mempengaruhi proses bisnis institusi. Untuk menghindari masalah ini di masa depan, diperlukan audit keamanan informasi. Audit ini dapat dilakukan dengan menggunakan *framework* COBIT 5. Dalam penelitian ini, audit keamanan informasi dilakukan terhadap keamanan informasi *data center* dengan fokus pada proses APO13 (*Manage Security*) dan DSS05 (*Manage Security Service*). Penelitian ini Penelitian ini dilakukan melalui tahap *Initiation*, *Planning the Assessment*, Briefing, *Data Collection*, *Data Validation*, *Process Attribute Level* dan *Reporting the Result*. Hasil penelitian ini diketahui tingkat kemampuan APO13 dan DSS05 pada saat ini (*As Is*) bernilai 1,54 dan 1,68 atau pada level 2, yang berarti proses APO13 dan DSS05 telah dilakukan dan dipelihara sesuai dengan rencana kerja. Oleh karena itu tingkat berikutnya (*to be*) ditetapkan pada level 3. Untuk mencapai level 3, beberapa rekomendasi diberikan untuk menutupi *gap* yang telah ditentukan dalam proses APO13 dan DSS05. *Data center* harus membuat rencana kerja yang rinci, *data center* yang dikelola dengan baik dan memiliki standar yang jelas untuk diterapkan agar dapat mencapai tujuan bisnis

Kata Kunci: *COBIT 5, Data Center, Keamanan Informasi. DSS05, APO13*

ABSTRACT

A data center of an institution was observed and analyzed in order to get description about its information security. The data center had ever experienced incidents of information security which is Shell Injection. As a result, some websites were not accessible for a moment. This incident can affect business processes of the institution. In order to avoid this problem in the future, this institution needs information security audit. This audit can be conducted by using Framework COBIT 5. In this research, an information security audit was conducted to Data Center Information Security by using Framework COBIT 5, focus on the process DSS05 (Manage Security Service) and APO13 (Manage Security). This research was conducted through some stages of initiation, planning the assessment, briefing, data collection, data validation, process attribute level and reporting the result. The research result shows that the capability level of APO13 and DSS05 at this moment (as is) worth 1.54 and 1.68 or stays at level 2, which means process of APO13 and DSS05 had been done and maintained in accordance with the work plan. Therefore the next level (to be) set at level 3. In order to achieve level 3, some recommendations provided to cover the gap that has been determined in the process APO13 and DSS05. The data center have to make a detail work plan, well managed data center and have clear standard to be implemented in order to reach the business goal.

Keywords: *COBIT 5, Data Center, Information Security. DSS05, APO13*

DOI: 10.15408/jti.v10i2.7026

I. PENDAHULUAN

Kemajuan Teknologi Informasi (TI) yang sangat pesat menjadikan TI sebagai aspek terpenting dalam pemenuhan kebutuhan perusahaan. Adanya Teknologi Informasi (TI) dipandang dapat memberikan solusi terkait proses-proses bisnis perusahaannya. Sehingga banyak perusahaan yang memberikan banyak sumber dayanya untuk meningkatkan efisiensi, efektivitas, dan kinerjannya dengan mengandalkan Teknologi Informasi (TI).

Pentingnya Teknologi Informasi (TI) dalam melakukan proses-proses bisnis tidak dapat terlepas dari aspek keamanan informasi. Kemananan informasi mutlak diperhatikan untuk menghindari terjadinya kebocoran-kebocoran rahasia pengguna dan informasi-informasi penting perusahaan sesuai dengan aspek-aspek tujuan keamanan informasi yang mencangkup *Confidentiality*, *Integrity dan Availability*. Untuk memastikan bahwa proses-proses bisnis terhindar dari insiden-insiden yang berkaitan dengan keamanan informasi maka setiap perusahaan memerlukan suatu penerapan Tata Kelola TI (*IT Governance*) yang berkaitan dengan keamanan informasi.

Islam memandang keamanan informasi sebagai aset yang sangat penting dan berharga dalam mendapatkan pengetahuan dalam rangka mencapai masyarakat yang makmur dengan didukung menggunaan IT. Nabi Muhammad telah menyampaikan bahwa seorang muslim harus selalu berkata tentang hal-hal baik atau lebih baik diam. Selain itu bahwa muslim yang baik adalah muslim yang baik ucapan maupun tindakannya tidak merugikan orang lain. Islam meandang bahwa informasi dan komunikasi sebagai proses yang terdiri dari 3 fase aktivitas utama, yaitu pengumpulan, proses dan penyebaran. 3 fase inilah yang yang menjadi *frame* Analisa prinsip keamanan informasi dalam islam [1].

IT Governance merupakan bagian dari proses tata kelola perusahaan yang terdiri dari proses manajemen, prosedur dan kebijakaan yang ditetapkan dalam rangka memberikan suatu keputusan dan arahan pada layanan Teknlogi Informasi (TI) dan sumber daya termasuk pada pertimbangan resiko, kepatuhan dan kinerja [2]. Keamanan Informasi adalah melindungi kerahasiaan, integritas dan ketersediaan aset informasi, baik dalam penyimpanan, pengolahan, atau transmisi. itu dicapai melalui penerapan kebijakan, pendidikan, pelatihan kesadaran, dan teknologi [3]). Pada perusahaan yang memiliki skala besar diperlukan menerapkan *IT Governance* yang mencangkup keterlibatan seluruh *stakeholder* sesuai dengan proporsinya..

Berdasarkan wawancara pada Koordinator Bidang Keamanan dan *Data Center*, telah terjadi serangkaian peretasan sebanyak 22 sejak beberapa tahun yang lalu. Insiden paling besar adalah adanya serangan *shell injection,* yaitu penyusupan *malware* kedalam sistem sehingga mengakibatkan beberapa domain tidak dapat. Sealian itu, banyak laporan yang masuk kepada *helpdesk* terkait dengan keamanan. namun, pusat komputer tidak pernah melakukan audit audit pada keamaman *data center*.

Analisa keamanan informasi merupakan hal yang penting untuk menjamin keamanan asset TI di sebuah institusi. sebuah *framework* untuk dapat memetakan insiden apa saja yang kemungkinan terjadi terkait Keamanan Informasi dan bagaimana penanganan-penanganan agar kemungkinan insiden yang terjadi dapat diantisipasi. Untuk itu, Pusat Komputer dapat menggunakan sebuah framework. Pusat Komputer dapat menerapkan framework Control Objective for Information and Related Technology (COBIT) untuk mengaudit keamanan data center.

Control objectivre for Information and Related Technology (COBIT) adalah seperangkat sumber daya yang berisi semua informasi yang dibutuhkan organisasi untuk tata kelola TI dan kerangka kontrol. COBIT memberikan praktek yang baik diseluruh domain dan kerangka proses dalam struktur kelola logis untuk membantu mengoptimalkan kemampuan TI dalam investasi dan memastikan bahwa TI berhasil dalam memberikan kebutuhan bisnis [4].

Dibandingkan dengan versi sebelumnya, COBIT 5 lebih berorientasi pada prinsip sehingga ada prinsip baru dalam tata kelola Teknologi Informasi yaitu *Governance of Enterprise IT* (GEIT), COBIT 5 menyebutkan secara spesifik bagian-bagian *enablers*, memiliki definisi model referensi proses yang baru dengan tambahan domain *governance* dan beberapa proses baru yang merupakan modifikasi dari proses sebelumnya dengan mengintegrasikan konten pada COBIT 4.1, *Risk IT*, dan *Val IT*, dan menyelaraskan dengan *best practice* yang ada seperti ITIL V3 dan TOGAF.

Dalam menentukan proses yang akan dipilih untuk melakukan audit, COBIT memberikan cara dengan pemetaan IT Goal terhadap proses-proses COBIT. Terdapat 17 IT *Goals* yang terbagi menajdi 4 sektor yaitu *Financial*, *Customer*, *Internal*, dan *Learning and Growth*. Berdasarkan hasil analisa permasalahan yang muncul pada penelitian ini, maka sektor IT *Goals* yang paling sesuai adalah sektor *Internal* dengan *IT Goals* ke sepuluh yaitu *Security of Information*, *Processing Infrastructure* and *Application*. Pada IT Goals tersebut terdiri dari EDM03 (Memastikan Optimasi Risiko), APO12 (Mengelola Risiko), APO13 (Mengelola Keamanan), BAI06 (Mengelola Perubahan), dan DSS05 (Mengelola Layanan Keamanan).

Dalam penelitian ini, Analisa keamanan informasi *data center* menggunakan COBIT 5. Namun, setelah melakukan kuesioner pada pihak Pusat Komputer maka ditentukan proses domain yang dipilih yaitu APO13 (Mengelola Keamanan) dan DSS05 (Mengelola Layanan Keamanan).

II. TINJAUAN PUSTAKA

2.1 *IT Governance*

IT Governance merupakan bagian dari proses tata kelola perusahaan yang terdiri dari proses manajemen, prosedur dan kebijakaan yang ditetapkan dalam rangka memberikan suatu keputusan dan arahan pada layanan Teknologi Informasi (TI) dan sumber daya termasuk pada pertimbangan resiko, kepatuhan dan kinerja. [2].

2.2 *Information Security*

Keamanan informasi adalah untuk melindungi kerahasiaan, integritas dan ketersediaan aset informasi, baik dalam penyimpanan, pengolahan, atau transmisi. Hal ini dicapai melalui penerapan kebijakan, pendidikan, pelatihan dan kesadaran, dan teknologi [3].

Dalam keamanan informasi saat ini telah berkembang menjadi tiga konsep utama yang menjadi standar utama dalam industri keamanan yang disebut dengan CIA *triangel* yaitu:

1. *Confidentiality*, Merupakan usaha untuk menjaga informasi dari pihak yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan informasi yang diberikan kepada pihak lain.
2. *Integrity*, Keaslian pesan yang dikrim melalui sebuah jaringan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
3. *Availability*, ketersediaan berhubungan dengan ketersediaan infromasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses informasi.

2.3 *Data Center*

Data center adalah suatu fasilitas khusus yang disusun untuk pengelolaan dan dukungan sumber daya komputer yang dianggap penting untuk satu atau lebih organisasi. dalam *data center* tertentu, mencakup struktur bangunan khusus, struktur *power backup*, *cooling system*, ruangan khusus (seperti pintu masuk dan ruang komunikasi), lemari perangkat, struktur kabel, perangkat jaringan, sistem penyimpanan, *server*, *mainframe*, aplikasi perangkat lunak, sistem keamanan fisik, pusat pemantauan, dan banyak sistem pendukung lainnya. Semua sumber daya ini saling berinterkasi dan dikelola oleh petugas khusus [5].

Layanan yang diberikan *Data Center* [6]:

1. Infrastruktur yang Menjamin Keberlangsungan Bisnis

Service tersebut harus memiliki kriteria pemilihan lokasi *data center*, kuantifikasi ruang *data center*, *laying-out* ruang dan instalasi *data center*, sistem elektrik yang dibutuhkan, pengaturan infrastruktur jaringan yang *scalable*, pengaturan sistem pendingan dan *fire suppression.*

2. Infrastruktur Keamanan *Data Center*

Service keamanan pada *data center* mencangkup fitur keamanan akses user (dapat berupa biometrik atau kartu akses), petugas keamanan, gembok, *access control list*, *firewall*, IDS dan *host* IDS, fitur keamanan pada Layer 2 (*Datalink Layer*) dan *Layer* 3 (*Network Layer*) disertai dengan manajemen keamanan.

3. Optimasi Aplikasi

Optimasi Aplikasi berkaitan dengan protokol internet pada *transport layer session layer* untuk meningkatkan waktu respon suatu server. *Transport layer* adalah layer *end-to-end*

yang paling bawah antara aplikasi sumber dan tujuan, menyediakan *end-to-end flow control*, *end-to-end error detection and correction*, dan *congestion control* tambahan. Sedangkan *session layer* menyediakan riteri dialog, *token management* dan sinkronisasi data. Berbagai isu yang terkait dengan hal ini adalah *load balancing*, *caching*, dan terminasi SSL, yang bertujuan untuk mengoptimalkan jalannya suatu aplikasi dalam suatu sistem.

4. Infrastruktur IP (*internet protocol*).

Infrastruktur IP menjadi layanan utama pada *data center*. Servis ini disediakan pada layer 2 dan layer 3. Layer 2 hubungan antara *farms server* dan perangkat layanan, memungkinkan akses media, mendukung sentralisasi yang *reliable*, *loop-free*, *predictabel*, dan *scalable*. Sedangkan pada layer 3 memungkinkan *fast-convergence routed network*. Layanan tambahan *Intelligent Network Services* meliputi fitur-fitur yang memungkinkan *application services network-wide*, fitur yang paling umum adalah mengenai *QoS (Quality of Services), multicast*, *private LANS* dan *policy-based routing*.

5. *Storage*

Berkaitan dengan infrastruktur penyimpanan adalah arsitektur SAN, *fibre channel switching*, replikasi, *backup* serta *archival*.

Kriteria perancangan *data center* setidaknya harus mencangkup sebagai berikut [6]:

1. Availability

Data center diciptakan untuk mampu memberikan operasi yang berkelanjutan dan terus-menerus bagi suatu perusahaan baik dalam keadaan normal maupun dalam keadaan terjadinya suatu kerusakan yang berarti atau tidak. *Data center* harus dibuat sebisa mungkin mendekati *zero-failure* untuk seluruh komponennya.

2. *Scalability* dan *Flexibility*

Data center harus mampu beradaptasi dengan pertumbuhan kebutuhan yang cepat atau ketika adanya servis baru yang harus disediakan oleh *data center* tanpa melakukan perubahan yang cukup berarti bagi *data center* secara keseluruhan.

3. Keamanan

Keamanan pada *Data center* harus dibangun seketat mungkin baik pengamanan secara fisik maupun non-fisik agar mampu menyimpan berbagai aset perusahaan yang berharga dengan aman.

Aspek Perancangan *Data Center* yaitu [6]:

1. Lokasi

Berada di luar radius mitigasi bencana/gunung berapi (>15km), Tidak berada dalam jalur patahan geologi.

2. Sarana Fasilitas

Generator listrik cadangan, catuan PKL dengan minimum 2 sumber daya pembangkit yang berbeda untuk tier tinggi, UPS, dengan baterai berkapasitas memadai yang mampu menyediakan pasokan daya sebelum genset dihidupkan, pengatur udara (HVAC: *Heating*, *Ventilation*, *and Air Conditioning*) yang mampu menjaga suhu dan kelembaban, sistem pentanahan, tahanan pentanahan terintegrasi <0,5ohm.

3. Komunikasi

Memiliki koneksi komunikasi data network lebih dari 1 sumber dengan lebih dari 1 operator untuk tier tinggi, Jika diperlukan, penyiapan koneksi komunikasi data dapat menggunakan akses satelit, penyiapan jalur komunikasi untuk kordinasi dan komando, misal menggunakan Radio HF/SSB. Pengamanan jalur komunikasi untuk menjaga confidentiality suatu data atau informasi.

2.4 COBIT 5

COBIT 5 merupakan panduan generasi terbaru ISACA yang membahas tata kelola manajemen TI. COBIT 1 dibuat berdasarkan pengalaman penggunaan COBIT selama lebih dari 15 tahun oleg banyak perusahaan dan pengguna di lingkungan bisnis, komunitas TI, risiko asuransi maupun keamanan [7].

Gambar 1 merupakan skema lima prinsip COBIT [7] :

1. *Meeting stakeholder needs*, hal ini sangat penting untuk mendefinisikan dan menghubungkan tujuan perusahaan dan *IT-related goals* terbaik untuk mendukung kebutuhan *stakeholder*.

2. *Covering the enterprise end-to-end*, Perusahaan harus beralih dari *managing IT as a cost* menjadi *managing IT as a asset*, dan manajer bisnis harus bertanggung jawab atas pengelolaan dan pengelolaan aset terkait TI dalam fungsinya sendiri.

3. *Applying a single integrated framework*, Dengan menggunakan kerangka tata kelola terpadu yang tunggal, organisasi dapat memberikan nilai optimum dari aset dan sumber daya TI mereka.

4. *Enabling a holistic approach*, *Governance of Enterprise IT* (GEIT) membutuhkan pendekatan holistik yang memperhitungkan banyak komponen, juga dikenal sebagai enabler. Enabler mempengaruhi apakah sesuatu akan berhasil. COBIT 5 memiliki tujuh enabler untuk meningkatkan GEIT, termasuk prinsip, kebijakan dan kerangka kerja; proses; budaya; informasi dan orang.

5. *Separating governance from management*, Proses tata kelola memastikan bahwa tujuan dicapai dengan mengevaluasi kebutuhan pemangku kepentingan, menetapkan arah melalui prioritas dan pengambilan keputusan; dan memantau kinerja, kepatuhan dan kemajuan. Berdasarkan hasil dari kegiatan tata kelola, manajemen bisnis dan TI kemudian merencanakan, membangun, menjalankan dan memantau kegiatan untuk memastikan keselarasan dengan arah yang ditetapkan.

Model referensi Proses Model referensi proses COBIT 5 adalah penerus dari model proses COBIT 4.1 dengan model risiko TI dan Val IT yang juga terintegrasi. Model proses pada COBIT 5 terdiri dari 32 proses manajemen dan 5 proses tata kelola yang terhimpun dalam 5 domain [8] yaitu:

1. *Evaluate, Direct and Monitor* (EDM)
   Tata kelola memastikan bahwa tujuan perusahaan dicapai dengan mengevaluasi kebutuhan, kondisi dan pilihan pemangku kepentingan; menetapkan arah melalui prioritas dan pengambilan keputusan; dan memantau kinerja, kepatuhan dan kemajuan terhadap arah dan tujuan yang disepakati.

2. *Align, Plan and Organize* (APO)
   Domain mencakup penggunaan informasi & teknologi dan bagaimana cara terbaik untuk digunakan dalam perusahaan guna mencapai tujuan dan sasaran perusahaan. Ini juga menyoroti bentuk organisasi dan infrastruktur yang harus diambil untuk mencapai hasil optimal dan untuk menghasilkan manfaat paling banyak dari penggunaan TI. Tabel berikut mencantumkan proses TI tingkat tinggi.

3. *Build, Acquire and Implement* (BAI)
   Domain Build, Acquire and Implement (BAI) mencakup identifikasi persyaratan TI, memperoleh teknologinya, dan menerapkannya dalam proses bisnis perusahaan saat ini.

4. *Deliver, Service and Support* (DSS)
   Berfokus pada aspek pengiriman teknologi informasi. Ini mencakup bidang-bidang seperti pelaksanaan aplikasi dalam sistem TI dan hasilnya, dan juga, proses dukungan yang memungkinkan pelaksanaan sistem TI ini efektif dan efisien.

5. *Monitor, Evaluate and Assess* (MEA)
   Domain *Monitor, Evaluate and Assess* (MEA) berkaitan dengan strategi perusahaan dalam menilai kebutuhan perusahaan dan apakah sistem TI saat ini masih sesuai dengan tujuan yang dirancang dan pengendalian yang diperlukan untuk mematuhi persyaratan peraturan. Pemantauan juga mencakup masalah penilaian independen terhadap efektivitas sistem TI dalam kemampuannya untuk memenuhi tujuan bisnis dan proses pengendalian perusahaan oleh auditor internal dan eksternal.

Dalam implementasinya, COBIT 5 terbagi menjadi 7 tahapan [9] yaitu:

1. Tahap 1, dimulai dari inisiatif melakukan perubahan pada level manajemen eksekutid diwujudkan dengan kasus bisnis.

2. Tahap 2, fokus pada pendefinisian ruang lingkup implementasi atau perbaikan menggunakan pemetaan *framework* COBIT 5.

3. Tahap 3, menetapkan target peningkatan. Diikuti oleh Analisa yang lebih dalam

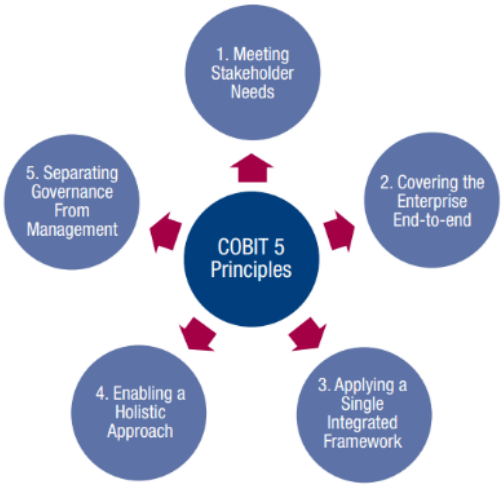
untuk mengidentifikasi sokusi yang paling potensial.

4. Tahap 4, merencanakan solusi praktis dengan mengidentifikasi proyek yang didukung oleh kasus bisnis yang dapat dibenarkan

5. Tahap 5, mengubah solusi dilakukan hari-perhari. Penetapan perhitungan dilakukan untuk memastikan kesesuaian dengan ketercapaian bisnis dan pengukuran kinerja

6. Tahap 6, fokus pada operasi keberlanjutan dari pengelolaan manajemen dan monitoring.

7. Tahap 7, mengevaluasi kesuksesan, mengidentifikasi kebutuhan terhadap tata kelola atau manajemen dan kebutuhan untuk peningkatan secara terus menerus.



Gambar 1. Prinsip COBIT 5 [7]

2.5 *Process Assessment Model* (PAM)

Model ini merupakan dasar untuk penilaian kemampuan proses TI suatu perusahaan pada COBIT 5 dan program pelatihan dan sertifikasi bagi para penilai. Proses penilaian ini dibuktikan dengan mengaktifkan proses penilaian yang dapat diandalkan, konsisten, dan berulang di bidang tata kelola dan manajemen TI.

2.6 Proses APO13 (*Manage Security*)

Mendefinisikan, mengoperasikan dan mengawasi sistem untuk manajemen keamanan informasi. Tujuan dari proses tersebut adalah menjaga agar dampak dan kejadian dari insiden masih berada dalam batas *resiko* yang daat diterima perusahaan [11].

Sub proses pada APO13 sebagai berikut:

1. APO13.1, Membangun dan Memelihara SMKI
2. APO13.2, Mendefinisikan dan Mengelola rencana Penanganan Keamanan Informasi.
3. APO13.3, Mengawasi dan Mengkaji Sistem Manajemen Keamanan Informasi

2.7 Proses DSS05 (*Manage Security Service*)

DSS05 mengenai melindungi informasi perusahaan untuk mempertahankan tingkatan dari keamanan Informasi yang dapat diterima oleh perusahaan sesuai dengan kebijaksanaan keamanan. Menetapkan dan mempertahankan peran keamanan informasi dan hak akses dan melakukan pengawasan keamanan. [11].

Sub proses pada APO13 sebagai berikut:

1. DSS05.1, melindungi Sistem dari *Malware*
2. DSS05.2, mengelola Jaringan dan Keamanan Konektivitas
3. DSS05.3, mengelola Keamanan *Endpoint*
4. DSS05.4, mengelola Identitas *User* dan Akses Lojik
5. DSS05.5, mengelola Akses Fisik Terhadap aset TI
6. DSS05.6, mengelola Dokumen Sensitif dan Perangkat Output
7. DSS05.7, mengawasi Infrastruktur untuk Kejadian Terkait Keamanan

Gambar. 2. Siklus implementasi COBIT 5

III. METODOLOGI

Data untuk penelitian ini diperoleh dari wawancara dengan Koordinator dan Keamanan *Data Center*. Dari koordinator keamanan didapatkan informasi tentang insiden yang terjadi di *data center*, tindakan apa yang telah dilakukan, penanganan informasi keamanan, kebijakan pusat komputer dan informasi lainnya yang mendukung penelitian. Selain itu, pengamatan ke *data center* telah dilakukan ke *data center* yang dipilih. Untuk mendapatkan data pendukung tentang kejadian keamanan informasi di *data center*, kami juga membagikan kuesioner kepada beberapa responden dan memetakan hasilnya ke dalam tabel RACI. Setelah data diperoleh, beberapa tahap Analisa data berdasarkan COBIT 5 *Assessment Process Activities* (APA) dilakukan.

Tahapan Analisa data berdasarkan COBIT 5 *Assessment Process Activities* (APA) yang terdiri dari [12]:

1. *Initiation,* tahapan ini bertujuan untuk menjelaskan hasil identifikasi
2. *Planning The Assessment,* tahapan melakukan penilaian yang bertujuan mendapatkan hasil evaluasi berupa kuesioner yang berkaitan dengan ruang lingkup analisa
3. *Briefing,* tahapan ini dilakukan pemberian arahan terhadap responden.
4. *Data Collection,* tahapan ini dilakukan pengumpulan bukti-bukti yang terdapat pada Pusat Komputer sebagai bahan penilaian
5. *Data Validation,* pada tahap ini dilakukan untuk mengetahui kuesioner yang menjadi bahan dalam menentukan *capability level* dan *gap*
6. *Process Atribute Level,* tahap ini dilakukan untuk mengetahui seberapa jauh tingkat kapabilitas dan kelemahan yang perlu ditingkatkan
7. *Reporting The Result,* hasil penentuan *capability level* dan *gap* dilaporkan untuk memberikan rekomendasi kepada perusahaan

IV. ANALISA

4.1 *Initiation*

Dari hasil observasi diketahui *data center* saat ini Pusat Komputer telah menerapkan keamanan yang terdiri dari:

1. Perangkat keras

Data center telah menerapkan sistem keamanan termasuk sidik jari di pintu masuk kantor yang hanya bisa diakses oleh karyawan pusat komputer, *doorlock* otomatis sehingga tidak memungkinkan orang lain masuk ke data center tanpa izin, selain sidik jari juga diaplikasikan ke Pintu masuk ruang data center yang hanya bisa diakses oleh koordinator keamanan dan *data center* dan satu orang staf, dipasang CCTV untuk memantau *data center* 24 jam.

2. Perangkat Lunak

Sistem komputer telah menerapkan perangkat lunak antivirus di linux untuk mengantisipasi akses *malware* yang masuk ke sistem di *data center*, dan *firewall* untuk menyaring akses jaringan, untuk mempertimbangkan keselamatan serta mendeteksi aktivitas mencurigakan dalam suatu sistem.

Penentuan ruang lingkup diperoleh dari hasil pemetaan kebutuhan *enterprise* dengan COBIT, maka diketahui proses yang sesuai dengan dengan kebutuhan adalah APO13 dan DSS05.

4.2 *Planning The Assessment*

Purposive sampling digunakan untuk menentukan responden dengan pertimbangan khusus sehingga dianggap layak menjadi responden. Sampel yang diambil adalah sampel yang memiliki peran dan tanggung jawab yang sesuai dengan objek yang diteliti. Responden terpilih kemudian disesuaikan dengan RACI dalam setiap proses.

4.3 *Briefing*

Briefing disajikan dengan bentuk input, proses, keluaran proses DSS05 dan APO13, jadwal pelaksanaan kuesioner yang dimulai pada tanggal 8 September sampai 9 September 2016, pengumpulan kuesioner pada tanggal 26 September 2016, rekapitulasi kuesioner mulai tanggal 27-30 September 2016, dan melaporkan hasilnya pada tanggal 15 Oktober 2016. Jadwal kegiatan penelitian disajikan pada Tabel 1.

4.4 *Data Collection*

Pada tahap keempat peneliti melakukan pengumpulan data yang terdapat di Pusat Komputer yang dapat dijadikan bukti-bukti untuk memenuhi tingkat kapabilitas 1 di tiap-

tiap proses yang telah dilakukan. Dari hasil pengumpulan data yang dilakukan, Pusat Komputer telah memenuhi tingkat kapabilitas 1 baik untuk proses APO13 maupun DSS05.

4.5 *Data Validation*

Pada tahapan kelima ini peneliti melakukan validasi data dari hasil kuesioner yang telah didistribusikan kepada responden sesuai dengan pemetaan RACI *Chart*. Tujuan dari tahap ini adalah untuk mengetahui hasil perhitungan kuesioner dan mendapatkan evaluasi penilaian *capability level*.

Jawaban kuesioner yang diperoleh dari responden diidentifikasi dalam tabel di Bagan RACI APO13 (Tabel 2) dan Bagan RACI APO13 (Tabel 3).

Tabel 1. Jadwal aktivitas penelitian

No	Kegiatan	Jadwal
1	Observasi	8 Juni-30 September 2016
2	Pelaksanaan Kuesioner	8-9 September 2016
3	Pengumpulan Kuesioner	26 September 2016
4	Rekapitulasi Kuesioner	27-30 September 2016
5	Laporan	15 Oktober 2016

V. HASIL DAN PEMBAHASAN

5.1 *Process Atribute Level*

Pada tahapan ini, ditentukan *level*, nilai kapabilitas tingkat kapabilitas dari hasil kuesioner yang telah diperoleh dan menentukan tingkat kapabilitas selanjutnya (*to be*).

Tabel 2. Rekapitulasi APO13

No	Sub Proses	Persentase	Kondisi (*As Is*)
1	APO13.1	58,33%	3
2	APO13.2	50%	3
3	APO13.3	60%	2

Tabel 3. Rekapitulasi jawaban DSS05

No	Sub Proses	Persentase	Kondisi (*As Is*)
1	DSS05.1	58,33%	2
2	DSS05.2	55,55%	3
3	DSS05.3	55,55%	3
4	DSS05.4	42,75%.	3
5	DSS05.5	42,85%.	3
6	DSS05.6	60%	3
7	DSS05.7	60%.	3

Tabel 4. Kapabilitas APO13

No	Sub Proses	Kapabilitas	
		Nilai	Level
1	APO13.01	1,91	2
2	APO13.02	1,71	2
3	APO13.03	1,0	1
Rata-rata		1,54	2

Perdasarkan Tabel 4 dapat diketahui kondisi saat ini (*as is)* pada APO13 bernilai 1.54 atau kapabilitas level berada pada level 2 (*managed*). Artinya *data center* sudah dapat mengelola keamanan, merencanakan rencana kerja, memonitor dan memberikan laporan.

Untuk kapabilitas DSS05, dapat dilihat pada Tabel 5, dengan nilai 1.7 (level 2), yang artinya sudah memenuhi atribut level 1 and 2.

Tabel 5. Kapabilitas DSS05

No	Sub Proses	Capabilitas	
		Nilai	Level
1	DSS05.01	0,75	1
2	DSS05.02	2,11	2
3	DSS05.03	1,88	2
4	DSS05.04	1,87	2
5	DSS05.05	1,64	2
6	DSS05.06	1,70	2
7	DSS05.07	2,00	2
Hasil		1,7	2

5.2 Pencapaian Pusat Komputer

Berdasarkan *Benchmark* Panduan *data center* Kominfo maka untuk menghasilkan tingkat kapabilitas 3, peneliti melakukan pengamatan kelengkapan yang telah dicapai Pusat Komputer. Hasil pencapaian pada proses APO13 dan DSS05 telah dideskripsikan pada Tabel 6 dan 7.

Tabel 6. Pencapaian APO13

No	Pencapaian	Ketersediaan		
		Ada	Tidak	Bukti
1	Pencegahan kebakaran	Ya		alat pemadam kebakaran
2	Penggunaan listrik secara aman	Ya		UPS
3	Penggunaan perangkat transmisi data optik		Tidak	
4	Pengangkatan beban berat		Tidak	

Tabel 7. Pencapaian DSS05

No	Pencapaian	Ketersediaan		
		Ada	Tidak	Bukti
1	Setiap jendela memungkinkan akses langsung ke *data center*, diberi pengaman fisik	Ya		Teralis
2	*Data center* harus diamankan selama 24 jam dengan paling sedikit 1 orang petugas per *shift*		Tidak	
3	Perangkat sistem pemantau visual (CCTV) harus dipasang untuk memantau dan merekam setiap aktivitas pada ruang komputer, ruang mekanik dan kelistrikan, ruang telekomunikasi dan kawasan kantor	Ya		CCTV
4	Akses ke dalam ruang komputer menggunakan perangkat yang dikendalikan dengan mekanisme otentifikasi	Ya		*Finger print*

5.3 Penentuan *Gap*

Pada tahap ketujuh, peneliti melakukan pelaporan dari hasil evaluasi yang bertujuan untuk memberikan rekomendasi dalam mengelola keamanan dan mengelola layanan keamanan. Berikut rekomendasi yang dihasilkan:

1. Pusat Komputer direkomendasikan memiliki prosedur untuk pencegahan kebakaran seperti adanya SOP atau mekanisme jika terjadi kebakaran
2. Pusat Komputer direkomendasikan untuk memiliki prosedur untuk menangani penggunaan listrik secara aman seperti adanya SOP atau kebijakan ketika listrik mati
3. Pusat Komputer direkomendasikan untuk memiliki SOP untuk mengatur pengangkatan beban berat.

Tabel 8. Penentuan gap

Proses	Keterangan	*Gap*
APO13	Mengelola Keamanan	- Pusat Komputer telah memiliki sistem pencegahan kebakaran, namun belum memiliki prosedur pencegahan kebakaran. - Pusat Komputer telah memiliki perangkat keamanan listrik UPS namun belum memiliki prosedur penggunaan listrik secara aman - Pusat Komputer belum memiliki panduan keamanan terkait pengangkatan beban berat.
DSS05	Mengelola Layanan Keamanan	- Pusat Komputer belum mengamankan *data center* selama 24 jam dengan paling sedikit satu orang per *shift*.

VI. KESIMPULAN

Berdasarkan hasil analisa yang telah dilakukan pada thapan sebelumnya, maka dapat disimpulkan pada proses APO13 (Mengelola Keamanan Informasi) dan DSS05 (Mengelola Layanan Keamanan) diketahui tingkat kapabilitas saat ini berada pada level 2 (*Managed Process*) dengan nilai kapabilitas masing-masing 1,54 dan 1,70 yaitu proses telah dijalankan, dikontrol, dikelola dengan tepat. Yaitu direncanakan berdasarkan dengan rencana kerja organisasi, dimonitor untuk hasilnya dilaporkan pada laporan akuntabilitas organisasi dan disesuaikan sesuai dengan visi dan misi organisasi.

Setelah melakukan analisa keamanan informasi *data center*, (Tabel 4 dan 5) pada proses APO13 (Mengelola Keamanan Informasi) dan DSS05 (Mengelola Layanan Keamanan) diketahui tingkat kapabilitas saat ini berada pada level 2 (*Managed Process*). Maka ditetapkan nilai kapabilitas yang harus dicapai selanjutnya berada pada level 3

(*Established Process*). Artinya proses telah dijalankan dengan kebijakan-kebijakan yang telah dibuat untuk mencapai hasil dari proses. Untuk mencapai tingkat kapabilitas yang diharapkan, Pusat Komputer harus menutup gap dengan membuat kebijakan dengan detil, dikelola dengan standar yang jelas sehingga mampu mencapai tujuan. Selain itu, pada tingkat kapabilitas ini Pusat Komputer harus dapat mengimplementasikan kebijakan dan standar yang dibuat.

REFERENSI

[1] Zulhuda, S. "Information Security In The Islam Perspective: Principle and Practices," Information and Communication Technology for The Muslim World (ICT4M), March 13, 2010.

[2] Van Grembergen, W. "Introduction to the minitrack "IT governance and its mechanisms" HICSS 2013," Proceedings of the Annual Hawaii International Conference on System Sciences, 2013.

[3] Whitman, M.E. "Principles of Information Security," Course Technology Whitman, M. E., & Mattord, H. J. (2012). Principles of Information Security. Course Technology, 2012, June 7, 2012.

[4] ITGI, IT Assurance Guide: Using COBIT, USA: ITGI, 2007.

[5] Gustavo, S. Data Center Fundamentals, Indanapolis: Cisco Press, 2014.

[6] Jayaswal, K. Administering Data Centers: Servers, Storage, and Voice Over IP, Indianapolis: Wiley Publishing, Inc, 2006.

[7] Isaca, COBIT: A Business Framework for the Governance and Management of Enterprise IT, USA: Isaca, 2013.

[8] Isaca, COBIT 5: Enabling Process, USA: Isaca, 2012.

[9] Isaca, COBIT 5: Implementation, USA: ISaca, 2012.

[10] Isaca, Process Assessment Model: Using COBIT 5, USA: ISaca, 2013.

[11] Isaca, COBIT 5: Enabling Processes, USA: Isaca, 2012.

[12] Isaca, COBIT 5: Foundation With Case Study (ITG-2531.10), USA: Isaca, 2012.