Audit Tata Kelola Keamanan Data Teknologi Informasi Menggunakan COBIT 4.1 Pada PT. KLM.

Umar Faruq Vista[1], Bambang Soedijono W A[2], Ferry Wahyu Wibowo[3*]
[1]Universitas AMIKOM Yogyakarta
[2,3]Magister Teknik Informatika Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara, Condong Catur, Depok, Sleman, Yogyakarta 55283 - Indonesia
[1]umar.vista@students.amikom.ac.id, [2]bambang.s@amikom.ac.id, [3]ferry.w@amikom.ac.id

INTISARI

Pada saat ini, perkembangan sebuah teknologi informasi sangatlah maju dan pesat. Teknologi tersebut dapat memiliki data yang berisiko terhadap hilangnya data atau data dicuri. Maka, diperlukan analisis keamanan informasi yang terdapat pada PT. KLM sehingga dapat ditangani yang dapat menjaga kerahasian data. Dalam analisis ini diperlukan Deliver and Support cobit yaitu COBIT 4.1 yang digunakan untuk menilai atau mengukur tingkat kematangan dari perusahaan tersebut. Penelitian ini bertujuan untuk mengetahui tatakelola teknologi informasi berjalan dan tingkat kematangan berdasarkan Deliver and Support COBIT 4.1. Penelitian ini menggunakan metode yang terdapat pada COBIT 4.1 dengan menggunakan sub domain DS5 yang memiliki fungsi untuk memelihara integritas dari informasi dan melindungi aset-aset informasi yang dimiliki perusahaan PT.KLM dalam proses manajemen keamanan. Setelah dilakukan analisis pada sub domain DS5 pada Deliver and Support COBIT 4.1 didapatkan hasil nilai kematangan dengan jumlah 3.56 dari ukuran nilai 0 sampai 5, yang berarti bahwa PT.KLM telah memiliki tata kelola teknologi informasi yang baik.

Kata kunci— *Tata kelola, Keamanan, COBIT 4.1, Tingkat Kematangan,Sub domain DS5.*

ABSTRACT

The development of an information technology is very advanced and rapid now. The technology can have data that is at risk of losing stolen data or data. Then an information security analysis is needed at PT. KLM can be handled which can maintain the confidentiality of data. In the analysis, a cobit Deliver and Support is needed, namely COBIT 4.1 which is used to assess or measure the maturity level of the company. This study aims to determine the current information technology management and maturity level based on the COBIT 4.1 Deliver and Support . This study uses the method found in COBIT 4.1 by using the DS5 sub domain which has a function to maintain the integrity of information and protect the information assets owned by the company PT.KLM in the security management process. After analyzing DS5 sub domain on COBIT 4.1 Deliver and Support , the results of maturity values were obtained with the amount of 3.56 from the size values of 0 to 5, which means that PT. KLM already has good information technology governance.

Kata kunci— *Governance, Security, COBIT 4.1, Maturity Level, Sub domain DS5.*

I. PENDAHULUAN

Kebutuhan teknologi informasi pada sebuah perusahaan sangatlah penting. Hal ini dikarenakan dapat meningkatkan kinerja dan menghemat waktu pada proses bisnis perusahaan. Agar fungsi tersebut dapat berjalan dengan lancar maka membutuhkan tata kelola TI yang sesuai dan benar dengan tujuan dapat memberikan keberhasilan suatu perusahaan dalam mencapai taget yang ingin dituju. Salah satu bagian yang diperhatikan adalah bagian keamanan.

Bagian keamanan berperan penting dalam menjaga semua informasi tetap rahasia,tersedia dan dapat diakses oleh pihak yang berwenang. Agar bagian tersebut tidak mengalami masalah yang membahayakan informasi ketika sistem yang dijalankan sesuai dengan ketentuan serta dijauhkan dari masalah kejahatan seperti pencurian data maka perlu adanya penelitian ini untuk menganalisis keamanan informasi menggunkan *Deliver and Support* COBIT 4.1 yang telah ditetapkan oleh ITGI (*The IT Governance Institute*) dan ISACA (*Information System Audit and Control Association*). *Deliver and Support* ini adalah kerangka kerja yang akan digunakan oleh perusahaan dalam mencapai target yang ingin dicapai.

Penelitian ini mengambil sub domain DS5 pada kerangka COBIT 4.1 yang memiliki peran untuk memelihara integritas informasi yang terdapat pada perusahaan dan melindungi aset teknologi yang berhubungan dengan pengelolaan keamanan.

Dalam penelitian yang dilakukan oleh Loisa, Hosea, Claudio, Alvin, Anthonio, Fernandes, dan Andry (2018). Mereka melakukan penelitian tentang Audit sistem keamanan teknologi informasi di Pt. MNC Sekuritas Menggunakan Cobit 4.1 Domain DS5. Penelitian tersebut dilakukan untuk mengetahui tingkat keamanan yang ada agar, tidak mengalami kendala yang serius ketika sistem yang diterapkan tidak berjalan dengan semestinya dan terhindar dari kejahatan *hacker* atau pihak-pihak yang ingin memasuki tanpa mempunyai hak akses, maka diperlukannya suatu analisis keamanan informasi yang mengunakan *Deliver and Support* COBIT 4.1. Alasan mereka mengunakan *Deliver and Support* COBIT 4.1 adalah karena *Deliver and Support* COBIT 4.1 merupakan kerangka kerja yang dapat digunakan oleh perusahaan tersebut untuk membantu mencapai tujuan yang diinginkan dan mereka mengambil sub domain DS 5 dikarenakan sub tersebut mempunyai kebutuhan memelihara integritas dari informasi dan melindungi aset teknologi informasi membutuhkan proses manajemen keamanan.

Jika penelitian ini tdak diberlakukan pada PT. KLM maka akan menyebakan data-data tersebut rawan dalam jangka yang panjang. Dikhawatirkan terjadi pencurian data-data yang penting ini suatu saat akan menyebabkan kerugian atau malasah dalam jangka pendek maupun jangka panjang seperti jika data yang penting akan diketahui oleh pihak yang tidak bertanggung jawab jika tidak diorganisasikan dengan baik dan ini dapat menjadi salah satu masalah sehingga dibutuhkan suatu analisis keamanan informasi pada perusahaan ini. Hal ini juga dapat meminimalisir kerawanan dan ancaman yang dapat menggangu kinerja perusahaan tersebut yang disebabkan oleh perkembangan teknologi informasi dan komunikasi yang semakin canggih dan kompleks.

Dalam penelitian ini akan dilakukan pengukuran tingkat kematangan (maturity level) untuk memastikan keamananan sistem di perusahaan kemenag berdasarkan *Deliver and Support* COBIT 4.1. Untuk melakukan pengukuran tingkat kematangan tersebut maka peneliti akan mengumpulkan data terlebih dahulu dengan cara melihat secara langsung tempat perusahaan tersebut dengan begitu peniliti dapat melihat proses kinerja yang ada pada perusahaan ini. Setelah melihat kinerja dari perusahaan tersebut maka penelti akan memberikan beberapa kuesioner kepada pegawai perusahaan berdasarkan *Deliver and Support* COBIT 4.1 lalu dilanjutkan penghitungan hasil dari kuesioner tersebut dan hasil perhitungan tersebut dianalisis sehingga dapat mengetahui tingkat kematangan keamanan yang ada. Langkah selanjutnya setelah mengetahui tingkat kematangan, peneliti dapat mengeluarkan beberapa rekomendasi sesuai dengan *Deliver and Support* COBIT 4.1 yang dapat diterapkan pada perusahaan tersebut sehingga dapat membantu proses kinerja yang ada.

A. Rumusan Masalah

Analisis yang sesuai dengan *Deliver and Support* COBIT 4.1, jika dilakukan dengan benar maka dapat membantu proses kinerja PT KLM. Berikut ini merupakan rumusan masalah yang ada:

Bagaimana tingkat kematangan memastikan keamanan sistem informasi di Perusahaan Kementerian Agama Pangkal Pinang diukur dengan menggunakan *Deliver and Support* COBIT 4.1?

B. Tujuan

Tujuan dari penelitian ini adalah mengetahui tata kelola sistem keamanan dan tingkat kematangan dari sistem dengan menggunakan COBIT 4.1 dan perusahaan PT. KLM mengetahui potensi kekurangan dengan tingkat keamanan sistem informasi dikelola dan memudahkan pihak manajemen untuk mengetahui arah sistem informasi berjalan dengan seharusnya

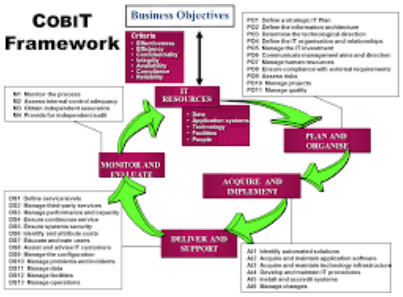
C. Manfaat

Manfaat yang didapat seperti penelitian ini memberikan pengetahuan hasil dari pengukuran tingkat kematangan pada aspek keamanan menurut kerangka kerja COBIT 4.1.

II. METODOLOGI PENELITIAN

Pengukuran tata kelola dengan COBIT 4.1 pada aspek keamanan dinilai tepat karena COBIT memiliki standar pada *Deliver and Support* domain yang berisikan dari kumpulan proses yang menampilkan aktivitas terkendali dan terstruktur. Dasar ini cukup untuk digunakan pada perusahaan PT. KLM dalam mengukur tingkat kematangan pada aspek keamanannya.

Di dalam COBIT 4.1 terdapat model proses yang dibagi menjadi 4 domain dan 34 kontrol objektif tingkat atas. Kerangka kerja Cobit secara keseluruhan ditampilkan dalam gambar 1. Pada gambar 1 menampilkan gambaran proses COBIT 4.1 yang terdiri dari 4 Domain dan 34 macam proses.



Gambar 1. Proses Cobit 4.1

Walaupun COBIT 4.1 secara khusus sebagai parameter keamanan namun didalamnya terdapat satu domain yang membahas tentang keamanan teknologi informasi. Domain tersebut adalah DS5 (*Delivery and Support*) yang mempunyai 11 kontrol objektif yang dapat dipakai dalam menentukan sistem keamanan sehingga dijadikan alat untuk pengauditan keamanan teknologi informasi pada PT. KLM.

A. Tinjauan Pustaka

Tinjauan Pustaka merupakan sarana untuk menunjukkan keaslian penelitian. Bagian ini memuat uraian sistematis tentang informasi hasil penelitian sebelumnya yang relevan dengan penelitian yang akan dilakukan. Penelitian ini juga menjadikan penelitian yang telah dilakukan sebelumnya sebagai bahan tinjauan dan pembanding antara penelitian yang telah ada dan penelitan ini.

1) Penelitian Loisa, Hosea, Claudio et al (2018) meneliti tingkat kematangan sebuah perusahaan investasi pada bidang jasa keuangan yang telah terintegrasi dan tersebar di Indonesia. Perusahaan tersebut adalah perusahaan PT MNC Sekuritas (MNC Sekuritas) yang dimiliki oleh PT MNC Investama Tbk melalui perusahaan yang dikendalikannya yaitu PT. MNC Kapital Indonesia Tbk. Dalam penelitian mereka dibutuhkan analisis keamanan informasi dengan menggunakan *Deliver and Support* COBIT 4.1. Alasan mereka menggunakan *Deliver and Support* COBIT 4.1 adalah untuk menghindari masalah yang serius saat penerapan sistem tidak bekerja dengan semestinya dan mencegah kejahatan yang dilakukan oleh *hacker* atau pihak yang tidak bertanggungjawab atas hak akses pada sistem tersebut. Dalam *Deliver and Support* COBIT 4.1 terdapat 4 domain dan mereka memilih domain *Deliver and Support (DS)* dengan kontrol objek DS5 yang membahas tentang pemastian keamanan sistem. Penelitian mereka menghasilkan rata-rata tingkat kematangan 3 yang berada pada level 3 sehingga mereka menyimpulkan bahwa kepedulian perusahaan mengenai sistem keamanan dinilai sudah baik dan komunikasi berlangsung secara konsisten dan terdokumentasi.

2) Sebuah Penelitian yang dilakukan oleh Ayu, Eko, dan Rudy (2017) meneliti tentang penyusunan tata kelola keamanan informasi pada produksi film animasi pada PT. XX. Perusahaan PT.XX merupakan perusahaan swasta yang memproduksi film animasi. Dalam penelitian mereka dibutuhkan analisis keamanan informasi dengan menggunakan SNI ISO/IEC 27001:2009. Alasan mereka menggunakan SNI ISO/IEC 27001:2009 adalah tersedianya kerangka kerja untuk netralitas penggunan teknologi dengan adanya kerahasiaan dan integritas atas informasi yang dimiliki serta kebutuhan pihak-pihak berkepentingan sesuai dengan hak wewenang yang diperoleh. Penelitian mereka bertujuan untuk menyusun tata kelola informasi yang baik untuk PT. XX agar produksi film animasi dapat berjalan dengan baik. Penelitian mereka menghasilkan perancangan kebijakan keamanan informasi dan pedoman klasifikasi. Pada penelitian tersebut menggunakan metode gap analisis.

3) Penelitian Aziz (2017) meneliti tentang pengevaluasian keamanan data pada Bank Perkreditan Rakyat (BPR) XYZ melalui audit tata kelola teknologi informasi. Sistem informasi di BPR XYZ terkait dengan kegiatan utama perbankan seperti produk tabungan, deposito, dan kredit. Dalam penelitiannya dibutuhkan analisis keamanan informasi dengan menggunakan kerangka kerja COBIT 4.1. Alasan dia menggunakan kerangka kerja COBIT 4.1 adalah untuk meningkatkan keamanan data pada BPR XYZ dan sebagai alat untuk melakukan analisis. Dalam framework COBIT 4.1 terdapat 4 domain dan dia memilih domain Acquire and Implement (AI) dan Deliver and Support (DS) dengan kontrol objek AI2, AI3, DS3, DS5, DS11, dan DS12. Penelitiannya menghasilkan rata-rata tangka kematangan dengan nilai 2.38 yang berada pada skala level 2 dalam artian tata kelola sudah dilakukan tetapi belum baku. Pada penelitian tidak diterangkan realibilitas terhadap hasil kuesioner yang telah diisi responden guna mendapatkan hasil optimal. Maka penelitian yang akan diajukan akan menguji realibilitas terhadap hasil kuesioner.

4) Penelitian berikutnya dilakukan oleh Darwis dan Yuniarwati (2016) meneliti tentang audit tata kelola teknologi informasi sebagai upaya penigkatan keamanan data pada dinas pendidikan dan kebudayaan Kabupaten Pesawaran. Dinas pendidikan dan kebudayaan

kabupaten adalah dinas pemerintah yang bertigas dalam dunia pendidikan yang ada pada Kabupaten Pesawaran. Dinas pendidikan dan kebudayaan tersebut mengelola data dari masing-masing sekolah yang dapat digunakan dalam pengolahan data sertifikasi. Dalam penelitian mereka dibutuhkan analisis keamanan informasi dengan menggunakan framework COBIT 4.1. Alasan mereka menggunakan *framework* COBIT 4.1 adalah untuk mengetahui tingkat kematangan dan memberikan rekomendasi sistem keamanan berdasarkan analisis *framework* COBIT 4.1. Dalam *framework* COBIT 4.1 terdapat 4 domain dan mereka memilih domain *Acquire and Implement (AI)* dan *Deliver and Support (DS)* dengan kontrol objek AI2, AI3, DS3, DS5, DS11, dan DS12. Penelitian ini dilakukan untuk tujuan mengetahui pengelolaan tatakelola teknologi informasi dan tingkat kematangan teknologi informasi berdasarkan metode COBIT 4.1. Penelitian mereka menghasilkan nilai rata-rata angka kematangan 3,73 yang berada pada level 3 sehingga membutuhkan perhatian lebih pada proses tersebut untuk mempertahankan teknologi informasi yang ada.

B. Landasan Teori

1) Keamanan Sistem Informasi

Keamanan informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki atau suatu usaha pencegahan atas serangan untuk mendapatkan sesuatu dari sistem informasi baik melalui akses yang tidak semestinya maupun penggunaan yang tidak semestinya. Didalam keamanan informasi ada 4 hal yang perlu diperhatikan yaitu :

- *Confidentiality*: Penjagaan informasi dari pihak yang tidak memiliki hak akses terhadap informasi tersebut.
- *Integrity*: Informasi yang dikirim dan diterima harus asli, maksudnya tidak dapat diubah oleh pihak yang tidak bertanggungjawab atas informasi tersebut.
- *Authentication*: agar penerima informasi dapat memastikan keaslian informasi tersebut datang dari orang yang dimintai informasi.
- *Avability*: Informasi yang berada pada sistem jaringan dapat tersedia pada waktu kapanpun ketika dibutuhkan.

Pengimplementasian seperangkat alat kontrol yang layak, seperti kebijakan, pedoman kerja, struktur organisasi hingga perangkat lunak akan memperoleh keamanan informasi. Keamanan informasi tersebut memiliki berbagai macam risiko yang akan dihadapi dari berbagai perspektif yaitu internal dan eksternal seperti bencana alam.

Salah satu contoh kasus adanya kebocoran informasi yang terjadi pada tahun 2015 yaitu kasus perusahaan Anthem. Perusahaan tersebut merupakan perusahaan asuransi kesehatan Amerika. Pada saat itu pihak perusahaan mengumumkan kepada nasabahnya berkenaan serangan *cyber*. Perusahaan pemegang polis dibeberapa produknya diantaranya *Blue Cross* dan *Blue Shield* menggunakan layanan dari perushaan Anthem. Jumlah nasabah dan karyawan yang terkena serangan mencapai 80 juta pada satu minggu sebelum serangan berhasil terdeteksi. Pelaku kejahatan mencuri identitas personal nasabah dari *server* perusahaan, dengan cara masuk ke *database*, menggunakan data kredensial milik *administrator*, dan kemudian mengunduh data-data tersebut.

2) COBIT

Pada tahun 1967 didirikan Sebuah organisasi dengan bidang tata kelola teknologi informasi di Amerika Serikat yang bernama ISACA. Pada tahun 1996, ISACA mengembangkan sebuah kerangka kerja manajemen teknologi informasi untuk membantu suatu bisnis dalam mengembangkan, mengatur, dan menerapkan strategi seputar manajemen informasi dan tata kelola yang disebut dengan COBIT *(Control Objectives for Information and Related Technologies)*. Awalnya Cobit dirancang untuk membantu komunitas audit keuangan menavigasi dengan lebih baik pertumbuhan lingkungan teknologi informasi. Lalu pada tahun 1998, COBIT diperluas untuk diterapkan diluar komunitas audit dan kemudia pada tahun 2000, COBIT membawa manajemen teknik informasi dan teknik tata kelola informasi yang ditemukan dalam kerangka kerja saat ini.

Penggunaan COBIT dengan cepat mendapatkan perhatian besar yang diberikan terhadap *corporate governance* dan kebutuhan perusahaan sehingga dapat berbuat lebih dengan sumber daya yang sedikit meskipun ketika terjadi kondisi ekonomi yang sulit. COBIT telah tersedia dalam bahasa yang umum sehingga semua pihak mampu memahaminya.

COBIT memiliki fokus utama yaitu harapan bahwa melalusi adopsi COBIT ini perusahaan akan mampu meningkatkan nilai tambah melalui penggunaan TI dan mengurangi risiko-risiko dengan hubungan erat yang teridentifikasi didalamnya.

3) COBIT 4.1

COBIT 4.1 diterbitkan pada tahun 2007 dan memiliki 2 tugas yaitu pada tata

kelola (governance) dan kepatuhan (compliance). COBIT 4 memiliki prinsip yaitu sebagai penyedia informasi bagi organisasi dengan cara mengelola dan mengendalikan sumberdaya TI (aplikasi, informasi,infrastruktur dan orang) dengan menggunakan sekumpulan proses-proses yang terstruktur. Agar tujuan manajemen dalam mengelola dan mengendalikan sumberdaya TI dapat dilakukan maka diperlukan "kebijakan, perencanaan dan prosedur, dan ada struktur organisasi" yang dirancang dengan baik. Untuk mewujudkan tujuan manajemen tersebut, COBIT memberikan kerangka kerja tata kelola TI dan panduan secara detail *(DCO – detailed control objective)*. Panduan ini terdiri atas empat domain utama dengan 34 proses pengendalian TI. Domain tersebut berjumlah 4 yaitu:

- *Plan and Organize - PO*
  Domain ini mencangkup masalah mengidentifikasikan cara terbaik TI untuk memberikan kontribusi yang maksimal terhadap pencapaian tujuan bisnis organisasi
- *Acquire and Implement - AI*
  Domain ini bertanggung jawab pada proses pemilihan, pengadaan dan penerapan TI yang digunakan.
- *Deliver and Support - DS*
  Domain ini bertangungjawab atas proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan
- *Monitor and Evalute – ME.*
  Domain ini bertanggungJawab atas proses pengawasan pengelolaan TI pada organisasi seluruh kendali-kendali yang diterapkan setiap proses TI harus diawasi dan dinilai kelayakannya secara berkala

Setiap proses memiliki keterkaitan dengan domain untuk mendapatkan hasil pengelolalan TI yang baik. Adapun kriteria kontrol pada pengelolaan TI dalam COBIT 4.1 berupa efektivitas, efisiensi, kerahasiaan, integritas, ketersediaan, kepatuhan, dan keandalan.

4) *Maturity Model*

Maturity Model mempunyai model kematangan (*maturity models*) untuk mengontrol proses-proses TI dengan menggunakan metode penilaian (*scoring*) sehingga suatu organisasi dapat menilai proses-proses TI yang dimilikinya dari skala *nonexistent* sampai dengan optimised (dari 0 sampai 5) (ITGI, 2007). 0 – *Non Existent*, Perusahaan sama sekali tidak peduli akan pentingnya teknologi informasi untuk kelola secara baik oleh pihak manajemen.

- *Initial / Ad Hoc,*
  Perusahaan secara reaktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya.
- *Repeatable but Intituitive*,
  Perusahaan telah memiliki pola yang berulangkali dilakukan dalam melakukan manajemen aktivitas terkait dengan tata kelola teknologi informasi, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan.
- *Defined*,
  Perusahaan telah memiliki prosedur baku formal dan tertulis yang telah disosialkan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.
- *Managed and Measurable*,
  Perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun objektif kinerja setiap
  penerapan aplikasi teknologi informasi yang ada.
- *Optimised*,
  Perusahaan telah meng implementasikan tata kelola teknologi informasi yang mengacu pada "*Best Practice*".

Dalam menghitung indeks tingkat kematangan (IKA) dapat menggunakan rumus sebagai berikut:

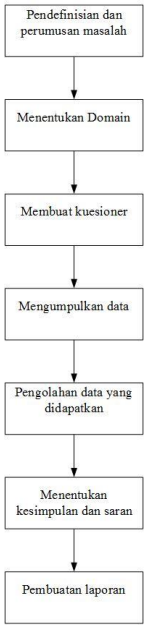
$$\text{IKA} = \sum \left(\frac{Total\ Jawaban}{Jumlah\ Responden}\right) \ldots\ldots..(1)$$

Dari rumus maka akan didapatkan indeks kematangan dan akan dilihat hasil tersebut masuk dalam *level* ke berapa. Dengan adanya *maturity level model*, maka organisasi dapat mengetahui posisi kematangannya saat ini, dan secara terus menerus serta berkesinambungan harus berusaha untuk meningkatkan levelnya sampai tingkat tertinggi agar aspek *governance* terhadap teknologi informasi dapat berjalan secara efektif. Salah satu cara menghitung tingkat kematangan adalah sebagai berikut:

- Mengembangkan kuesioner dengan mengacu pada tingkat kematangan proses tata kelola TI berdasarkan *framework* COBIT 4.1.
- Menghitung bobot semua proses tata kelola berdasarkan hasil kuesioner.
- Menghitung tingkat kematangan berdasarkan proses-proses tata kelola terkait.
- Menentukan nilai kontribusi tiap tingkat kematangan dengan cara
- membagi nilai tingkat kematangan dengan total tingkat kematangan.
- Mengalikan nilai kontribusi dengan masing-masing tingkat kematangan.
- Menjumlahkan semua nilai kontribusi yang didapat.
- Total Nilai Kontribusi = Tingkat Kematangan Proses

C. Tahapan Penelitian

Dalam penelitian ini akan menggunakan metode yang akan ditampilkan pada gambar 2.



Gambar 2. Langkah-langkah Penelitian

Langkah-langkah tersebut dibagi menjadi 7, langkah tersebut adalah:

1. Pendefinisian dan perumusan masalah
   Langkah awal ini dilakukan perumusan masalah pada objek penelitian yang berhubungan keamanan sistem informatka.
2. Menentukan Domain
   Langkah kedua yaitu memilih atau menetukan domain yang pantas terkait keamanan teknologi informasi. Maka digunakan DS5 dengan peran sebagai pemasti keamanan.
3. Membuat kuesioner
   Pada langkah ini, peneliti membuat kuesioner sesuai dengan *Deliver and Support* COBIT 4.1 yang akan dibagikan kepada responden.
4. Mengumpulkan data
   Peneliti memberikan pertanyaan dasar dan akan mewawancari narasumber pada PT.KLM lalu jawaban tersebut dikumpulkan.
5. Pengolahan data yang didapatkan
   Data yang didapatkan akan diolah.
6. Menentukan kesimpulan dan saran
   Tahap ini akan dibuatkan kesimpulan berdasarkan hasil yang telah didapatkan dan saran untuk perbaikan pada perusahaan PT.KLM.
7. Pembuatan laporan
   Tahap terakhir ini adalah semua hasil akan dituliskan dalam bentuk laporan.

D. Metode Pengumpulan Data

Dalam penelitian ini data-data yang dikumpulkan menggunakan metode sebagai berikut:

1. Wawancara
   Dalam metode ini, penulis akan membuatkan beberapa pertanyaan yang akan diajukan kepada narasumber pada perusahaan PT.KLM, pertanyaan tersebut akan ditanyakan secara acak akan tetapi sudah mencangkup semua data yang diinginkan. Hasil dari mewawancari narasumber tersebut akan digunakan untuk mendukung peneliti yang didapatkan dari hasil kuesioner.
2. Observasi
   Metode ini akan merupakan cara peneliti mendapatkan data dengan mengunjungi dan mengamati secara langsung kinerja dari pengguna teknologi informasi pada perusahaan PT.KLM.
3. Kuesioner
   Data dikumpulkan dengan menggunakan sekumpulan daftar pertanyaan kepada pihak yang terkait dalam sistem informasi dengan ditentukan melalui metode sampling. Kuesioner yang akan digunakan yaitu kuesioner sesuai dengan kerangka kerja COBIT 4.1 pada domain *Deliver*

and Support (DS) dengan kontrol objek DS5. Metode digunakan dalam mengumpulkan data dengan cara memberikan pernyataan kepada responden dan diminta memilih apakah ia sangat setuju, setuju, netral, tidak setuju, atau sangat tidak setuju terhadap sistem yang akan diusulkan.

E. Analisis Data

Berdasarkan data hasil kuesioner dilakukan analisis untuk menilai tingkat kematangan saat ini untuk proses DS5. Pada analisis tingkat kematangan saat ini, dilakukan penilaian terhadap masing-masing aktivitas. Sedangkan untuk hasil jawaban kuesioner tingkat kematangan, akan tersedia 4 pilihan jawaban dengan nilai 0-5. Tingkat kematangan atribut diperoleh dari perhitungan total pilihan jawaban kuesioner dengan rumus dan pembobotan pilihan jawaban. Hasil tersebut akan dikategorikan berdasarkan *level* sehingga dapat disimpulkan. Adapun rumus perhitung-annya adalah

$$\text{Rata-rata} = \sum Xi = \frac{X1 + X2}{n} + ...+ \frac{Xn}{n}$$

Keterangan:
$\sum$ = Jumlah dari X
X_1 = Nilai point pada setiap pertanyaan
n = Jumlah Kuesioner

III. HASIL DAN PEMBAHASAN

Pada hasil pengindetifikasian dapat dibuat proses bisnis teknologi informasi yang dibutuhkan pada penelitian dan ditampilkan pada tabel 1.

Tabel 1. Domain Yang digunakan

Domain	Proses
Delivery and Support	DS 5

Pada tabel 1 terdapat detail detail kontrol objektif (alat kontrol dari proses teknologi informasi). Pada penelitian ini ada 7 detail kontrol objektif. Adapun hasil penilaian pada domain DS5 akan ditampilkan pada tabel 2.

Tabel 2. Hasil Penilaian domain DS5

Delivery and Support (DS)		
DS5 Memastikan Keamanan Sistem		*Hasil*
DS5.1	Pengelolaan Keamanan.	4
DS5.2	Perencanaan Keamanan TI.	3
DS5.3	Pengelolaan Identitas.	3
DS5.4	Pengelolaan akun pengguna.	3
DS5.5	Pengujian keamanan, pengawasan, dan pemerhatian.	3
DS5.9	Pencegahan, pendektesian dan pengoreksian perangkat lunak berbahaya	4
DS5.10	Pengamanan Jaringan	4
DS5.11	Menukar Data Rawan	4
Rata-rata		3.5

Dari tabel 2 dapat dijelaskan bahwa:
DS5.1: Didapatkan nilai *maturity level* 4 yaitu *Managed and Measurable* karena sudah memiliki ukuran yang diterapkan pada kerangka pengelolaan sistem keamanan. Dengan artian Sistem keamanan sudah terstandarisasi. Salah satu buktinya adalah adanya pembedaan hak akses terhadap masing pelaku dalam aplikasi teknologi informasi pada PT .KLM.
DS5.2: Diberikan nilai *maturity level* 3 yaitu *Defined Level* karena PT. KLM sudah
Memberikan arahan rencana keamanan TI pada orang yang bertanggung jawab dengan cara mengirimkan pesan surel ke semua pegawai.
DS5.3: Diberikan nilai *maturity level* 3 yaitu *Defined Level* karena teknologi informasi pada PT. KLM telah ada pengecekan dan penggolongan hak ases. Setiap pengguna sudah dikenali dan diklasifikasi dengan baik serta hak akses telah dibatasi dan ditetapkan dengan baik. Pernyataan ini didukung dengan kartu akses dan presensi menggunkan sidik jari sebelum memulai bekerja. ID pengenal dan kata sandi yang khusus untuk masuk ke dalam sistem pada setiap komputer di PT. KLM.
DS5.4: Diberikan nilai maturity level 3 yaitu *Defined Level* karena penggolongan hak akses pengguna yang berhubungan dengan tata cara pengelolaan akun di PT. KLM sudah mempunyai tata cara yang baik. Penggolongan tersebut seperti tingkatan Super Admin, tigkatan Admin dan tingkatan pegawai secara hakikat pemilik akun di PT. KLM.
DS5.5: Diberikan nilai maturity level 3 yaitu *Defined Level* karena mempunyai tata cara yang baik dalam menguji, menjaga dan memerhatikan keamanan TI. Hal ini didukung dengan aplikasi perangkat lunak pengawas dalam menguji, menjaga dan memerhatikan. Peringatan akan disampikan melalui surel jika ada *trouble* di PT KLM.

DS5.9: Diberikan nilai *maturity level* 4 yaitu Managed Level karena tata cara mencegah aplikasi berpotensi merusak keamanan system, mendeteksi dan memperbaiki jika terjadi kerusakan telah dilakukan dengan baik. Pernyataan ini didukung oleh pemakain aplikasi pendeteksi virus resmi dan berbayar. Lalu komputer pegawai tidak diperbolehkan menginstal aplikasi mencurigakan dan mengunci akses seperti tempat kaset dan *flashdisk* dalam PT KLM.

DS5.10: Diberikan nilai *maturity level* 4 yaitu *Managed Level* karena kebijakan dan tat cara keamanan jaringan di PT. KLM sudah ditentukan dengan baik

DS5.11: Diberikan nilai *maturity level* 4 yaitu *Managed Level* karena PT. KLM sudah memakai persyaratan dan tata cara yang memakai atauran yang telah ditetapkan bagian pemerintah seperti OJK.

IV. KESIMPULAN

Menurut pembahasan yang telah dipaparkan pada bab sebelumnya, maka didapatkan kesimpulan yaitu *maturity level* (tingkat kematangan) dalam pengauditan dalam pemastian keamanan sistem yang berjalan di PT KLM pada domain DS5 COBIT 4.1 dikategorikan tingkat 3 dengan nilai 3.5 yang berada pada *Defined Process*. Hal menunjukkan keadaan perusahaan sudah mempunyai tata cara berstandarkan formal dan tertulis serta sudah diberitahukan kepada seluruh pihak manajemen dan karyawan agar ditaati dan dilaksanakan dalam setiap pekerjaan. Rasa peduli untuk sistem keamanan dihitung telah baik dan hubungan terjadi dengan tetap dan tercatat dalam dokumen.

REFERENSI

[1] J. Loisa, H. Hosea, A. Claudio, … A. A.-J. of B., and undefined 2018, "Audit Sistem Keamanan Teknologi Informasi di PT. MNC Sekuritas Menggunakan COBIT 4.1 Domain DS5," Journal.Ubm.Ac.Id, no. September, 2018.

[2] A. C. Dewi, E. Nugroho, and R. Hartanto, "Penyusunan Tata Kelola Keamanan Informasi Pada Produksi Film Animasi (Kasus Di Pt. Xx)," Pros. SNATIF, pp. 297–302, 2017.

[3] A. Aziz, "Evaluasi Keamanan Data Pada Melalui Audit Tata Kelola Teknologi Informasi Berdasarkan," no. 1, pp. 1–5, 2017.

[4] D. Darwis and . Yuniarwati, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 4.1 sebagai Upaya Peningkatan Keamanan Data pada Dinas Pendidikan dan Kebudayaan Kabupaten Pesawaran," Explore, vol. 7, no. 1, 2016.

[5] H. Haviluddin, H. J. Setyadi, P. P. Widagdo, and M. Taruk, "Perbandingan Fasilitas Cobit 4.0/4.1 Dan Cobit 5 Frameworks : Studi Pengguna Berdasarkan Literatur," Pros. SAKTI (Seminar Ilmu Komput. dan Teknol. Informasi), vol. 1, no. 1, pp. 30–37, 2016.

[6] T. Sutabri, Konsep Sistem Informasi. Yogyakarta: CV ANDI OFFSET, 2012