*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

# AUDIT SISTEM KEAMANAN TEKNOLOGI INFORMASI DI PT. MNC SEKURITAS MENGGUNAKAN COBIT 4.1 DOMAIN DS5

## *Information Technology Security System Audit at PT. MNC Securities Using COBIT 4.1 DS5 Domain*

**Julia Loisa[1)], Hosea[1)], Adam Christian Claudio[1)], Alvin[1)], Anthonio[1)], Johanes Fernandes Andry[1)]**

[1)]Sistem Informasi/Fakultas Teknologi dan Desain, Universitas Bunda Mulia

Diterima 08 Juni 2018 / Disetujui 31 Juli 2018

### *ABSTRACT*

*Information technology requires professional handling because IT has risks and costs that are not small. One aspect that is also an important part of information technology (IT) is the security aspect. hence the need for an information security analysis that uses COBIT 4.1 framework. COBIT 4.1 Framework is a framework that can be used by an agency or company to help achieve the desired goals. COBIT 4.1 Framework on DS5 sub domains has a need to maintain the integrity of information and to protect information technology assets (IT) requires a security management process. After conducting research, PT. MNC Securities gets an average maturity value of 3 on the DS5 Domain which means Defined Process. With the highest maturity value of 5 falling in the DS5.3, DS5.7, DS5.9, DS5.10 and DS5.11 sub domain and the lowest maturity value of 0, namely in DS5.6 and DS5.8. Based on these results, it can be concluded that the application of IT security at PT. MNC Sekuritas is good enough even though there are still some parts that need to be improved so that the results are maximized.*
***Keywords:*** *Security Audit, COBIT 4.1, Domain DS5.*

### ABSTRAK

Teknologi informasi membutuhkan penanganan yang profesional karena TI memiliki resiko dan biaya yang tidak kecil. Salah satu aspek yang menjadi bagian penting juga dalam teknologi informasi (TI) adalah aspek keamanan. maka diperlukannya suatu analisis keamanan informasi yang menggunakan framework COBIT 4.1. Framework COBIT 4.1 merupakan kerangka kerja yang dapat digunakan oleh suatu instansi atau perusahaan untuk membantu mencapai tujuan yang diinginkan. Framework COBIT 4.1 pada sub domain DS5 mempunyai kebutuhan untuk memelihara integritas dari informasi dan untuk melindungi aset teknologi informasi (TI) membutuhkan proses manajemen keamanan. Setelah melakukan penelitian, PT. MNC Sekuritas mendapatkan nilai kematangan rata-rata 3 pada Domain DS5 yang berarti *Defined Process*. Dengan nilai kematangan paling tinggi 4 yang jatuh di sub domain DS5.3, DS5.7, DS5.9, DS5.10 dan DS5.11 lalu nilai kematangan paling rendah diangka 0 yaitu di DS5.6 dan DS5.8. Berdasarkan hasil tersebut, dapat disimpulkan bahwa penerapan keamanan TI pada PT. MNC Sekuritas sudah cukup baik meskipun masih ada beberapa bagian yang perlu ditingkatkan agar hasil menjadi maksimal.
**Kata Kunci:** *Audit Keamanan, COBIT 4.1, Domain DS5.*

## PENDAHULUAN

Teknologi informasi (TI) merupakan suatu kebutuhan yang sangat penting bagi semua instansi maupun perusahaan, karena dipercaya dapat meningkatkan efektifitas dan efesiensi proses bisnis perusahaan. Banyak organisasi melakukan investasi besar dalam TI untuk mengamankan atau mempertahankan keunggulan kompetitif (Andry, 2016 & Applegate et al, 2003). Namun dalam pengelolaannya, TI membutuhkan penanganan yang profesional karena TI memiliki resiko dan biaya yang

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

tidak kecil. Salah satu aspek yang menjadi bagian penting juga dalam teknologi informasi (TI) adalah aspek keamanan.

Seiring dengan berkembangnya sistem informasi dan teknologi informasi pada saat ini, beberapa hal penting yang menjadi faktor penentu agar sistem yang berjalan dapat befungsi dengan baik dan benar adalah tata kelola keamanan TI yang diterapkan. Sebuah sistem mengumpulkan dan menganalisis data dan menghasilkan laporan yang tujuannya adalah membantu para manajer dan manajemen memecahkan masalah terstruktur (Andry et al, 2016 & Andry et al, 2018 & Reddy et al, 2009)

Untuk mengetahui tingkat keamanan yang ada, framework COBIT 4.1 yang dikeluarkan oleh organisasi ISACA memberikan layanan kerangka kerja secara komprehensif untuk membantu manajemen TI dalam sebuah perusahaan dan instansi mencapai tujuan yang diharapkan.

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 sistem tanpa mempunyai hak akses, maka diperlukannya suatu analisis keamanan informasi yang menggunakan framework COBIT 4.1. Framework COBIT 4.1 merupakan kerangka kerja yang dapat digunakan oleh suatu instansi atau perusahaan untuk membantu mencapai tujuan yang diinginkan. Framework COBIT 4.1 pada sub domain DS5 mempunyai kebutuhan untuk memelihara integritas dari informasi dan untuk melindungi aset teknologi informasi (TI) membutuhkan proses manajemen keamanan.

Proses ini meliputi pendirian dan pemeliharaan peran dan pertanggungjawaban, kebijakan-kebijakan, standar-standar, dan prosedur IT Security. Manajemen keamanan dapat dibagi menjadi 3 bagian penting, meliputi penyelenggaraan pengawasan keamanan (security monitoring) dan pengujian periodik (periodic testing) dan pengimplementasian tindakan koreksi untuk mengidentifikasikan kelemahan keamanan dan kejadiannya.

*Korespondensi Penulis:
E-mail: jloisa@bundamulia.ac.id

## STUDI PUSTAKA

### Keamanan Sistem Informasi

Keamanan sistem informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, mengoptimalkan pengembalian investasi (*return on investment*). Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing-kan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan. (Sarno et al, 2009).

Hasil evaluasi dengan menggunakan ISO 17799:2000 dapat menunjukkan seberapa baik (atau seberapa buruk) keamanan informasi yang diterapkan oleh suatu organisasi atau perusahaan (Mokodompit et all, 2016).

### COBIT

COBIT (Control Objectives for Information and Related Technology) adalah kerangka kerja tata kelola IT (IT Governance Framework) dan kumpulan perangkat yang mendukung dan memungkinkan para manager untuk menjembatani jarak (gap) yang ada antara kebutuhan yang dikendalikan (control requirement), masalah teknis (technical issues) dan resiko bisnis (bussiness risk). COBIT mempermudah perkembangan peraturan yang jelas (clear policy development) dan praktik baik (good practice) untuk mengendalikan IT dalam organisasi. COBIT menekankan keputusan terhadap peraturan, membantu organisasi untuk meningkatkan nilai yang ingin dicapai dengan penggunaan IT, memungkinkan untuk menyelaraskan dan menyederhanakan penerapan dari kerangka COBIT (ITGI, 2007).

### Kerangka Kerja COBIT

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

COBIT di rancang terdiri dari 34 high level control objectives yang menggambarkan proses TI yang terdiri dari 4 domain yaitu: Plan and Organise, Acquire and Implement, Deliver and Support dan Monitor and Evaluate. Berikut kerangka kerja COBIT yang terdiri dari 34 proses TI yang terbagi ke dalam 4 domain pengelolaan, yaitu:

1. Plan and Organise (PO), mencakup masalah mengidentifikasikan cara terbaik TI untuk memberikan kontribusi yang maksimal terhadap pencapaian tujuan bisnis organisasi. Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi organisasi. Domain PO terdiri dari 10 control objectives, yaitu:
    a. PO1 – Define a strategic IT plan
    b. PO2 – Define the information architechture
    c. PO3 – Determine technological direction
    d. PO4 – Define IT processes, organisation and relationships
    e. PO5 – Manage the IT investment
    f. PO6 – Communicate management ains and direction
    g. PO7 – Manage IT human resource
    h. PO8 – Manage quality
    i. PO9 – Asses and manage IT risks
    j. PO10 – Manage projects
2. Acquire and Implement (AI), domain ini menitikberatkan pada proses pemilihan, pengadaaan dan penerapan TI yang digunakan. Pelaksanaan strategi yang telah ditetapkan, harus disertai solusi-solusi TI yang sesuai dan solusi TI tersebut diadakan, diimplementasikan dan diintegrasikan ke dalam proses bisnis organisasi. Domain AI terdiri dari 7 control objectives, yaitu:
    a. AI1 – Identify automated solutions
    b. AI2 – Acquire and maintain application software
    c. AI3 – Acquire and maintain technology infrastructure
    d. AI4 – Enable operation and use
    e. AI5 – Procure IT resources
    f. AI6 – Manage changes
    g. AI7 – Install and accredit solutions and changes
3. Deliver and Support (DS), domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan. Domain DS terdiri dari 13 control objectives, yaitu:
    a. DS1 – Define and manage service levels
    b. DS2 – Manage third-party services
    c. DS3 – Manage performance and capacity
    d. DS4 – Ensure continuous service
    e. DS5 – Ensure systems security
    f. DS6 – Identify and allocate costs
    g. DS7 – Educate and train users
    h. DS8 – Manage service desk and incidents
    i. DS9 – Manage the configuration
    j. DS10 – Manage problems
    k. DS11 – Manage data
    l. DS12 – Manage the physical environment
    m. DS13 – Manage operations.
4. Monitor and Evaluate (ME), domain ini menitikberatkan pada proses pengawasan pengelolaan TI pada organisasi seluruh kendali-kendali yang diterapkan setiap proses TI harus diawasi dan dinilai kelayakannya secara berkala. Domain ini fokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan internal dan eksternal. Berikut proses-proses TI pada domain monitoring and evaluate:
    a. ME1 – Monitor and evaluate IT performance
    b. ME2 – Monitor and evaluate internal control
    c. ME3 – Ensure regulatory compliance
    d. ME4 – Provide IT Governance

Dengan melakukan kontrol terhadap ke 34 obyektif tersebut, organisasi dapat memperoleh keyakinan akan kelayakan tata kelola dan kontrol yang diperlukan untuk

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

lingkungan TI. Untuk mendukung proses TI tersebut tersedia lagi sekitar 215 tujuan kontrol yang lebih detil untuk menjamin kelengkapan dan efektifitas implementasi.

### *Maturity Model*

Model Maturity COBIT 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 perduli akan pentingnya teknologi informasi untuk kelola secara baik oleh pihak manajemen.

1 - Initial / Ad Hoc, Perusahaan secara reaktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya.

2 - 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 ketidakkonsistenan.

3 – 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.

4 - 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.

5 – Optimised, Perusahaan telah meng implementasikan tata kelola teknologi informasi yang mengacu pada “Best Practice”.


Gambar 1. *Maturity Model*

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: (ITGI, 2007).

1. Mengembangkan kuisioner dengan mengacu pada tingkat kematangan proses tata kelola TI berdasarkan framework COBIT 4.1.
2. Menghitung bobot semua proses tata kelola berdasarkan hasil kuisioner.
3. Menghitung tingkat kematangan berdasarkan proses-proses tata kelola terkait.
4. Menentukan nilai kontribusi tiap tingkat kematangan dengan cara membagi nilai tingkat kematangan dengan total tingkat kematangan.
5. Mengalikan nilai kontribusi dengan masingmasing tingkat kematangan.
6. Menjumlahkan semua nilai kontribusi yang didapat.
7. Total Nilai Kontribusi = Tingkat Kematangan Proses.

## METODOLOGI PENELITIAN

### Prosedur Penelitian

Peneliti menggunakan prosedur dibawah ini untuk mengembangkan seluruh hasil penelitian:

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*


Gambar 2. Prosedur Penelitian

Prosedur penelitian diatas dibagi menjadi 9 tahapan, yaitu:

1. Memilih dan Menentukan Objek Penelitian, Pada tahap ini dilakukan pemilihan terhadap perusahaan yang ingin diaudit. Kami memilih perusahaan PT MNC Sekuritas.
2. Mendefinisikan dan Merumuskan Masalah, Tahap ini peneliti melakukan pendefinisian dan perumusan masalah terkait keamanan sistem informasi yang ada pada objek penelitian.
3. Menentukan Metodologi Penelitian, Menentukan jenis penelitian dan metode penelitian. Kami memilih jenis penelitian kualitatif dan metode penelitian deskriptif dengan teknik pengumpulan data melalui wawancara. Kami mewawancarai satu narasumber yang menjabat sebagai IT Supervisor di PT MNC Sekuritas.
4. Memilih dan Menentukan Domain COBIT, Setelah menentukan objek penelitian yang ingin diaudit, tahap selanjutnya adalah memilih domain yang sesuai dengan lingkup penelitian berdasarakan COBIT 4.1. Kami memilih domain Delivery and Support ke-5 yaitu Memastikan Keamanan Sistem.
5. Membuat Pertanyaan Wawancara, Pada tahap ini, kami membuat beberapa pertanyaan wawancara yang berkaitan dengan tiap-tiap sub bagian dari DS5.
6. Menggali dan Mengumpulkan Data Yang Dibutuhkan, Setelah membuat pertanyaan-pertanyaan wawancara, kami melakukan wawancara langsung kepada narasumber untuk menggali data yang dibutuhkan, kemudian mengumpulkan hasil jawaban wawancara.
7. Mengolah Data Yang Sudah Diperoleh, Data yang sudah diperoleh dari hasil wawancara, diolah untuk menjawab rumusan masalah yang ada.
8. Membuat Kesimpulan dan Saran, Pada tahap ini kami membuat kesimpulan berdasarkan hasil penelitian. Saran disajikan pula untuk perbaikan perusahaan di masa yang akan datang.
9. Membuat Laporan, Ditahap terakhir peneliti menuangkan seluruh hasil penelitian dalam berupa laporan ilmiah.

**Objek Penelitian**

PT MNC Sekuritas (MNC Sekuritas) sepenuhnya (99,9%) dimiliki oleh PT MNC Investama Tbk, melalui anak perusahaannya PT MNC Kapital Indonesia, Tbk, yang merupakan salah satu perusahaan investasi di bidang jasa keuangan yang terintegrasi dan terbesar di Indonesia.

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

Didirikan pada bulan November 1989 di Surabaya, MNC Sekuritas yang awalnya dikenal sebagai PT. Bhakti Investama memulai sepak terjangnya di bidang perdagangan efek, sekaligus menjadi cikal bakal MNC Group. Seiring perjalanan waktu, MNC Sekuritas terus berkembang menjadi salah satu perusahaan sekuritas lokal yang menyediakan jasa pasar modal secara lengkap. Saat ini MNC Sekuritas memiliki 3 divisi usaha. Divisi Equity menyediakan layanan perantara perdagangan saham, bagi nasabah ritel, institusi, maupun high networth. Divisi Online Trading telah menyediakan platform online trading MNC Trade New yang dapat diakses dengan mudah melalui berbagai perangkat, dengan sistem operasi Android maupun IOS. Divisi Fixed Income melayani transaksi perdagangan Surat Utang Negara, seperti Obligasi Negara Ritel, Saving Bonds Ritel (SBR), Sukuk Negara Ritel (SUKRI), dan obligasi korporasi. Divisi Investment Banking membantu klien dalam aktivitas Corporate Finance, seperti penjaminan emisi efek, financial advisory mencakup restrukturisasi, penggabungan usaha & akusisi, originasi dan sindikasi, serta private placement. Didukung oleh tim riset yang berkompeten dan professional, MNC Sekuritas secara konsisten memberikan layanan riset dan analisa pasar kepada nasabah untuk membantu meraih keuntungan optimal dan meminimalisasi resiko investasi.

MNC Sekuritas berhasil masuk dalam ranking 3 besar perusahaan sekuritas swasta lokal yang tercatat di Bursa Efek Indonesia based on value per Desember 2016. YTD Desember 2016, MNC Sekuritas juga mencatatkan pertumbuhan market sharenya sebesar 62 % dan pertumbuhan trading value sebesar 112,5 % secara YoY dari tahun 2015. Secara peringkat, MNC Sekuritas mencatatkan kenaikan dari peringkat 22 per Desember 2015 menjadi peringkat 14 per Desember 2016. Melalui berbagai inovasi dan peningkatan layanan bagi nasabah, MNC Sekuritas berkomitmen untuk terus menjadi perusahaan sekuritas terbaik dan terpercaya di Indonesia.

## HASIL DAN PEMBAHASAN

Hasil Analisis data mencakup tentang penerapan dan pengukuran kinerja tingkat kematangan terhadap keamanan sistem teknologi informasi di PT MNC Sekuritas. Data yang didapat dari hasil wawancara diolah sesuai metode COBIT 4.1. untuk mengetahui tingkat kematangan saat ini dan mengetahui tingkat kematangan yang diharapkan kedepan sehingga akan diketahui gap diantara tingkat kematangan saat ini dengan tingkat kematangan yang diharapkan. Berdasarkan hasil pengurukuran tersebut akan menghasilkan hasil audit yang dapat memberikan saran dan rekomendasi untuk PT MNC Sekuritas.

### Hasil Audit

DS5 Memastikan keamanan sistem. Hasil Perhitungan dari domain DS5 adalah seperti ditampilkan pada tabel berikut:

Tabel 1. Hasil Audit DS5

| Domain | Keterangan | Hasil |
|---|---|---|
| DS5.1 | Manajemen Keamanan TI (Managementof IT Security) | 3 |
| DS5.2 | Rencana Keamanan TI (IT Security Plan) | 3 |
| DS5.3 | Manajemen Identitas (Identity Management) | 4 |
| DS5.4 | Manajemen Akun Pengguna (User Account Management) | 3 |
| DS5.5 | Uji Coba Keamanan, Penjagaan dan Pemantauan (Security Testing, Surveillance and monitoring) | 3 |
| DS5.6 | Definisi Insiden Keamanan (Security Incident Definition) | 0 |
| DS5.7 | Proteksi Teknologi Keamanan (Protection of Security Technology) | 4 |
| DS5.8 | Manajemen Kunci | 0 |

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

| | | |
|---|---|---|
| | Kriptografi (Cryptographic Key Management) | |
| DS5.9 | Pencegahan Software Berbahaya, Deteksi dan Perbaikan (Malicious Software Prevention, Detection and Correction) | 4 |
| DS5.10 | Keamanan Jaringan (Network Security) | 4 |
| DS5.11 | Pertukaran Data Sensitif (Exchange of Sensitive Data) | 4 |
| Rata-rata | | 3 |

Penjelasan pemberian nilai masing-masing sub bagian dari DS5:

DS5.1: Diberikan nilai maturity level 3 yaitu Defined Level karena PT MNC Sekuritas sudah memiliki kerangka manajemen sistem keamanan yang jelas. Sistem keamanan sudah terstandarisasi. Salah satu buktinya adalah akses terbatas (limited access) bagi semua karyawan untuk masuk kedalam gedung, setiap lantai, ruang kerja dan ruang Data Center (khusus IT saja) di PT MNC Sekuritas.

DS5.2: Diberikan nilai maturity level 3 yaitu Defined Level karena PT MNC Sekuritas sudah mengkomunikasikan rencana keamanan TI mereka ke seluruh pemegang kepentingan dengan cara mengirimkan email ke semua karyawan.

DS5.3: Diberikan nilai maturity level 4 yaitu Managed Level karena Identifikasi pengguna, otentikasi dan otorisasi sudah dibakukan di PT MNC Sekuritas. Setiap user sudah teridentifikasi dengan baik serta pembatasan hak akses yang sudah ditetapkan dengan baik. Hal ini terbukti dengan adanya access card dan finger print bagi semua karyawan sebelum user masuk ke dalam ruang kerja. User ID dan Password yang unik untuk login ke setiap PC user di PT MNC Sekuritas.

DS5.4: Diberikan nilai maturity level 3 yaitu Defined Level karena hak-hak user yang berkaitan dengan rangkaian prosedur manajemen akun pengguna di PT MNC Sekuritas sudah memiliki prosedur yang baik. Terdapat Super Admin level, Admin level dan User level secara hirarki user account di PT MNC Sekuritas.

DS5.5: Diberikan nilai maturity level 3 yaitu Defined Level karena PT MNC Sekuritas sudah memiliki prosedur yang baik dalam pengujian, penjagaan dan pemantauan keamanan TI. Salah satu buktinya adalah adanya monitoring software dalam melakukan pengujian, penjagaan dan pemantauan. Alert dikirim dalam bentuk email bila terjadi masalah di PT MNC Sekuritas.

DS5.6: Diberikan nilai maturity level 0 yaitu Non-existent karena belum adanya kesadaran, pendefinisikan secara jelas dan pengkomunikasian karakteristik dari insiden keamanan yang potential terjadi sehingga dapat diklasifikasikan dan diperlakukan dengan baik oleh peristiwa dan proses manajemen masalah di PT MNC Sekuritas.

DS5.7: Diberikan nilai maturity level 4 yaitu Managed Level karena tanggung jawab untuk keamanan IT sudah ditugaskan, dikelola dan dilaksanakan dengan jelas di PT MNC Sekuritas. Proses standar dalam proteksi teknologi keamanan mengarah ke perbaikan tingkat keamanan. Hal ini terbukti dengan penggunaan secure tunneling, melakukan update patches secara online terhadap perangkat keamaan IT setiap hari di PT MNC Sekuritas.

DS5.8: Diberikan nilai maturity level 0 yaitu Non-existent karena belum adanya prosedur pengamanan data di PT MNC Sekuritas dengan cara disandikan untuk mencegah kebocoran rahasia ketika seseorang telah mencuri data penting perusahaan.

DS5.9: Diberikan nilai maturity level 4 yaitu Managed Level karena prosedur pencegahan software berbahaya, deteksi dan perbaikan di PT MNC Sekuritas sudah dilaksanakan dengan baik. Hal ini terbukti dengan penggunaan antivirus resmi dan berbayar, melakukan update antivirus setiap hari pada server dan PC user, tidak memberikan akses kepada user untuk

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

melakukan instalasi software, menutup akses CD ROM dan USB flashdisk di PT MNC Sekuritas.

DS5.10: Diberikan nilai maturity level 4 yaitu Managed Level karena Kebijakan dan prosedur keamanan jaringan di PT MNC Sekuritas sudah dilengkapi dengan ketentuan yang sudah ditetapkan dengan baik. Hal ini terbukti dengan:

1. Prosedur secara teknik: Melakukan pembatasan akses bagi setiap user dan departemen, memasukkan white list terhadap port atau software yang diperbolehkan untuk diakses dan dipergunakan.
2. Ketentuan secara prosedur: Meminta user mengisi form dan ditandatangani oleh atasan dan disetujui oleh Direktur.

DS5.11: Diberikan nilai maturity level 4 yaitu Managed Level karena PT MNC Sekuritas sudah menggunakan syarat dan prosedur yang diatur dalam ketentuan yang dikeluarkan oleh instansi pemerintah, misalkan OJK, Bapepam.

Pada pengukuran Marturity level ini digunakan pengambilan data melalui wawancara. Narasumber yang dilibatkan untuk wawancara adalah pada Departemen IT yang kesehariannya mengoprasikan secara langsung dan mengetahui masalah yang berkaitan dengan proses terpilih. Hasil perhitungan mendapati rata-rata nilai sistem keamanan teknologi informasi PT MNC Sekuritas sebesar 3. Dari nilai ini dapat tarik kesimpulan bahwa sistem keamanan teknologi informasi dilakukan secara Defined Process artinya adanya kesadaran keamanan dan prosedur keamanan sudah distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Kemudian diamanatkan bahwa proses-proses tersebut harus diikuti. Namun penyimpangan tidak mungkin dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang berjalan.

## KESIMPULAN DAN SARAN

### Kesimpulan

Berdasarkan uraian yang telah di jelaskan pada bab sebelumnya, dapat disimpulkan bahwa tingkat kematangan (maturity level) pengelolaan proses untuk memastikan keamanan sistem yang ada di PT MNC Sekuritas pada domain DS5 Cobit 4.1 berada di level 3 yang termasuk dalam skala Defined Process yaitu Kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan pegawai untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Kepedulian mengenai sistem keamanan dinilai sudah baik dan komunikasi berlangsung secara konsisten dan terdokumentasi.

### Saran

Dalam proses penelitian ini ada beberapa yang dapat ditangkat lagi, antara lain:

5. Melakukan proses audit keamanan teknikal seperti pengecekan kriptografi.
6. Melakukan proses audit keamanan teknikal untuk bagian jaringan.

## DAFTAR PUSTAKA

Andry, J.F. (2016). Performance Measurement of Information Technology Governance: A Case Study. Jurnal Sistem Informasi (Journal of Information Systems). 2/12, 56-62.

Andry, J.F., Suroso., J.S., Bernanda, D.Y., Improving Quality of SMEs Information System Solution with ISO 9126, Journal of Theoretical and Applied Information Technology, 96(14) (2018), 4610-4620.

Andry, J.F., Agung, H., Erlyana, Y., Management Information System for Order Fulfillment: A Case Study, Proceeding of 9th International Seminar on Industrial Engineering and Management, (2016).

Applegate LM, Austin RD & McFarlan FW. Corporate information strategy

*Journal of Business and Audit Information Systems*
*Vol. 1 (No. 2): no 12 – no 20. Th. 2018*
*p-ISSN 2615-6431*
*e-ISSN 2620-7907*

and management: text and cases. 6th edn. Boston, MA: McGraw-Hill; 2003

IT Governance Institute, COBIT 4.1 Framework, Control Objective, Management Guidelines, Maturity Models, Rolling Meadows, IL 60008 USA: ITGI, 2007.

ISACA. (2007). *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*. Information System Audit and Control Association.

Mokodompit, M.P., Nurlaela. Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000. Jurnal Sistem Informasi Bisnis, 02(2016)

Reddy, G.S., Srinivasu, R., Rikkula, S.R., Rao, V.S., Management Information System to Help Managers for Providing Decision Making in an Organization, International Journal of Reviews in Computing, (2009), 1-6.

Sarno, R. & Iffano, I., 2009. Sistem Manajemen Keamanan Informasi berbasis ISO 27001. ITS Press. Surabaya