Jurnal Accounting Information System
AIMS
Jurnal Accounting Information System (AIMS)
Volume 6 No. 1 | Maret 2023 : 75-88
DOI: 10.32627
https://jurnal.masoemuniversity.ac.id/index.php/aims
p-ISSN: 2615-7381
e-ISSN: 2621-7279

# Audit Keamanan Sistem Informasi Menggunakan Cobit 5 di PT. Paramita Surya Makmur Plastika

**Titan Parama Yoga[1], R. Yadi Rakhman Alamsyah[2], Silca Silkillah Adwa[3]**
[1,3]Sistem Informasi, Universitas Informatika dan Bisnis Indonesia, Indonesia
[2]Informatika, Universitas Informatika dan Bisnis Indonesia, Indonesia
titanparamayoga@gmail.com

**Info Artikel**
***Sejarah artikel :***
Diterima Februari 2023
Direvisi Maret 2023
Disetujui Maret 2023
Diterbitkan Maret 2023

***ABSTRACT***
*One of the main problems for a company is information system security. High security is needed to maintain the confidentiality and misuse of information in the organization. To improve the security of business operations and the quality of information technology resources, it is necessary to evaluate to optimize the security of existing information technology assets. The purpose of this research is to carry out an information system security audit at PT. Paramita Surya Makmur Plastika using COBIT 5 and documenting the information system audit findings of PT. Paramita Surya Makmur Plastika to produce an audit report. Based on the results of research that has been carried out through interviews and questionnaires using COBIT 5 and using the APO13 and DSS05 sub domains, the results show that the existing capability is at level 1 while the expected capability level is at level 3 andt the capability gap is 2.*

***Keywords*** **:** *Audit; Security; Information System; COBIT 5.*

**ABSTRAK**
Salah satu masalah utama bagi sebuah perusahaan yaitu keamanan sistem informasi. Keamanan yang tinggi diperlukan untuk menjaga kerahasiaan dan penyalahgunaan informasi dalam organisasi. Untuk meningkatkan keamanan operasi bisnis dan kualitas sumber daya teknologi informasi, perlu adanya evaluasi untuk mengoptimalkan keamanan aset teknologi informasi yang ada. Tujuan dari penelitian ini yaitu, melaksanakan audit keamanan sistem informasi di PT. Paramita Surya Makmur Plastika menggunakan framework COBIT 5 dan melakukan pendokumentasian temuan audit sistem informasi PT. Paramita Surya Makmur Plastika untuk dibuatkan laporan hasil audit. Berdasarkan hasil dari penelitian yang telah dilakukan melalui wawancara dan kuisioner dengan menggunakan *framework* COBIT 5 dan menggunakan sub domain APO13 dan DSS05 didapatkan hasil bahwa *Capability Existing* berada pada level 1 sedangkan *Capability Level* yang diharapkan adalah level 3 sehingga *Capability Gap* yaitu 2.

**Kata Kunci :** Audit; Keamanan; Sistem Informasi; COBIT 5.

## PENDAHULUAN

Dijaman yang sudah canggih ini, teknologi informasi mempunyai peranan penting dalam perkembangan bisnis suatu organisasi atau perusahaan. Hal itu menyebabkan suatu informasi yang dulu sulit untuk diperoleh , kini bisa diperoleh dengan mudah dan optimal. Konsumen yang terlayani pun akan merasa puas dan menjadi konsumen setia dari organisasi tersebut.

Salah satu masalah utama bagi sebuah organisasi atau perusahaan yaitu keamanan sistem informasi. Contohnya, seperti belum pernah dilakukannya

p-ISSN: 2615-7381
e-ISSN: 2621-7279

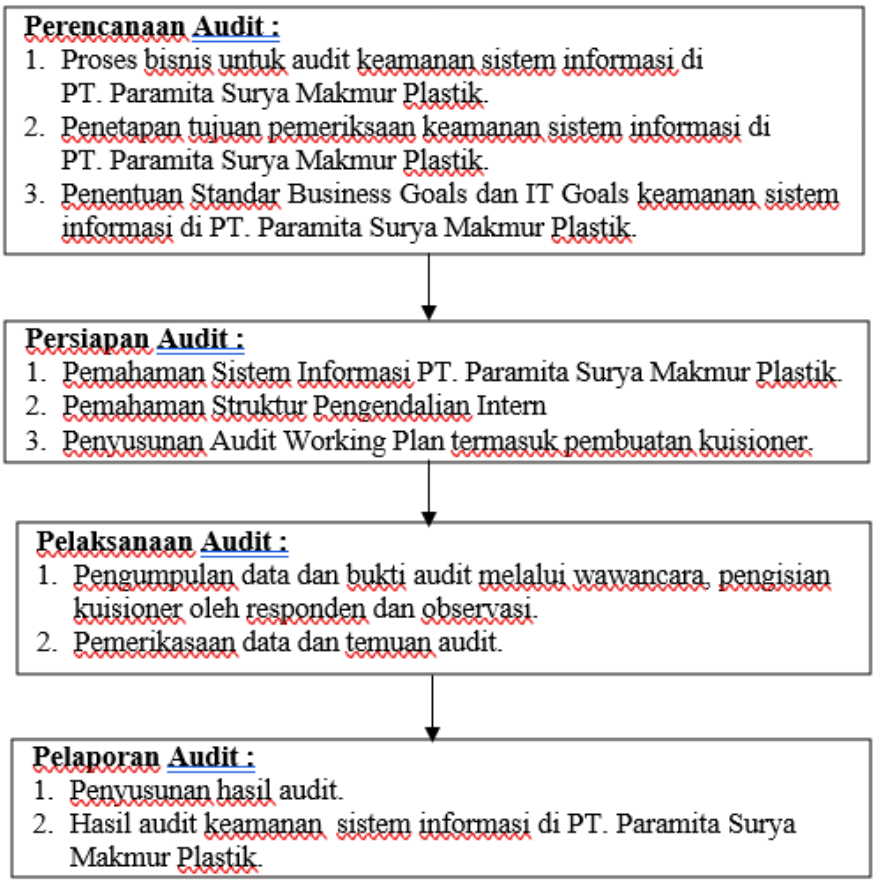
evaluasi tingkat kematangan terhadap keamanan sistem, kurangnya pendokumentasian laporan, pedoman dan SOP (*Standart Operasional System*). Untuk memberikan peningkatan keamanan sistem informasi yang sudah ada, alangkah baiknya dilakukan evaluasi tingkat kematangan keamanan sistem informasi agar menjamin kelangsungan proses bisnis yang ada. (Aritonang, Udayanti, & Iksan, 2018)

*Framework* yang berisi semua informasi yang dibutuhkan organisasi untuk mengelolah sistem informasi yaitu *Control objectivre for Information and Related Technology* (COBIT). COBIT memberikan praktek yang baik diseluruh domain dan kerangka proses dalam struktur kelola logis untuk membantu mengoptimalkan kemampuan teknologi informasi (TI) dalam investasi dan memastikan bahwa teknologi informasi (TI) berhasil dalam memberikan kebutuhan bisnis. (Matin, Arini, & Warhani, 2017).

Keamanan yang tinggi diperlukan untuk menjaga kerahasiaan dan penyalahgunaan informasi dalam organisasi. Untuk meningkatkan keamanan operasi bisnis dan kualitas sumber daya teknologi informasi, perlu adanya evaluasi untuk

## METODE

Metodologi penelitian yang akan diterapkan pada penelitian ini terdapat empat tahapan yaitu Perencanaan Audit, Persiapan Audit, Pelaksanaan Audit dan Pelaporan Audit.




**Gambar 1. Tahapan Audit Sistem Informasi**

p-ISSN: 2615-7381
e-ISSN: 2621-7279

Pada tahap perencanaan, penetapan ruang lingkup termasuk penentuan *Business Goals* dan *IT Goals* dari keamanan sistem informasi di PT. Paramita Surya Makmur Plastik. Hal ini didasari dari hasil wawancara dengan bagian General Manager dimana memiliki kewenangan mengatur sistem informasi di PT. Paramita Surya Makmur Plastik dengan harapan bahwa *Business Goals* dan *IT Goals* sesuai dengan tujuan dari keamanan sistem informasi agar pada proses audit didapat hasil yang objektif dan terarah.

Tahap perencanaan selesai mendapatkan *Business Goals*, *IT Goals* dan *IT Process* dari sistem informasi, maka tahap selanjutnya adalah tahap persiapan audit dimana pada tahapan ini semua pernyataan pada tahapan perencanaan akan dicocokkan dengan proses bisnis yang telah dipetakan di PT. Paramita Surya Makmur Plastik sesuai dengan apa yang telah dilakukan di tahapan perencanaan secara objektif.

Tahap pelaksanaan audit adalah tahapan dimana terdapat tiga cara pengumpulan materi untuk proses perhitungan ketaatan dan uji kematangan, diantaranya yaitu:

1. Wawancara
   Wawancara dilakukan dengan Bu Sasa selaku manager pada PT. Paramita Surya Makmur Plastika. Kegiatan ini berguna untuk memperoleh data-data yang diperlukan dalam analisis terhadap proses bisnis yang saat ini berjalan di PT. Paramita Surya Makmur Plastika.
2. Kuisioner
   Standar COBIT 5 digunakan dalam penyusunan Kuesioner/Angket dimana isinya terdapat beberapa domain atau klausul. Setiap klausul terdiri dari beberapa pertanyaan yang harus dijawab oleh responden di PT. Paramita Surya Makmur Plastik dengan cara memilih jawaban "Y" atau "N" sesuai dengan kesesuaian dengan apa yang dirasakan benar oleh responden.
   Kuisioner akan dibuat berdasarkan COBIT 5 proses APO13 dan DSS05, yang terdiri dari kuisioner sebagai berikut:
   a. APO13.1 : Membangun dan memelihara Sistem Manajemen Keamanan Informasi.
   b. APO13.2 :Mendefinisikan dan mengelola rencana penanganan keamanan informasi.
   c. APO13.3 : Memantau dan meninjau Sistem Manajemen Keamanan Informasi.
   d. DSS05.01 : Melindungi terhadap Malware dan mengelola keamanan jaringan dan konektivitas.
   e. DSS05.02 : Mengelola keamanan endpoint.
   f. DSS05.03 : Mengelola identitas pengguna dan akses logis.
   g. DSS05.04 : Mengelola kases fisik ke aset TI.
   h. DSS05.05 : Mengelola dokumen sensitif dan perangkat output.

   Kuisioner ini merupakan alat untuk membantu mengumpulkan data berdasarkan domain APO13 dan DSS05 dalam COBIT 5 yang diteliti.
3. Observasi
   Tahapan ini dilakukan untuk mendapatkan kesesuaian hasil kuesioner dengan keadaan sistem sehingga temuan dan rekomendasi yang dihasilkan

p-ISSN: 2615-7381
e-ISSN: 2621-7279

menjadi lebih maksimal. Observasi pada PT. Paramita Surya Makmur Plastika dilakukan dengan cara pengumpulan data dengan melihat langsung proses aplikasi perusahaan PT. Paramita Surya Makmur Plastika. Hasil dari pengamatan tersebut adalah kegiatan operasional logistic di PT. Paramita Surya Makmur Plastika yang sudah berjalan dengan baik. Namun, saat ini belum ada tata kelola keamanan sistem informasi yang menjadi masalah di PT. Paramita Surya Makmur Plastika.

## HASIL DAN PEMBAHASAN

### Penilaian data dan temuan audit untuk *Process Number* APO13

*Proses Number* APO13 memiliki turunan untuk penetapan hasil sebagai berikut:

**Tabel 1. *Outcome* dari *Process Number* APO13**

| *Outcome* | *Description* |
|---|---|
| APO13.01 | Sebuah sistem di tempatkan pada tempat yang dianggap efektif untuk menangani persyaratan keamanan informasi perusahaan. |
| APO13.02 | Sebuah rencana keamanan telah dibentuk, diterima dan dikomunikasikan di seluruh perusahaan. |
| APO13.03 | Solusi keamanan informasi diimplementasikan dan dioperasikan secara konsisten di seluruh perusahaan. |

Total dari prosentase *achievement/outcome* menentukan nilai dari *Total Achievement PA 1.1* dan *Rating by Criteria* untuk APO13, namun prosentase *achievement/outcome* masing-masing *outcome* ditentukan berdasarkan prosentase *achievement/component*. Komponen dari masing-masing *outcome* yaitu sebagai berikut.

**Tabel 2. Komponen dari masing-masing outcome pada *Process Number* APO 13**

| *Outcome* | *Component* | *Number* | *Description* |
|---|---|---|---|
| APO13.01 | *Work Product Output* | APO13-WP1 | Kebijakan SMKI |
| | | APO13-WP2 | Pernyataan lingkup SMKI |
| | | APO13-WP5 | Laporan audit SMKI |
| | | APO13-WP6 | Rekomendasi untuk meningkatkan SMKI |
| | *Base Practice + Work Product Input* | APO13-BP1 | Membangun dan memelihara SMKI |
| | | APO13-BP3 | Memantau dan meninjau SMKI |
| APO13.02 | *Work Product Output* | APO13-WP3 | Rencana perlakuan resiko keamanan informasi |
| | | APO13-WP4 | Kasus bisnis keamanan informasi |
| | ***Base Practice + Work Product Input*** | **APO13-BP2** | Mendefinisikan dan mengelola rencana perlakuan resiko |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| *Outcome* | *Component* | *Number* | *Description* |
|---|---|---|---|
| APO13.03 | *Work Product Output* | APO13-WP5 | Laporan audit SMKI |
| | | APO13-WP6 | Rekomendasi untuk meningkatkan SMKI |
| | *Base Practice* + *Work Product Input* | APO13-BP3 | Memantau dan meninjau SMKI |

Proses *component* diperoleh dari total semua jawaban "Y" dibagi dengan total jumlah pertanyaan dari setiap *component*, seperti tabel berikut.

**Tabel 3. Tabulasi Penilaian Audit Terhadap *Process Number* APO13**

| *Number* | *Description* | *Achievement / Component* | *Achievement / Component* | *Outcome* | *Total Achievement PA 1.1 (APO13)* |
|---|---|---|---|---|---|
| APO13-WP1 | Kebijakan SMKI | **100%** | **88%** $\frac{(100\%+83\%)}{2}$ | APO13-01 | **83%** $\frac{(88\%+93\%+70\%)}{3}$ |
| APO13-WP2 | Pernyataan lingkup SMKI | | | | |
| APO13-WP5 | Laporan audit SMKI | | | | |
| APO13-WP6 | Rekomendasi untuk meningkatkan SMKI | | | | |
| APO13-BP1 | Membangun dan memelihara SMKI | **75%** | | | |
| APO13-BP3 | Memantau dan meninjau SMKI | | | | |
| APO13-WP3 | Rencana perlakuan resiko keamanan informasi | **100%** | **93%** $\frac{(100\%+86\%)}{2}$ | APO13-02 | |
| APO13-WP4 | Kasus bisnis keamanan informasi | | | | |
| APO13-BP2 | Mendefinisikan dan mengelola rencana perlakuan resiko | **86%** | | | |
| APO13-WP5 | Laporan audit SMKI | **100%** | **70%** $\frac{(100\%+40\%)}{2}$ | APO13-03 | |
| APO13-WP6 | Rekomendasi untuk meningkatkan SMKI | | | | |
| APO13-BP3 | Memantau dan meninjau SMKI | 40% | | | |

**Penilaian data dan temuan audit untuk *Process Number* DSS05**

*Process Number* DSS05 memiliki turunan seperti tabel berikut.

p-ISSN: 2615-7381
e-ISSN: 2621-7279

**Tabel 4. *Outcome* dari *Process Number* DSS05**

| *Outcome* | *Description* |
|---|---|
| DSS05-01 | Jaringan dan keamanan komunikasi memenuhi kebutuhan bisnis |
| DSS05-02 | Informasi diproses, disimpan, dan dikirimkan oleh perangkat *endpoint* yang dilindungi. |
| DSS05-03 | Semua pengguna unik diidentifikasi dan memiliki hak akses sesuai dengan peran bisnis mereka. |
| DSS05-04 | Tindakan fisik telah dilaksanakan untuk melindungi informasi dari akses yang tidak sah, kerusakan dan gangguan ketika sedang diproses, disimpan atau dikirimkan. |
| DSS05-05 | Informasi elektronik benar-benar dijamin bila disimpan, ditransmisikan atau dihancurkan. |

Total dari prosentase *achievement/outcome* menentukan nilai dari *Total Achievement PA 1.1* dan *Rating by Criteria* untuk DSS05, namun prosentase *achievement/outcome* masing-masing *outcome* ditentukan berdasarkan prosentase *achievement/component*. Komponen dari masing-masing outcome yaitu sebagai berikut.

**Tabel 5. Komponen dari masing-masing outcome pada Process Number DSS05**

| *Outcome* | *Component* | *Number* | *Description* |
|---|---|---|---|
| DSS05-01 | *Work Product Output* | DSS05-WP1 | Kebijakan pencegahan perangkat lunak berbahaya |
| | | DSS05-WP2 | Evaluasi potensi ancaman |
| | | DSS05-WP10 | Karakteristik insiden keamanan |
| | | DSS05-WP11 | Log peristiwa keamanan |
| | | DSS05-WP12 | Tiket insiden keamanan |
| | | DSS05-WP13 | Inventarisasi dokumen sensitif dan perangkat |
| | | DSS05-WP14 | Hak akses |
| | *Base Practice + Work Product Input* | DSS05-BP1 | Melindungi malware |
| | | DSS05-BP2 | Mengelola keamanan jaringan dan konektivitas |
| | | DSS05-BP7 | Memonitor infrastruktur untuk acara yang berhubungan dengan keamanan |
| DSS05-02 | *Work Product Output* | DSS05-WP3 | Kebijakan keamanan konektivitas |
| | | DSS05-WP4 | Hasil tes penetrasi |
| | | DSS05-WP5 | Kebijakan keamanan untuk perangkat endpoint |
| | *Base Practice + Work Product Input* | DSS05-BP1 | Melindungi terhadap *malware* |
| | | DSS05-BP3 | Mengelola keamanan endpint |
| DSS05-03 | *Work Product Output* | DSS05-WP6 | Hak akses pengguna disetujui |
| | | DSS05-WP7 | Hasil tinjauan dari akun pengguna dan hak istimewa |
| | *Base Practice + Work Product Input* | DSS05-BP4 | Mengelola identitas pengguna dan akses logis |

Proses *component* diperoleh dari total semua jawaban "Y" dibagi dengan total jumlah pertanyaan dari setiap *component*, seperti tabel berikut.

p-ISSN: 2615-7381
e-ISSN: 2621-7279

**Tabel 6. Tabulasi Penilaian Audit Terhadap *Process Number* DSS05**

| *Number* | *Description* | *Achievement / Component* | *Achievement / Outcome* | *Outcome* | *Total Achievement PA 1.1 (DSS05)* |
|---|---|---|---|---|---|
| DSS05-WP1 | Kebijakan pencegahan perangkat lunak berbahaya | **43%** | **56%** $\frac{(43\%+70\%)}{2}$ | DSS05-01 | **68%** $\frac{(56\%+47\%+100\%+86\%+80\%)}{2}$ |
| DSS05-WP2 | Evaluasi potensi ancaman | | | | |
| DSS05-WP10 | Karakteristik insiden keamanan | | | | |
| DSS05-WP11 | Log peristiwa keamanan | | | | |
| DSS05-WP12 | Tiket insiden keamanan | | | | |
| DSS05-WP13 | Inventarisasi dokumen sensitif dan perangkat | | | | |
| DSS05-WP14 | Hak akses | | | | |
| DSS05-BP1 | Melindungi terhadap malware | **70%** | | | |
| DSS05-BP2 | Mengelola keamanan jaringan dan perangkat | | | | |
| DSS05-BP7 | Memonitor infrastruktur untuk acara yang berhubungan dengan keamanan | | | | |
| DSS05-WP3 | Kebijakan keamanan konektivitas | 33% | 47% $\frac{(33\%+60\%)}{2}$ | DSS05-02 | |
| DSS05-WP4 | Hasil tes penetrasi | | | | |
| DSS05-WP5 | Kebijakan keamanan untuk perangkat endpoint | | | | |
| DSS05-BP1 | Melindungi malware | 60% | | | |
| DSS05-BP3 | Mengelola keamanan endpoint | | | | |
| DSS05-WP6 | Hak akses pengguna disetujui | 100% | 100% $\frac{(100\%+100\%)}{2}$ | DSS05-03 | |
| DSS05-WP7 | Hasil tinjauan dari akun | | | | |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| | | | | |
|---|---|---|---|---|
| | pengguna dan hak istimewa | | | |
| DSS05-BP4 | Mengelola identitas pengguna dan akses logis | 100% | | |
| DSS05-WP8 | Menyetujui permintaan akses | 100% | 86% | DSS05-04 |
| DSS05-WP9 | Akses log | | (100%+71%) / 2 | |
| DSS05-BP5 | Mengelola akses fisik ke TI | 71% | | |
| DSS05-BP6 | Mengelola dokumen sensitif dan perangkat output | 80% | 80% | DSS05-05 |

Total achievement PA 1.1 dari masing-masing domain, dimasukkan kedalam format sebagai berikut.

**Tabel 8. Rating untuk Domain APO13**

| **Process Name** | **Level 1** | **Level 2** | | **Level 3** | | **Level 4** | | **Level** 5 | |
|---|---|---|---|---|---|---|---|---|---|
| **APO13** | **PA 1.1** | **PA 2.1** | **PA 2.2** | **PA 3.1** | **PA 3.2** | **PA 4.1** | **PA 4.2** | **PA 5.1** | **PA5.2** |
| **Rating by Criteria** | 83% | 58% | 50% | 55% | 38% | 42% | 65% | 70% | 67% |
| **Rating** | F | L | P | L | P | P | L | L | L |
| **Capability Level Achieved** | 1 | 1 | Stop! | Stop! | Stop! | Stop! | Stop! | Stop! | Stop! |

**Tabel 9. Rating untuk Domain DSS05**

| **Process Name** | **Level 1** | **Level 2** | | **Level 3** | | **Level 4** | | **Level** 5 | |
|---|---|---|---|---|---|---|---|---|---|
| **DSS05** | **PA 1.1** | **PA 2.1** | **PA 2.2** | **PA 3.1** | **PA 3.2** | **PA 4.1** | **PA 4.2** | **PA 5.1** | **PA5.2** |
| **Rating by Criteria** | 68% | 46% | 50% | 55% | 42% | 71% | 45% | 50% | 67 % |
| **Rating** | L | P | P | L | P | L | P | P | L |
| **Capability Level Achieved** | 1 | Stop! | Stop! | Stop! | Stop! | Stop! | Stop! | Stop! | Stop! |

Perolehan *rating by criteria* menjadi dasar penentuan rating yang diperoleh dari:

a. N (*Not Achieved* / Tidak Tercapai)
   Kategori ini terjadi apabila, *range* yang didapatkan dari *rating by criteria* berkisar antara 0%-15%.
b. P (*Partially Achieved* / Sebagian Tercapai)
   Katerogi ini terjadi apabila, *range* yang didapatkan dari *rating by criteria* berkisar antara 15%-50%.

p-ISSN: 2615-7381
e-ISSN: 2621-7279

c. L (*Large Achieved* / Sebagian Besar Tercapai)
   Kategori ini terjadi apabila, *range* yang didapatkan dari *rating by criteria* berkisar antara 50%-85%.
d. F (*Fully Achieved* / Sepenuhnya Tercapai)
   Kategori ini terjadi apabila, *range* yang didapatkan dari *rating by criteria* berkisar antara 85%-100%.

**Penilaian Hasil Existing**

Perolehan rating dari masing-masing domain diperoleh, tahap selanjutnya yaitu penilaian terhadap hasil *existing*, diantaranya:

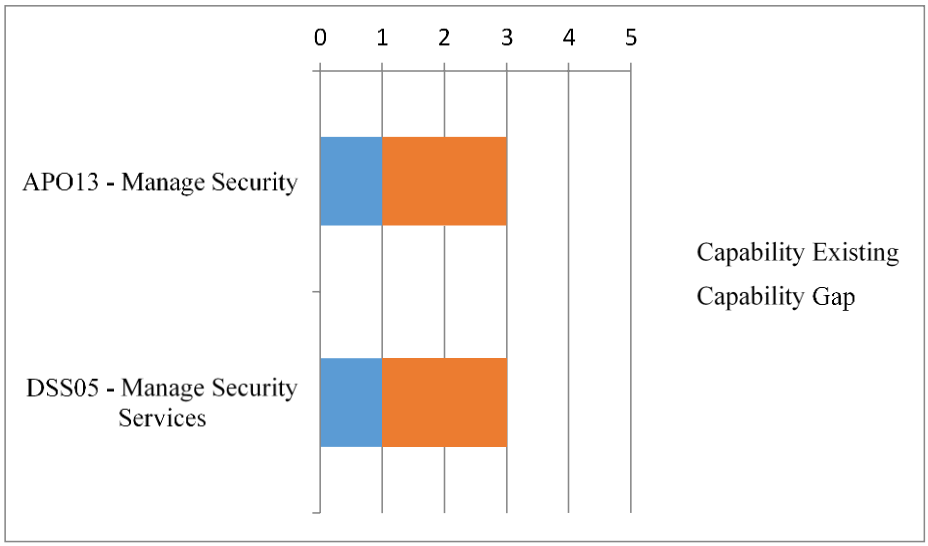
1. Kondisi *existing* APO13
   Hasil yang diperoleh dari kondisi *existing* APO13 diantaranya:
   a. Sistem manajemen keamanan informasi berjalan baik karena penentuan ruang lingkup lebih terperinci terutama untuk hal karakteristik perusahaan, organisasi, lokasi, aset, dan teknologi.
   b. Sistem manajemen keamanan informasi di PT. Paramita Surya Makmur Plastika telah sesuai dengan organisasi, aset dan teknologi.
   c. Sistem manajemen keamanan informasi di PT. Paramita Surya Makmur Plastika telah sejajar dengan keseluruhan manajemen keamanan.
   d. Adanya komunikasi antara manajemen terkait peran dan tanggung jawab manajemen terhadap keamanan informasi.
   e. Adanya masukkan untuk desain dan pengembangan manajemen.

2. Kondisi *existing* DSS05
   Hasil yang diperoleh dari kondisi *existing* DSS05 diantaranya:
   a. Bagian Sistem Informasi mengarahkan tentang kesadaran perangkat lunak yang berbahaya.
   b. Bagian Sistem Informasi menginstal dan mengaktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas.
   c. Bagian Sistem Informasi mendistribusikan semua perangkat lunak.
   d. Bagian Sistem Informasi menyaring lalu lintas data yang masuk seperti *email* dan *download* untuk melindungi informasi yang tidak diminta seperti *spyware, phising email* dan lain-lain.
   e. Bagian Sistem Informasi memastikan bahwa semua pengguna dan aktivitas mereka pada sistem IT dapat diidentifikasi.

**Gap**

Gap yaitu kesenjangan antara levet yang ingin dicapai dengan level *capability* yang telah dicapai. Dari hasil *existing* APO13 dan DSS05 maka diperoleh grafik seperti berikut.

p-ISSN: 2615-7381
e-ISSN: 2621-7279




**Gambar 1. Grafik *Capability Existing* dan *Capability Gap***

Grafik tersebut menunjukkan bahwa level yang diinginkan oleh perusahaan berada pada level 3, namum kenyataannya *level capability* sistem informasi PT.Paramita Surya Makmur Plastika berada pada level 1.

**Rekomendasi**

1. Rekomendasi APO13
   a. Melakukan pelatihan keamanan sistem informasi kepada para pengguna sistem informasi PT. Paramita Surya Mamkur Plastika.
   b. Bagian sistem informasi mendapatkan otorisasi dari manajemen untuk menerapkan, mengoperasikan dan bahkan mengubah Sistem Manajemen Keamanan Informasi.
   c. Melakukan ulasan dan pembahasan secara reguler yang membahas tentang kebijakan dan tujuan Sistem Manajemen Keamanan Informasi di PT.Paramita Surya Makmur Plastika.
   d. Melakukan internal audit Sistem Manajemen Keamanan Informasi pada interval yang direncanakan.
   e. Melakukan tinjauan manajemen Sistem Manajemen Keamanan Informasi secara teratur untuk memastikan bahwa lingkup tetap memadai dan perbaikan dalam proses Sistem Manajemen Keamanan Informasi dapat diidentifikasi.
2. Rekomendasi DSS05
   a. Meninjau dan mengevaluasi informasi tentang adanya ancaman baru
   b. Melakukan pelatihan berkala tentang bahayanya malware.
   c. Melakukan pengujian berkala untuk kecukupan sistem perlindungan.
   d. Mendefinisikan dan mengkomunikasikan sifat dan karakteristik insiden terkait keamanan potensial sehingga mereka dapat dengan mudah dikenali dan dampaknya dipahami untuk memungkinkan respon yang sepadan
   e. Mengidentifikasi semua kegiatan pengolahan informasi dengan peran fungsional, koordinasi dengan unit bisnis.
   f. Melakukan pelatihan berkala tentang kesadaran keamanan fisik

p-ISSN: 2615-7381
e-ISSN: 2621-7279

**Laporan Hasil Audit**

Berdasarkan hasil penelitian dari audit keamanan sistem informasi PT. Paramita Surya Makmur Plastika, *capability level* keamanan sistem informasi PT. Paramita Surya Makmur Plastika, yaitu:

**Tabel 10. Hasil Audit Keamanan Sistem Informasi PT. Paramita Surya Makmur Plastika**

| Domain | *Capability Level* | *Capability Existing* | Kondisi *existing* | Rekomendasi |
|---|---|---|---|---|
| **APO13** | 3 | 1 | a. Sistem manajemen keamanan informasi berjalan baik karena penentuan ruang lingkup lebih terperinci terutama untuk hal karakteristik perusahaan, organisasi, lokasi, aset, dan teknologi.<br>b. Sistem manajemen keamanan informasi di PT. Paramita Surya Makmur Plastika telah sesuai dengan organisasi, aset dan teknologi.<br>c. Sistem manajemen keamanan informasi di PT. Paramita Surya Makmur Plastika telah sejajar dengan keseluruhan manajemen keamanan.<br>d. Adanya komunikasi antara manajemen terkait peran dan tanggung jawab manajemen terhadap keamanan informasi.<br>e. Adanya masukkan untuk desain dan pengembangan manajemen. | a. Melakukan pelatihan keamanan sistem informasi kepada para pengguna sistem informasi PT. Paramita Surya Mamkur Plastika.<br>b. Bagian sistem informasi mendapatkan otorisasi dari manajemen untuk menerapkan, mengoperasikan dan bahkan mengubah Sistem Manajemen Keamanan Informasi.<br>c. Melakukan ulasan dan pembahasan secara reguler yang membahas tentang kebijakan dan tujuan Sistem Manajemen Keamanan Informasi di PT.Paramita Surya Makmur Plastika.<br>d. Melakukan internal audit Sistem Manajemen Keamanan Informasi pada interval yangdirencanakan.<br>e. Melakukan tinjauan manajemen Sistem Manajemen Keamanan Informasi secara teratur untuk memastikan bahwa lingkup tetap memadai dan perbaikan dalam proses Sistem Manajemen Keamanan Informasi dapat diidentifikasi. |

p-ISSN: 2615-7381
e-ISSN: 2621-7279

| Domain | *Capability Level* | *Capability Existing* | Kondisi *existing* | Rekomendasi |
|---|---|---|---|---|
| **DSS05** | 3 | 1 | a. Bagian Sistem Informasi mengarahkan tentang kesadaran perangkat lunak yangberbahaya.<br>b. Bagian Sistem Informasi menginstal dan mengaktifkan alat perlindungan terhadap perangkat lunak berbahaya di semua fasilitas.<br>c. Bagian Sistem<br>d. Bagian Sistem Informasi menyaring lalu lintas data yang masuk seperti *email* dan *download* untuk melindungi informasi yang tidak diminta seperti *spyware, phising email* dan lain-lain.<br>e. Bagian Sistem Informasi memastikan bahwa semua pengguna dan aktivitas mereka pada sistem IT dapat diidentifikasi. | a. Meninjau dan mengevaluasi informasi tentang adanya ancaman baru.<br>b. Melakukan pelatihan berkala tentang bahayanya *malware*.<br>c. Melakukan pengujian berkala untuk kecukupan sistem perlindungan.<br>d. Mendefinisikan dan mengkomunikasikan sifat dan karakteristik insiden terkait keamanan potensial sehingga mereka dapat dengan mudah dikenali dan dampaknya dipahami untuk memungkinkan respon yang sepadan.<br>e. Mengidentifikasi semua kegiatan pengolahan informasi dengan peran fungsional, koordinasi dengan unit bisnis.<br>f. Melakukan pelatihan berkala tentang kesadaran keamanan fisik. |

## PENUTUP

Berdasarkan hasil audit keamanan sistem informasi di PT. Paramita Surya Makmur Plastika didapatkan kesimpulan sebagai berikut: Hasil audit dan evaluasi dari sistem manajemen keamanan informasi pada sistem informasi PT. Paramita Surya Makmur Plastika yang didapatkan melalui kondisi *existing* domain APO13 dan DSS05 memperoleh level 1 pada *Capability Existing* dengan *Capability Level* yang diharapkan oleh perusahaan berada pada level 3. Oleh karena itu, *Capability Gap* pada kondisi tersebut yaitu 2 level. Serta Pencapaian *Capability Exisitng* pada APO13 dan DSS05 berada pada level 1.

p-ISSN: 2615-7381
e-ISSN: 2621-7279

Saran untuk penilaian terhadap sistem informasi PT. Paramita Surya Makmur Plastika kedepannya, lebih baik melakukan pembahasan keamanan sistem informasi dengan melibatkan semua domain yang ada pada COBIT 5 seperti domain EDM (*Evaluate, Direct and Monitor*) yang dapat mencapai tujuan perusahaan dengan mengevaluasi kebutuhan, kondisi dan pilihan pemangku kepentingan atau menggunakan domain BAI (*Build, Acquire and Implement*) yang dapat mencakup identifikasi persyaratan Teknologi Informasi. Selain itu, dapat menggunakan sub domain lain seperti DSS03 yang membahas *manage process* dan APO06 yang membahas *manage budget and costs*.

**DAFTAR PUSTAKA**

[1] Agus, I., & Verawati. (2019). Audit Tingkat Kematangan Sistem Informasi Uji Kompetensi Menggunakan COBIT 5 (Studi Kasus Amik DCC). TEKNIKA, 102-111.

[2] Aritonang, I. J., Udayanti, E. D., & Iksan, N. (2018). ITEJ (Information \ Technology Engineering Journals). Audit Keamanan Sistem Informasi Menggunakan Framework COBIT 5 (APO13).

[3] Bless, Y. C., Sasmita, G. M., & Cahyawan, A. A. (2014). Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus: FE UNUD). Merpati Vol.2, No.2.

[4] Ermana, F., Tanuwijaya, H., & Adrian Mastan, I. (2012). Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM. Jurnal Sistem Informasi dan Komputerisasi Akuntansi - Prodi SI – STIKOM Surabaya Vol.1, No.1.

[5] Gondodiyoto, S. (2007). Audit Sistem Informasi + Pendekatan CobIT. Mitra Wacana Media.

[6] Hutahaean, J. (2014). Konsep Sistem Informasi. Yogyakarta: Deepublish.

[7] ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. United States of America: IT Governance Institute.

[8] Kurniawan, K. (2020, April 19). 4 Pengertian Informasi Menurut Ahli. Retrieved Oktober 20, 2020 from Projasa Web: https://projasaweb.com/pengertian- informasi/#Sutanta_2011

[9] Kurniawan, T. A. (2020). Sistem Informasi Akuntansi Dengan Pendekatan Simulasi. Yogyakarta: Deepublish.

[10] Matin, I. M., Arini, & Warhani, L. K. (2017). JURNAL TEKNIK INFORMATIKA VOL.10 NO.2. ANALISIS KEAMANAN INFORMASI DATA CENTER, 119- 128.

[11] Octaviyanti, P., & Andry, J. F. (2018). Audit Sistem Enterprise Asset Management menggunakan Framework COBIT 5. IKRAITH_INFORMATIKA, 34-42.

[12] Pertama, P. P., & Ardiyasa, I. W. (2019). Audit Keamanan Sistem Informasi Perpustakaan STMIK STIKOM Bali Menggunakan Kerangka Kerja COBIT. JURNAL SISTEM DANINFORMATIKA, 77-86.

[13] Purba, A. D., Purnawan, I. K., & Pratama, I. P. (2018). Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. Merpati Vol. 3, 148-158.

p-ISSN: 2615-7381
e-ISSN: 2621-7279

[14] Sulaeman, F. S. (2015). Audit Sistem Informasi Framework Cobit 5. Media Jurnal Informatika Vol. 7, 37-42.

[15] Suryono, R. R., Darwis, D., & Gunawan, S. I. (2018). AUDIT TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 (STUDI KASUS: BALAI BESAR PERIKANAN BUDIDAYA LAUT LAMPUNG). TEKNOINFO, 16-22.

[16] Sutabri, T. (2012). Konsep Sistem Informasi. Yogyakarta: Andi.

[17] Turang, D. A., & Turang, M. C. (2020). Analisis Audit Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Pada Instansi X. Kumpulan jurnaL Ilmu Komputer (KLIK), 130-144.

[18] Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). Jurnal Sistem Informasi Bisnis, 47-54.

[19] Yoga, T. P. (2016). AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN ISO 27002:2013 DAN KERANGKA KERJA COBIT 5 PADA UNIVERSITAS INFORMATIKA DAN BISNIS INDONESIA.

[20] Yudana, M. (2017, Oktober 12). Audit Teknologi Sistem Informasi. Retrieved Oktober 20, 2020 from All About Indonesia: http://hutomoyudanesia.blogspot.com/2017/10/audit.html