# Evaluasi Kepatuhan *Logical* dan *Physical Security* Terhadap Kebijakan Pengamanan Data

**Khairunnisak Nur Isnaini[1], Wing Wahyu Winarno[2], Henderi[3]**
Univesitas AMIKOM Yogyakarta
Jl. Ring Road Utara Condong Catur, Depok, Sleman, Yogyakarta
Email :[1]khairunnisak.i@students.amikom.ac.id,
[2]wingwahyuwinarno@gmail.com,[3]henderiugm@gmail.com

***Abstract***

*IT assets in company should be protected to prevent damage, theft and breaches. This study is conducted to asses the employees's compliance to data security policy, specifically in logical security, password control management, and physical security in stmik xyz. The research used descriptive quantitative method and the data was collected by study documentation, interview and questionnaires which distributed to all employees based on raci chart table. The statistic data processing was done by validity and reliability test in order to ensure the consistency of its result, also to analyze the gap between current condition and future reference. The DSS5.4 (manage user identity and logical access) and the DSS5.5 (manage physcal access to IT assets) domain in the COBIT 5 are used as a tool for assessing employee compliance index. The results show that the level of employee compliance is generally at level 3(Established Process). It means that employees have implemented the policies, standards and operational procedures. The gap conditions are solved by giving the appropriate recommendations to relevant parties in order to the current policies can be improved in accordance with the results of the analysis and applicable standards.*

***Keywords:****Data Security Policy, Employee Compliance Level, COBIT 5, Gap Analysis, Recommendation*

***Abstraksi***

*Aset IT yang dimiliki oleh sebuah perusahaan atau instansi seharusnya dapat dijaga dengan baik agar terhindar dari kerusakan, pencurian, dan hal-hal yang merugikan lainnya. Penelitian ini dilakukan untuk mengukur tingkat kepatuhan karyawan terhadap kebijakan pengamanan data terutama pada aspek logical security, kontrol password, dan physical security di STMIK XYZ. Penelitian ini menggunakan metode kuantitatif deskriptif. Pengumpulan data dilakukan dengan cara studi dokumentasi, wawancara, pembagian kuisioner yang disebar kepada seluruh karyawan berdasarkan tabel RACI Chart. Selanjutnya penulis melakukan pengolahan data statistik berupa uji validitas dan realibilitas untuk menguji konsistensi kuisioner yang dibagikan serta melakukan analisa kesenjangan antara kondisi saat ini dan kondisi harapan. Domain DSS5.4 (manage user identity and logical access) dan DSS5.5(manage physcal access to IT assets) pada Famework COBIT 5 digunakan sebagai alat ukur menilai indeks tingkat kepatuhan karyawan. Hasil yang diperoleh menunjukkan bahwa tingkat kepatuhan karyawan secara umum berada pada level 3 (Established Process) yang berarti karyawan telah*

*menerapkan kebijakan, standar dan operasional prosedur. kondisi kesenjangan di atasi dengan pemberian rekomendasi yang tepat kepada pihak-pihak terkait agar kebijakan saat ini dapat diperbaiki atau ditambah sesuai dengan hasil analisis dan standar yang berlaku.*

***Kata Kunci:****Kebijakan Pengamanan Data, Tingkat Kepatuhan Karyawan, COBIT 5, Analisis Kesenjangan, Rekomendasi*

## 1. PENDAHULUAN

Perlindungan terhadap keamanan informasi dilakukan bertujuan mencegah terjadinya kerugian bagi kelangsungan hidup organisasi dan dilakukan oleh seluruh pihak-pihak yang terlibat dalam organisasi tersebut. Aspek-aspek keamaman tersebut antara lain kerahasiaan, integritas, dan ketersediaan. Strategi yang dapat dilakukan yaitu menerapkan aspek keamanan informasi karena aspek tersebut penting dalam usaha melindungi aset informasi dalam sebuah organisasi[1]. Adanya kontrol terhadap sejumlah kebijakan dan prosedur pada sebuah organisasi diharapkan dapat menjamin sasaran keamanan informasi yang dimaksud. Keamanan informasi yang baik dapat dicapai melalui penerapan upaya-upaya teknis (operasional) yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai [2].

STMIK X merupakan salah satu perguruan tinggi swasta berlokasi di Purwokerto Utara yang telah menerapkan berbagai macam teknologi informasi dalam menunjang aktivitasnya sehari-hari. Namun belum dapat dipastikan keseluruhan teknologi informasi yang digunakan maupun karyawan atau *staff* yang menggunakannya terhindar dari ancaman keamanan informasi. Berdasarkan 10 aspek keamanan informasi yang dijabarkan oleh [2] STMIK X masih berpotensi memiliki celah ancaman terhadap aspek-aspek keamanan keamanan informasi. Ancaman tersebut diakibatkan oleh beberapa insiden seperti terdapat ketidakjelasan akuntabilitas pemilik sistem yang ada seperti yang terjadi pada sistem yang digunakan oleh masing-masing program studi akibatnya terdapat kebocoran informasi karena kurang terkontrolnya pemakaian *device* untuk mengakses sistem tersebut meski pada jaringan yang sama. Ancaman lain pada aspek keamanan fisik dan lingkungan. Menurut [3] seharusnya sentra komputer yang dimiliki STMIK X dapat dikontrol dengan ketat agar tidak sembarang personel diperbolehkan masuk ke unit kerja tersebut.

Menurut [4]sistem komputer memiliki empat parameter keamanan yang sangat penting antara lain *physical security, system security, application security*, dan *data security*. *Physical security* merupakan perlindungan pertama yang langsung berhubungan dengan dunia luar. Sedangkan aspek setelahnya merupakan logical security yang membahas mengenai pengguna dapat masuk ke sistem, tingkat otoritas kepada masing-masing pengguna (sistem, program, dan data). *Logical security* menurut [3] penting untuk dilakukan karena bertujuan untuk melindungi data atau informasi dari perusakan atau penghancuran yang dilakukan baik secara sengaja maupun secara tidak sengaja dan menghindari serta mendeteksi perubahan terhadap informasi yang dilakukan oleh yang tidak berwenang.*Physical security* dilakukan agar organisasi dapat membuat langkah-langkah seperti meminimalkan risiko-risiko yang sewaktu-waktu dapat terjadi misalkan kebakaran, memiliki *physical security* yang memadai, dan memiliki program *recovery* yang memadai dan dapat dipertanggungjawabkan.

Kebijakan keamanan informasi sudah berjalan di STMIK X namun belum terdokumentasi dengan baik dan disebarluaskan ke semua pihak. Saat ini yang berjalan berupa Standar Operasional Prosedur penggunaan *hardware* yang ada di lingkungan kampus. Sedangkan kebijakan keamanan informasi bagian *software* yang dikendalikan bagian divisi teknologi informasi belum tertata dengan baik pada sisi pendokumentasian aturan-aturan yang melingkupinya. Hal tersebut dikarenakan Lembaga Penjaminan Mutu yang bertugas menjamin adanya kebijakan yang berjalan merupakan unit kerja yang baru berjalan sekitar satu tahun dan posisi kebijakan keamanan informasi secara menyeluruh masih berada pada tahap *planning*. Hal tersebut mengakibatkan karyawan cenderung mengabaikan dan tidak mematuhi kebijakan yang sudah berjalan sehingga berpotensi terkena ancaman kebocoran informasi seperti yang sudah terjadi sebelumnya.

Menurut [5] ketidakpatuhan karyawan terhadap kebijakan keamanan sistem informasi merupakan sebuah ancaman keamanan komputer yang serius. Penelitian sebelumnya oleh [6] membahas pembuatan program *Information Security Awareness* yang efektif berisi pemahaman program ISA dan kepatuhan perilaku terhadap keamanan informasi. Penelitian [7] membahas pentingnya evaluasi atas kelengkapan keamanan informasi pada perusahaan X. Penelitian [8] membahas tingkat kesadaran pegawai

terhadap keamanan informasi di Pemkot X berada pada level sedang sehingga perlu dilakukan perbaikan. Penelitian [9]membahas pengaruh informasi dan kesadaran tentang pentingnya keamanan informasi terhadap kepatuhan perilaku individudengan kebijakan keamanan informasi Penelitian lain[10]membahas evaluasi kelemahan-kelemahan pada sistem penyebab permasalahan keamanan informasi. Berdasarkan kelima penelitian yang telah dilakukan membuktikan bahwa keamanan informasi terhadap pengamanan data masih jarang diteliti oleh peneliti lain terutama pada aspek *logical* dan *physical security* dan hasil yang diperoleh peneliti sebelumnya, masih banyak karyawan atau pegawai yang kurang patuh atau sadar terhadap aspek keamanan informasi.

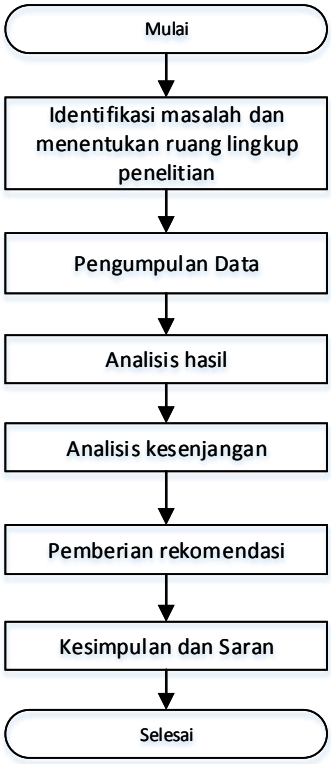
Kepatuhan karyawan pada prinsip dasar keamanan informasi saat ini dapat meningkat ketika terdapat *framework* yang dapat membantu dalam proses penilaian teknologi informasi untuk mencapai tujuan organisasi. Salah satu standar *framework* tersebut adalah COBIT (*Control Objectives for Information and Related Technologies*) 5. COBIT 5 telah menyediakan proses yang berkaitan dengan kebijakan keamanan informasi yaitu DSS5 (*Manage Security Services*) bertujuan untuk meminimalisir dampak bisnis yang ditimbulkan akibat insiden atau ancaman keamanan informasi. Penelitian [11] mengungkapkan bahwa COBIT 5 terbukti efektif untuk pengelolaan aturan dan tanggung jawab serta kebijakan. Selain itu, *COBIT 5 Framework* membantu perusahaan dalam pengelolaan perusahaan demi mencapai tujuannya.

Penelitian ini tentunya memiliki batasan masalah yaitu meneliti kepatuhan karyawan pada aspek *logical* dan *physical security* menggunakan COBIT 5 dengan *capability level* dan bertujuan untuk meningkatkan kepatuhan karyawan melalui rekomendasi sesuai dengan temuan-temuan hasil analisis.

## 2. METODE PENELITIAN

Metode penelitian yang digunakan adalah penelitian kuantitatif deskriptif. Menurut [12] penelitian dimulai dari mengidentifikasi masalah, mengumpulkan data, mengolah data, melakukan analisis untuk memperoleh tingkat kematangan kepatuhan karyawan dan kebijakan pengamanan data pada domain-domain yang sesuai, yang diperoleh pada kerangka kerja COBIT 5 hingga menyusun rekomendasi yang akan

diberikan kepada STMIK X. Alur penelitian tersebut terlihat pada gambar 1.




**Gambar 1.** Alur Penelitian

Keterangan

a. Identifikasi masalah dan menentukan ruang lingkup penelitian

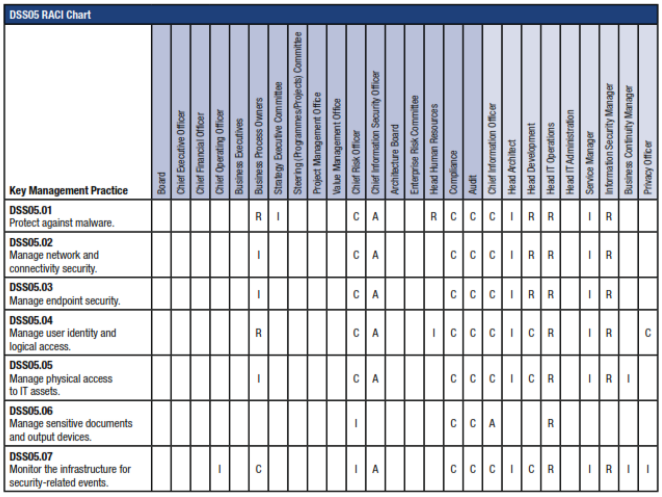
Identifikasi masalah yang terjadi di STMIK X dan dilanjutkan dengan menentukan ruang lingkup penelitiannya yaitu kepatuhan *logical* dan *physical security* terhadap kebijakan pengamanan data.

b. Pengumpulan data

Pengumpulan data yang dilakukan antara lain studi dokumentasi, wawancara, dan kuisioner. Studi dokumentasi [13]dilakukan dengan mengumpulkan dokumen pendukung penelitian yang diperoleh dari subyek penelitian. Wawancara dilaksanakan dengan mengadakan tanya jawab secara langsung kepada *staff IT* dan karyawan yang berkaitan dengan kebijakan pengamanan data. Tahapan pengumpulan data selanjutnya yaitu membagi kuisioner menggunakan skala likert seperti yang digunakan pada penelitian sebelumnya oleh [14]kepada responden berdasarkan sub domain COBIT 5 yaitu DSS5.4 (*Manage user identitiy and logical*

*access*) dan DSS5.5 (*Manage physical access to IT assets*) kepada karyawan instansi tersebut berdasarkan tabel RACI Chart.

RACI Chart memiliki fungsi tingkatan tanggung jawab untuk peran pada struktur organisasi. RACI Chart menurut [15]memiliki tingkatan antara lain *Responsible* merupakan pihak yang melakukan pekerjaan, *Accountable* merupakan pihak yang bertanggung jawab atas semua pekerjaan dan mengarahkan jalannya pelaksanaan aktivitas,*Consulted* merupakan penasihat yang dimintai pendapat terkait pekerjaan, dan *Informed* merupakan pihak yang mendapat informasi tentang kemajuan suatu pekerjaan. Tabel RACI Chart dapat dilihat pada gambar 2.



| DSS05 RACI Chart | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key Management Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
| **DSS05.01** Protect against malware. | | | | | | R | I | | | | C | A | | | R | C | C | C | I | R | R | | I | R | | | |
| **DSS05.02** Manage network and connectivity security. | | | | | | I | | | | | C | A | | | | C | C | C | I | R | R | | I | R | | | |
| **DSS05.03** Manage endpoint security. | | | | | | I | | | | | C | A | | | | C | C | C | I | R | R | | I | R | | | |
| **DSS05.04** Manage user identity and logical access. | | | | | | R | | | | | C | A | | | I | C | C | C | I | C | R | | I | R | | | C |
| **DSS05.05** Manage physical access to IT assets. | | | | | | I | | | | | C | A | | | | C | C | C | I | C | R | | I | R | I | | |
| **DSS05.06** Manage sensitive documents and output devices. | | | | | | | | | | | I | | | | | C | C | A | | | R | | | | | | |
| **DSS05.07** Monitor the infrastructure for security-related events. | | | | | I | | C | | | | I | A | | | | C | C | C | I | C | R | | I | R | I | I | |

**Gambar 2.** RACI Chart domain DSS5

Berdasarkan gambar 2 RACI Chart maka diketahui tingkatan responden antara lain dilihat pada tabel 1.

**Tabel 1.** Hasil RACI Chart domain DSS 5.4 dan DSS5.5.

| No | *Key Mangement Practice* | RACI Chart | | | |
|---|---|---|---|---|---|
| | | R | A | C | I |
| 1 | *Chief Executive Officer* | - | - | - | - |
| 2 | *Head IT Operation* | 2 | - | - | - |
| 3 | *Business Process Owners* | - | - | - | 1 |
| 4 | *Compliance* | - | - | 2 | - |

Menurut fungsi RACI Chart *Chief Excecutive Officer* diterjemahkan sebagai Ketua STMIK X, *Head IT Operations* diterjemahkan sebagai Ketua Laboran dan *IT Staff*, *Business Process Owners* diterjemahkan sebagai Ketua Lembaga Penjaminan Mutu sebagai pengawas kebijakan yang berjalan di instansi tersebut, dan *Compliance*

diterjemahkan sebagai karyawan yang melaksanakan kebijakan keamanan informasi tersebut berkompeten menjadi responden dalam pengisisan kuisioner.

c. Analisa hasil

Analisa hasil yang dilakukan antara lain analisis hasil wawancara untuk menaksir nilai aktual dan nilai ekspektasi dari tingkat kepatuhan karyawan dengan tingkat kematangan pada COBIT 5 serta analisis data yang tediri dari uji validitas dan uji reliabilitas kuisioner.

d. Analisa kesenjangan

Analisa kesenjangan dilakukan untuk mengetahui selisih dari hasil analisa nilai aktual dan nilai ekspektasi tingkat kepatuhan sehingga diperoleh hasil kesenjangan sebagai acuan pemberian rekomendasi.

e. Pemberian rekomendasi

Pemberian rekomendasi berdasarkan hasil analisis yang telah diperoleh sebelumnya melalui analisis hasil nilai aktual dan nilai kesenjangan.

f. Kesimpulan dan saran

Kesimpulan disusun berdasarkan hasil keseluruhan penelitian dan saran disusun untuk penelitian selanjutnya.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Analisis Hasil

Saat ini tekonologi informasi dikelola oleh unit pelaksana teknis teknologi informasi yang dibantu oleh unit pelaksana teknis laboratorium komputer dan diawasi oleh Lembaga Penjaminan Mutu. Jumlah karyawan pada masing-masing bagian dapat dilihat pada tabel 2.

**Tabel 2.**Jumlah karyawan di UPT Teknologi Informasi, Laboratorium Komputer dan Lembaga Penjaminan Mutu

| No | Unit Kerja | Jumlah Karyawan |
|---|---|---|
| 1 | Unit Pelaksana Teknis Teknologi Informasi | 2 orang |
| 2 | Unit Pelaksana Teknis Laboratorium Komputer | 11 orang |
| 3 | Lembaga Penjaminan Mutu | 4 orang |

Saat ini kebijakan yang telah dibuat dan diawasi oleh Lembaga Penjaminan Mutu terkait aspek *logical* dan *physical security* tertuang dalam beberapa Standar Operasional Prosedur. Standar Operasional tersebut di antaranya dapat dilihat pada tabel 3.

**Tabel 3.**Daftar Standar Operasional Prosedur yang dibuat oleh Unit Pelaksana Teknis Teknologi Informasi dan Laboratorium Komputer

| | |
|---|---|
| Unit Pelaksana Teknis Teknologi Informasi | a. Prosedur mutu pendaftaran email resmi untuk dosen, karyawan, mahasiswa, UKM, unit kerja.<br>b. Prosedur mutu integrasi sistem informasi.<br>c. Prosedur mutu pengaduan keamanan jaringan, aplikasi, dan data.<br>d. Prosedur mutu penyimpanan data institusi. |
| Unit Pelaksana Teknis Laboratorium Komputer | a. Prosedur mutu penggunaan LCD.<br>b. Prosedur mutu penggunaan komputer.<br>c. Prosedur mutu pengadaan komputer dan peripheral.<br>d. Prosedur pemasangan jaringan.<br>e. Prosedur mutu pelaksanaan praktikum laboratorium komputer.<br>f. Prosedur mutu instruksi kerja pendaftaran login mikrotik. |

Berdasarkan tabel 3 belum ditemukan adanya kebijakan khusus terkait cara mengamankan data di dalam masing-masing prosedur mutu yang telah dibuat atau prosedur mutu tersendiri secara terpisah. Selain itu berdasarkan 4 dari 10 aspek keamanan informasi oleh (Indrajit, 2014) kondisi STMIK X terkait aspek *logical* dan *physical security* terhadap kebijakan pengamanan data dapat dijabarkan sebagai berikut

a. Kebijakan keamanan

   Kebijakan keamanan informasi secara khusus belum tertuang di dalam masing-masing prosedur mutu maupun Standar Operasional Prosedur secara terpisah.

b. Klasifikasi dan kontrol aset

   Aset teknologi informasi di beberapa unit belum ditentukan kepemilikannya hal tesebut dilihat dari ketidakjelasan akuntabilitas pemilik sistem yang ada seperti yang terjadi pada sistem yang telah digunakan saat ini.

c. Keamanan fisik dan lingkungan

   Unit kerja divisi teknologi informasi belum memiliki sentra komputer dan ruang kerja khusus yang hanya dapat diakses oleh karyawan di unit kerja itu sendiri dan orang lain yang mendapat ijin sebelumnya. Selain itu, belum semua karyawan

menyadari pentingnya *clear desk* dan *clear screen* untuk mengurangi risiko akses tanpa ijin atau kerusakan terhadap dokumen-dokumen yang ada.

d. Pengontrolan akses

Pengontrolan akses yang ada di STMIK X belum terpenuhi secara keseluruhan seperti terjadinya insiden bocornya akses wifi mahasiswa yang diluar akun yang telah terdaftar dan akun-akun alumni mahasiswa masih dapat mengakses jaringan internet ketika berada di lingkungan kampus.

Berdasarkan hasil penyebaran kueisioner didapatkan 83 responden yang terdiri dari dosen dan karyawan sebagai pengguna, pengawas, dan pengelola teknologi informasi yang menilai kondisi kepatuhan karyawan pada aspek *logical* dan *physical security* terhadap kebijakan pengamanan data. Pada penelitian ini analisis data yang dilakukan adalah uji validitas dan uji reliabilitas untuk menguji alat ukur berupa kuesioner dan tingkat kematangan aktual kepatuhan karyawan pada aspek tersebut.

Uji validitas pada penelitian ini dilakukan menggunakan metode *bivariate pearson*. Hasil uji validitas pada penelitian ini diperoleh bahwa semua item pernyataan yang digunakan mempunyai koefisien hitung (*r* hitung) lebih besar dari *r* tabel. Besar *r* tabel adalah 0,5140 untuk *r* tabel dengan n= 15 dan $\alpha$ = 0,05 sehingga semua item pernyataan dinyatakan valid. Sedangkan uji reliabilitas pada penelitian ini menggunakan uji *cronbach-alpha*. Hasil uji reliabilitas dapat dilihat pada gambar 3 dan gambar 4.

**Tabel 4**. Hasil pemrosesan data pada *Case processing summary*

| Item pertanyaan | Besar R hitung total |
|---|---|
| P1 | 0,697 |
| P2 | 0,782 |
| P3 | 0,667 |
| P4 | 0,842 |
| P5 | 0,836 |
| P6 | 0,804 |
| P7 | 0,804 |
| P8 | 0,766 |
| P9 | 0,819 |
| P10 | 0,779 |
| P11 | 0,710 |
| P12 | 0,699 |
| P13 | 0,686 |
| P14 | 0,738 |
| P15 | 0,650 |

**Reliability Statistics**

| Cronbach's Alpha | N of Items |
|---|---|
| ,943 | 15 |

**Gambar 4.** Hasil uji reliabilitas

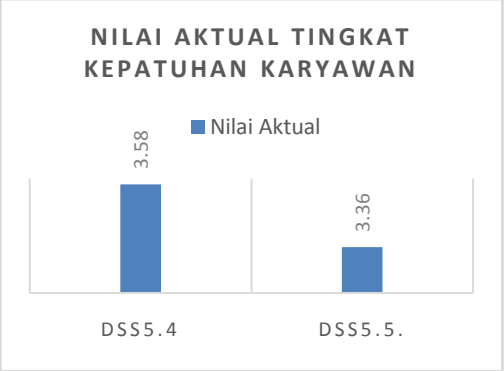
Semua data yang diproses valid sebesar 100% dan tidak ada data yang dikeluarkan. Pada gambar 4 menunjukkan bahwa alat ukur mempunyai nilai *cronbach-alpha* sebesar 0,943. Menurut Priyatno (2014) nilai *cronbcah's alpha* lebih dari 0,6 dianggap baik sehingga dapat dikatakan bahwa masing-masing item pernyataan dari kuisioner adalah sangat baik dan reliabel.

Nilai aktual tingkat kematangan kepatuhan karyawan pada aspek *logical* dan *physical security* diukur melalui *capability level*. Capability level pada COBIT 5 dapat dilihat pada tabel 5.

**Tabel 5.***Capability Level*

| No | *Capability Level* | Keterangan |
|---|---|---|
| 1 | Level 0 (*Incomplete Process*) | Proses ini tidak dilaksanakan atau gagal untuk mencapai tujuan prosesnya. |
| 2 | Level 1 (*Performed Process*) | Proses dilaksanakan dan mencapai tujuan prosesnya. |
| 3 | Level 2 (*Managed Process*) | Proses yang dilakukan sekarang diimplementasikan, dikelola dan produk kerja yang tepat ditetapkan, dikendalikan dan dipelihara. |
| 4 | Level 3 (*Established Process*) | Proses yang dikelola kini diterapkan menggunakan proses yang telah ditetapkan yang mampu mencapai hasil prosesnya. |
| 5 | Level 4 (*Predictable Process*) | Proses yang ditetapkan sekarang beroperasi dalam batas yang telah ditetapkan untuk mencapai hasil prosesnya. |
| 6 | Level 5 (*Optimizing Process*) | Proses diprediksi untuk terus ditingkatkan untuk memenuhi tujuan bisnis yang relevan saat ini dan tujunan bisnis masa datang. |

Nilai aktual tingkat kematangan kepatuhan karyawan pada aspek *logical* dan *physical security* dapat dilihat pada grafik gambar 5.




**Gambar 5.** Grafik nilai aktual tingkat kematangan kepatuhan karyawan

**Tabel 6.***Capability level* total

| Pernyataan DSS5 *(Manage Security Services)* | Nilai |
|---|---|
| *DSS05.04 Manage user identity and logical access.* | 3,58 |
| *DSS05.05 Manage physical access to IT assets.* | 3,36 |
| Rata-rata nilai | 3,47 |

Berdasarkan Tabel 6 *capability level* yang dicapai oleh karyawan STMIK X sebesar 3,47. Menurut tabel 4 nilai tersebut berada pada level 3 yaitu *Established Process*. Pada aspek *logical security* yang diterjemahkan dalam domain DSS05.04 dihasilkan nilai *capability level* sebesar 3,58 yang berarti karyawan diseluruh bagian telah melaksanakan kebijakan yang ada mengenai aspek tersebut di STMIK X. Berdasarkan Standar Operasional yang telah dibuat belum ditemukan secara spesifik terkait kebijakan keamanan informasi serta pengawasannya pada aspek *logical security*. Hal tersebut dapat dilihat dari ditemukannya ketidakjelasan akuntabilitas pemilik sistem di beberapa sistem informasi yang digunakan meskipun secara umum karyawan telah menyadari pentingnya keamanan pada *logical access* dan pengelolaan identitas pengguna.

Pada tabel 6 aspek *physical security* yang diterjemahkan dalam domain DSS05.05 dihasilkan nilai *capability level* sebesar 3,36 yang berarti telah dibuat kebijakan tentang pengelolaan aset *IT* dan akses fisiknya dalam kebijakan teknologi informasi yang ada di STMIK X meskipun belum secara keseluruhan melindungi seluruh aset-aset *IT* yang ada serta cara perlindungannya. Standar Operasional yang ada berupa cara-cara penggunaan *hardware* di lingkungan instansi tersebut agar dapat digunakan secara baik dan benar. Namun pada sisi pengelolaan keamanan akses fisik di beberapa bagian

belum terkontrol contohnya belum ditemukan ruangan sentra komputer atau *computer room* yang seharusnya dapat dijaga ketat agar tidak mudah di akses selain karyawan divisi teknologi informasi atau orang lain yang diberikan ijin sebelumnya.

Secara umum STMIK X dalam waktu dekat merencanakan pembuatan aturan dalam bentuk Standar Operasional Prosedur mengenai Sistem Manajemen Keamanan Informasi yang mengacu prosedur yang diterbitkan oleh SANS Institute. Standar Operasional Prosedur tersebut memuat pengelolaan dan pengawasan kebijakan keamanan informasi secara umum agar terdapat tanggung jawab masing-masing pengguna pada batasan-batasan regulasi dan hukum yang berlaku serta pengelolaan risiko-risiko yang sewaktu-waktu dapat mengancam aset-aset teknologi informasi. Berdasarkan *capability level* pada tabel 4 maka kondisi ekspektasi STMIK X dalam pengelolaan aspek *logical* dan *physical security* dalam kebijakan pengamanan data berada pada level 4 yaitu *Predictable Process*. *Predictable Process* yaitu proses yang ditetapkan sekarang beroperasi dalam batas yang telah ditetapkan untuk mencapai hasil prosesnya.

### 3.2. Analisis Kesenjangan

Analisis kesenjangan *capability level* kepatuhan karyawan pada aspek *logical* dan *physical security* terhadap kebijakan pengamanan data di STMIK X diperoleh dari selisih *capability level* yang diharapkan dengan *capability level* kondisi saat ini. Grafik kesenjangan dapat dilihat pada gambar 6.


**Gambar 6.** Grafik kesenjangan tingkat kematangan kepatuhan karyawan

Hasil tingkat kesenjangan keseluruhan terdapat pada Tabel 6.

**Tabel 7.** Tingkat kesenjangan pada masing-masing domain

| Domain | Nilai Eskpektasi | Nilai Aktual | Nilai Kesenjangan |
|---|---|---|---|
| *DSS05.04* | 4 | 3,58 | 0,42 |

| | | | |
|---|---|---|---|
| *DSS05.05* | 4 | 3,36 | 0,64 |
| Rata-rata nilai tingkat kesenjangan | | | 0,53 |

Berdasarkan Tabel 7. Nilai kesenjangan secara umum sebesar 0,53 namun kesenjangan paling tinggi terdapat pada domain DSS05.05 (*Manage physical access to IT assets*) sebesar 0,64. Kesenjangan tersebut dapat terjadi karena kebijakan pengamanan data secara fisik untuk melindungi aset *IT* belum sepenuhnya terdefinisi di dalam Standar Operasional Prosedur yang ada. Selain itu, belum terpenuhinya beberapa keamanan fisik seperti tersedianya sentra komputer atau *computer room* khusus bagi divisi teknologi informasi yang terpisah dengan ruangan unit lain maupun pengamanan pada personal komputer seperti *computer security steel cable* dan seperangkat *security kit* pada perangkat lain.

### 3.3. Pemberian Rekomendasi

Rekomendasi yang dapat diberikan antara lain

a. STMIK X membuat atau meningkatkan prosedur mutu yang telah berjalan dengan menambah prosedur pada pengamanan aset-aset teknologi informasi baik dari sisi pengguna dan pengelola dan munculnya batasan-batasan dalam penggunaan dan pengelolaannya sesuai aturan dan hukum yang berlaku.
b. Unit kerja teknologi informasi mengevaluasi dan menyempurnakan ruang lingkup prosedur mutu yang telah ada terkait kontrol terhadap sistem informasi yang digunakan agar tercipta akuntabiltas pemilik pada masing-masing sistem dan dapat memberikan perlindungan yang tepat untuk memelihara kontrol sistem tersebut.
c. Adanya pengadaan keamanan lingkungan fisik berupa pengadaan sentra komputer ataupun *computer room* untuk mengurangi risiko terjadinya akses tanpa ijin selain karyawan divisi teknologi informasi.
d. Adanya pengadaan keamanan fisik pada aset-aset IT yang lain seperti *PC security kit, drive lock, network security box*, dan sejenisnya.

## 4. KESIMPULAN

Kesimpulan pada penelitian ini antara lain

a. Aspek *logical* dan *physical security* adalah aspek penting dari keseluruhan bagian prinsip-prinsip dasar keamanan informasi.
b. Nilai aktual tingkat kematangan secara keseluruhan berada pada level 3 (*Established Process*). Pada level tersebut kebijakan yang saat ini berjalan telah mendefinisikan aspek *logical* dan *physical security* namun pada beberapa bagian aspek tersebut belum terpenuhi.
c. Nilai kesenjangan secara keseluruhan sebesar 0,53 namun kesenjangan paling tinggi terdapat pada domain DSS05.05 (*Manage physical access to IT assets*) sebesar 0,64. Kesenjangan tersebut dapat terjadi karena kebijakan pengamanan data secara fisik untuk melindungi aset *IT* belum sepenuhnya terdefinisi di dalam Standar Operasional Prosedur yang ada.
d. Rekomendasi yang diberikan berdasarkan hasil analisis pada kondisi aktual dan kondisi kesenjangan yang ada secara umum dan secara khusus yang memiliki nilai kesejangan tertinggi. Rekomendasi tersebut di antaranya evaluasi dan penyempurnaan pada prosedur mutu yang telah berjalan dengan menambah item aspek *logical* dan *physical security* dalam rangka mengamankan data di STMIK X. Selain itu, adanya pengadaan perlindungan keamanan fisik terhadap aset-aset IT seperti pengadaan *computer room, PC security kit, drive lock,*dan *network security box*.

## 5. SARAN

Saran-saran yang dapat diberikan antara lain

a. Adanya pengembangan objek yang diteliti di dalam COBIT 5 berdasarkan prinsip dasar keamanan informasi yaitu domain DSS 5 secara keseluruhan yang meliputi pengelolaan layanan keamanan dan domain APO 13 yang meliputi pengelolaan keamanan.
b. Pengukuran *capability level* dapat ditambah menggunakan metode PAM (*Process Assement Model*).
c. Pengukuran kepatuhan karyawan pada aspek *logical* dan *physical security* dapat ditambah dengan cara-cara mengelola risiko yang diterjemahkan pada domain APO

12 mengenai pengelolaan risiko dan EDM 03 mengenai pengoptimalan pengelolaan risiko.

**DAFTAR PUSTAKA**

[1] M. E. Whitman and H. J. Mattord, Principle of Information Security, Boston: Course Technology, 2013.

[2] R. E. Indrajit, Konsep dan Strategi Keamanan Informasi di Dunia Cyber, Yogyakarta: Graha Ilmu.

[3] IBISA, Keamanan Sistem Informasi, Yogyakarta: CV. ANDI OFFSET, 2011.

[4] IBISA, Physical Security, Yogyakarta: CV ANDI OFFSET, 2013.

[5] D. Sikolia and D. Biros, "Motivating Employees to Comply with Information Security Policies," *Journal of the Midwest Association for Information Systems (JMWAIS),* Vols. -, no. 2, 2016.

[6] S. Bauer, E. W. Bernroider and K. Chudzikowski, "Prevention Is Better Than Cure! Designing Information Security Awareness Programs To Overcome Users' Non-Compliance With Information Security Policies In Banks," *Journal of Computers and Security,* no. 68, 2017.

[7] E. L. Putra, B. C. Hidayanto and H. M. Astuti, "Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. dengan Menggunakan Indeks Keamanan Informasi (KAMI)," *Jurnal Teknik Pomits,* vol. 3, no. 2, 2014.

[8] M. Amin, "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (MCDA)," *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika,* vol. V, no. 1, 2014.

[9] S. Bauer, Bernroider and E. W.N., "From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization," September 2017.

[10] H. Affandi and A. Darmawan, "Audit Kemanan Informasi Menggunakan ISO 27002 Pada Data Center PT.Gigipatra Multimedia," *Jurnal TIM Darmajaya,* vol. I, no. 2, 2015.

[11] M. Wolden, R. Valverde and M. Talla, "The effectiveness of COBIT 5 Information Security Framework for Reducing Cyber Attacks on Supply Chain Management System On Supply Chain Management Systems," September 2017.

[12] Sugiono, Metode Penelitian dan Pengembangan Research and Development, Bandung: CV. Alfabeta, 2016.

[13] Sukandarrumidi, Metode Penelitian Petunjuk Praktis untuk Peneliti Pemuda, Yogyakarta: Gadjah Mada University Press, 2012.

[14] R. Papang and E. N. Sancoyo, "Penyusunan Tata Kelola Audit E-Procurement Instansi Pemerintah," *JNTETI,* vol. II, no. 3, 2013.

[15] D. M. Selvianti, Muraharwaty and W. Herwondo, "Perancangan Service Catalogue Management pada Layanan IT PUSAIR dengan menggunakan Framework ITIL Versi 3," *Jurnal Sistem Informasi,* vol. V, no. 4, pp. 436-445, 2015.