

**LAPORAN KERJA PRAKTIK**

**EVALUASI TATA KELOLA KEAMANAN SISTEM INFORMASI**

**MENGGUNAKAN *FRAMEWORK* COBIT 5**

**(STUDI KASUS: TSIRWAH INDONESIA)**

Diajukan untuk memenuhi persyaratan kelulusan

Matakuliah FTI335 – Kerja Praktik

Oleh:

Hanif Ibrahim / 312220016



**PROGRAM STUDI SISTEM INFORMASI**

**FAKULTAS TEKNOLOGI INFORMASI**

**UNIVERSITAS BALE BANDUNG**

**2024**

**LEMBAR PENGESAHAN**

**PROGRAM STUDI SISTEM INFORMASI**

**EVALUASI TATA KELOLA KEAMANAN SISTEM INFORMASI**

**MENGGUNAKAN *FRAMEWORK* COBIT 5**

**(STUDI KASUS: TSIRWAH INDONESIA)**

Oleh: Hanif Ibrahim / 312220016

disetujui dan disahkan sebagai  
**LAPORAN KERJA PRAKTIK**

Bandung, 12 Februari 2025

Koordinator Kerja Praktik

Denny Rusdianto, S.T., M.Kom  
NIP:04015704

**LEMBAR PENGESAHAN**

**PROGRAM STUDI SISTEM INFORMASI**

**EVALUASI TATA KELOLA KEAMANAN SISTEM INFORMASI**

**MENGGUNAKAN *FRAMEWORK* COBIT 5**

**(STUDI KASUS: TSIRWAH INDONESIA)**

Oleh: Hanif Ibrahim / 312220016

disetujui dan disahkan sebagai  
**LAPORAN KERJA PRAKTIK**

Bandung, 12 Februari 2025

Founder Tsirwah Indonesia

Hafidz Ramdhani

## ABSTRAK

Evaluasi tata kelola keamanan sistem informasi merupakan aspek krusial untuk memastikan keamanan, efisiensi, dan efektivitas operasional suatu organisasi. Penelitian ini dilakukan di Tsirwah Indonesia, sebuah perusahaan yang menggunakan bidang teknologi informasi dalam operasionalnya, dengan fokus mengevaluasi tata kelola keamanan menggunakan framework COBIT 5, khususnya pada domain DSS05 (*Manage Security Services*). Tujuan penelitian ini adalah untuk menilai tingkat kematangan tata kelola keamanan sistem informasi di Tsirwah Indonesia dan memberikan rekomendasi perbaikan. Metodologi yang digunakan meliputi analisis kuisioner kepada pemangku kepentingan untuk menilai tingkat kematangan subdomain DSS05, termasuk perlindungan terhadap malware, manajemen keamanan jaringan, pengelolaan identitas pengguna dan lainnya.

Hasil analisis menunjukkan bahwa tingkat kematangan rata-rata berada pada level 3 (*Established*) dan level 4 (*Predictable*), yang mencerminkan adanya prosedur formal namun masih memerlukan perbaikan untuk mencapai tingkat optimal (*Optimized*). *Gap analysis* mengidentifikasi kesenjangan antara tingkat kematangan saat ini dan yang diharapkan. Rekomendasi strategis disusun untuk meningkatkan keamanan sistem informasi, termasuk pelatihan, pembaruan kebijakan, dan penerapan teknologi perlindungan. Penelitian ini memberikan kontribusi signifikan dalam meningkatkan tata kelola keamanan informasi di Tsirwah Indonesia dan sebagai pengalaman praktis bagi mahasiswa dalam menerapkan ilmu yang telah dipelajari.

**Kata Kunci:** Tata Kelola Keamanan, COBIT 5, DSS05, Tsirwah Indonesia, Maturity Level, Evaluasi Sistem Informasi.

## KATA PENGANTAR

Puji Syukur kepada Tuhan Yang Maha Esa karna berkat dan karunianya penulis bisa menyelesaikan Laporan Kerja Praktek dengan Judul “Evaluasi Tata Kelola Keamanan Sistem Informasi Menggunakan *Framework* COBIT 5 (Studi Kasus: Tsirwah Indonesia)”, yang merupakan persyaratan kelulusan Matakuliah FTI335 Kerja Praktik.

Dalam penyusunan laporan kerja praktek ini penulis banyak mendapat saran, dorongan, bimbingan dan arahan dari berbagai pihak sehingga sangat membantu dalam melaksanakan Kerja Praktek dan Menyusun laporan ini. Maka dengan segala hormat dan kerendahan hati perkenankanlah penulis mengucapkan terimakasih kepada:

1. Orang tua, kakak-kakak, keponakan, dan saudara-saudara yang telah mendukung dalam bentuk moral maupun materi.
2. Bapak Yudi Herdiana, S.T., M.T selaku Dekan Fakultas Teknologi Informasi.
3. Ibu Rosmalina, S.T., M.Kom selaku Ketua Prodi Sistem Informasi.
4. Bapak Denny Rusdianto, S.T., M.Kom selaku Koordinator Lapangan Kerja Praktik dan Pembimbing Kerja Praktik.
5. Bapak Hafidz Ramdhani selaku Founder Tsirwah Indonesia dan Pembimbing Lapangan.
6. Kak Dewi, Kak Dennis, Kak Hani, Kak Divya dan Kak Wilda selaku rekan tim selama masa kerja praktik.
7. Teman-teman seperjuangan yang selalu mendukung dan membantu dalam penyusunan laporan kerja praktik.
8. Serta pihak-pihak lainnya yang telah membantu dalam penyusunan laporan kerja praktik ini.

Penulis menyadari bahwa banyak kekurangan dalam penulisan laporan ini. Oleh karena itu, kritik dan saran yang bersifat membangun akan penulis terima dengan baik, semoga dengan adanya laporan ini bermanfaat bagi semua.

## DAFTAR ISI

ABSTRAK .....	iii
KATA PENGANTAR .....	iv
DAFTAR ISI.....	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR .....	viii
BAB I PENDAHULUAN.....	1
I.1. Latar Belakang .....	1
I.2. Lingkup .....	3
I.3. Tujuan Praktik Kerja .....	3
BAB II TINJAUAN UMUM .....	4
II.1. Strukur Organisasi .....	4
II.2. Deskripsi Pekerjaan .....	5
II.3. Jadwal Kerja Praktik .....	6
BAB III TEORI PENUNJANG KERJA PRAKTIK .....	7
III.1. Teori Penunjang.....	7
III.2. Pengertian Dasar Sistem Informasi.....	8
III.2.1. Pengertian Sistem.....	8
III.2.2. Pengertian Informasi .....	8
III.2.3. Pengertian Sistem Informasi .....	8
III.3. Evaluasi.....	8
III.4. Tata Kelola IT.....	9
III.5. <i>Framework</i> COBIT 5.....	9
III.6. Analisa Maturity Level .....	11
III.7. Analisa Kesenjangan ( <i>Gap Analysis</i> ).....	13
III.8. DDoS (Distributed Denial of Service) Attack .....	13
BAB IV PELAKSANAAN PRAKTIK KERJA .....	14
IV.1. Input .....	14
IV.2. Proses .....	15
IV.2.1. Eksplorasi.....	15

IV.2.2. Evaluasi Tata Kelola Keamanan Sistem Informasi .....	16
IV.2.3. Pelaporan Hasil Kerja Praktik.....	18
IV.3. Pencapaian Hasil.....	18
IV.3.1. Analisa Tingkat Kematangan.....	18
IV.3.2. Ringkasan Tingkat Kematangan Domain DSS05.....	22
IV.3.3. Analisis Kesenjangan (GAP Analysis) .....	23
IV.3.4. Rekomendasi.....	24
<b>BAB V PENUTUP.....</b>	<b>26</b>
V.1. Kesimpulan dan saran mengenai pelaksanaan .....	26
V.1.1. Kesimpulan Pelaksanaan Kerja praktik .....	26
V.1.2. Saran Pelaksanaan Kerja praktik .....	26
V.2. Kesimpulan dan saran mengenai substansi .....	27
V.2.1. Kesimpulan .....	27
V.2.1. Saran .....	27
<b>DAFTAR PUSTAKA .....</b>	<b>29</b>

## DAFTAR TABEL

Tabel II.1. Jadwal Kerja Praktik .....	6
Tabel IV.1 Lembar Evaluasi Domain DSS 05 .....	18
Tabel IV.2. Tingkat Kematangan Subdomain DSS05.01 .....	19
Tabel IV.3. Tingkat Kematangan Subdomain DSS05.02 .....	19
Tabel IV.4. Tingkat Kematangan Subdomain DSS05.03 .....	20
Tabel IV.5. Tingkat Kematangan Subdomain DSS05.04 .....	20
Tabel IV.6. Tingkat Kematangan Subdomain DSS05.05 .....	21
Tabel IV.7. Tingkat Kematangan Subdomain DSS05.06 .....	21
Tabel IV.8. Tingkat Kematangan Subdomain DSS05.07 .....	21
Tabel IV.9. Ringkasan Tingkat Kematangan .....	22
Tabel IV.10. Analisis Kesenjangan (GAP Analysis) .....	23



## DAFTAR GAMBAR

Gambar II. 1. Struktur Organisasi Tsirwah.....	4
Gambar III.1 Prinsip COBIT 5.....	10
Gambar III.2 Analisa Maturity Levels .....	12
Gambar IV.1. Screenshoot DDoS Attack .....	14
Gambar IV.2. Rumus Perhitungan Kuesioner.....	18
Gambar IV.3. Grafik Analisis Kesenjangan .....	24

# **BAB I**

## **PENDAHULUAN**

### **I.1. Latar Belakang**

Evaluasi sistem informasi adalah proses penilaian independen terhadap sistem informasi suatu organisasi untuk mengevaluasi keamanan, efisiensi, efektivitas, dan kepatuhan terhadap kebijakan dan prosedur yang relevan. Tujuan Evaluasi ini adalah untuk memastikan bahwa sistem informasi beroperasi dengan baik, melindungi data sensitif, dan memenuhi tujuan organisasi (Doharma et al., 2021). Evaluasi sistem informasi membantu mengidentifikasi kekurangan, mengoptimalkan proses, serta mengurangi risiko yang dapat mengganggu operasi perusahaan.

Tsirwah Indonesia merupakan perusahaan yang bergerak di bidang IT untuk mendukung proses bisnisnya. Penggunaan IT pada Tsirwah Indonesia ini bertujuan untuk meningkatkan layanan yang diberikan terhadap *stakeholder* terutama informasi pemberitaan *online* kepada masyarakat. Untuk itu perlu adanya dukungan keamanan informasi yang bertujuan agar informasi yang diberikan dapat berjalan dengan lancar.

Evaluasi sistem informasi adalah salah satu bentuk dukungan keamanan informasi yang bertujuan untuk mengurangi atau menghindari ancaman terhadap keamanan data. Keamanan informasi merupakan bagian penting dari tata kelola organisasi. Jika keamanan informasi terganggu, kinerja TI akan terganggu. Hal ini karena keamanan informasi merupakan aspek penting dari kerahasiaan, integritas, dan ketersediaan. Jika ada masalah dengan sistem informasi, kegiatan operasional perusahaan akan secara tidak langsung terpengaruh (Wijaya & Aziz, 2019).

Berdasarkan wawancara yang dilakukan diketahui bahwa, belum lama ini tepatnya tanggal 12 Maret 2024 terjadi pembobolan keamanan sistem di Tsirwah Indonesia

ini terjadi karena DDoS (*Distributed Denial of Service*) Attack sehingga saat itu website Tsirwah tidak dapat diakses oleh pengguna. Akibatnya dari serangan ini merugikan bagi pihak Tsirwah dan juga orang-orang yang terlibat di dalamnya. Untuk menjaga keamanan sistem informasi perusahaan, maka diperlukan evaluasi tata kelola keamanan IT.

Masalah keamanan informasi merupakan hal penting dalam penyimpanan data dan informasi untuk mencegah ancaman terhadap sistem (Kadir, 2014). Masalah keamanan informasi sudah seharusnya menjadi perhatian oleh pihak Tsirwah Indonesia yang telah memanfaatkan sistem dan teknologi informasi dalam mendukung proses bisnisnya.

Dalam permasalahan ini, Tsirwah Indonesia memerlukan Evaluasi sistem informasi. Evaluasi sistem informasi ini mengacu pada *framework* COBIT 5. *Framework* COBIT 5 (*Control Objectives for Information and Related Technologies*) merupakan kerangka kerja untuk tata kelola IT yang diciptakan oleh ISACA (*Information System Evaluasi and Control Association*) dan ITGI (*IT Governance Institute*). COBIT memiliki model maturity yang dimaksudkan untuk mencapai tujuan secara keseluruhan dari proses penilaian dan dukungan perbaikan. Tujuannya adalah untuk menyediakan cara untuk mengukur kinerja dari setiap aspek sistem informasi, yang kemudian dapat diterapkan pada penilaian maturity (Wijaya & Aziz, 2019).

COBIT 5 mengukur tingkat pengelolaan keamanan informasi yang diterapkan pada perusahaan dengan menyediakan proses-proses yang memiliki kaitan dengan pengelolaan keamanan informasi. Proses tersebut adalah DSS05 (*Manage Security Services*) yang merupakan salah satu proses utama pada COBIT 5 untuk mengukur pengelolaan keamanan informasi (ISACA, 2012).

Berdasarkan permasalahan yang telah dijabarkan, diperlukan evaluasi tata kelola sistem informasi yang sesuai untuk Tsirwah Indonesia dengan menggunakan domain DSS05 (*Manage security services*), karena berkaca dari permasalahan

yang perlunya evaluasi di bagian pengelolaan keamanan sistem. Dengan demikian, tidak akan mengganggu kinerja sistem dan orang-orang yang terlibat di dalamnya serta mencegah kejadian serupa di masa yang akan datang.

Sesuai dengan latar belakang di atas, penulis tertarik untuk mengangkat menjadi sebuah judul laporan kerja praktik dengan judul “*Evaluasi Tata Kelola Keamanan Sistem Informasi Menggunakan Framework COBIT 5*” dengan Studi Kasus Tsirwah Indonesia.

## **I.2. Lingkup**

Lingkup kerja praktek yang dilaksanakan di Tsirwah Indonesia adalah evaluasi tata kelola sistem informasi terhadap keamanan sistem yang menyangkut hal berikut:

1. Evaluasi tata kelola keamanan sistem informasi ini menggunakan *framework* COBIT 5 yang berfokus kepada domain DSS05
2. Mengevaluasi tata kelola keamanan sistem informasi agar tidak terjadi hal serupa di masa yang akan datang.

## **I.3. Tujuan Praktik Kerja**

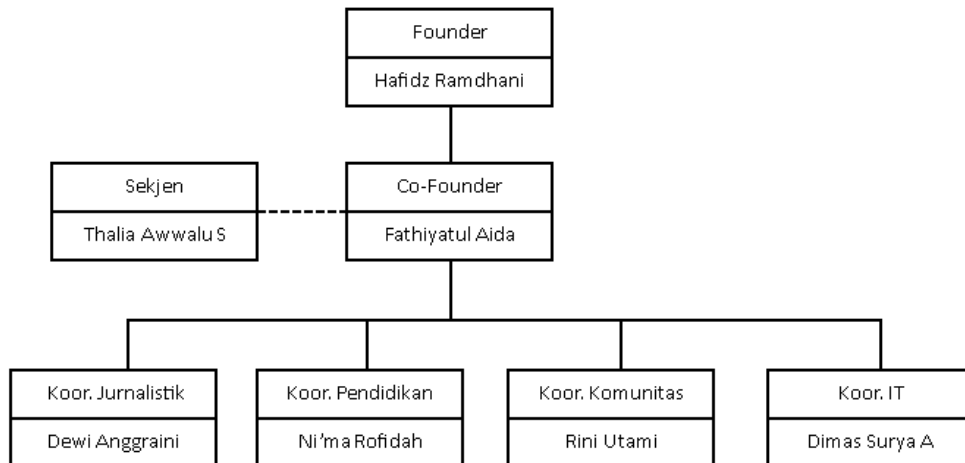
Tujuan praktik kerja di Tsirwah Indonesia adalah:

1. Sebagai salah satu syarat menyelesaikan studi jenjang strata 1 (S1) program studi Sistem informasi.
2. Mengevaluasi sistem informasi di Tsirwah Indonesia menggunakan *framework* COBIT 5
3. Pendarapan domain DSS05 (*Manage security services*) di Tsirwah Indonesia

## BAB II

### TINJAUAN UMUM

#### II.1. Strukur Organisasi



*Gambar II. 1. Struktur Organisasi Tsirwah*

1. Founder
  - a. Menetapkan visi, misi serta tujuan Tsirwah.
  - b. Mengambil keputusan yang strategis.
  - c. Memberikan arahan ke semua pengurus Tsirwah.
  - d. Membangun jaringan dengan mitra, lembaga serta komunitas serupa.
2. Co-Founder
  - a. Membantu founder mengerjakan tugasnya.
  - b. Mengelola keuangan dan operasional Tsirwah.
3. Sekjen
  - a. Mengelola administrasi dan dokumentasi Tsirwah.
  - b. Menyusun laporan kegiatan Tsirwah.
  - c. Mengkoordinasikan kegiatan antar divisi.
4. Koor. Jurnalistik

- a. Memastikan artikel yang akan dipublikasi telah sesuai SOP dan kaidah SEO.
  - b. Mengkoordinasikan pemateri yang mengisi materi pelatihan jurnalistik.
  - c. Mengkoordinasikan dengan editor dan publikator mengenai pembuatan artikel.
5. Koor. Pendidikan
- a. Mengembangkan dan mengkurasi materi pembelajaran.
  - b. Merancang program pendidikan yang lebih inovatif.
  - c. Melakukan evaluasi tenaga pendidik dan program yang telah berjalan.
6. Koor. Komunitas
- a. Membangun dan memelihara hubungan baik dengan anggota Tsirwah.
  - b. Mengumpulkan masukan dari anggota untuk evaluasi Tsirwah.
7. Koor. IT
- a. Memastikan website serta aplikasi Tsirwah berjalan dengan baik.
  - b. Menjamin data dan informasi pengguna Tsirwah.
  - c. Membuat desain yang akan dipublikasikan di media sosial

### Lingkup Pekerjaan

Divisi Jurnalistik di Tsirwah Indonesia memiliki lingkup pekerjaan memastikan setiap artikel yang akan terbit sudah sesuai dengan standard operasional Tsirwah serta SEO.

Ketika proses kerja praktik ini berlangsung, divisi Jurnalistik Tsirwah Indonesia sedang mengalami kebingungan akan koreksian yang lebih aman serta efektif sehingga perlu dilakukan evaluasi tata kelola sistem.

### II.2. Deskripsi Pekerjaan

Deskripsi pekerjaan yang dilakukan selama kerja praktik di divisi jurnalistik Tsirwah Indonesia yaitu mengoreksi artikel peserta yang masuk sesuai dengan anggota yang telah dibagi setiap selesai kelas menulis diselenggarakan agar artikel

yang akan dipublikasikan di website Tsirwah Indonesia sesuai dengan kaidah SOP Tsirwah serta kaidah SEO artikel ini di *publish* di [jurnalistik.tsirwah.com](http://jurnalistik.tsirwah.com)

### II.3. Jadwal Kerja Praktik

No	Kegiatan	Sept			Okt				Nov
		II	III	IV	I	II	III	IV	I
1	Pengenalan Tempat Kerja Praktek								
2	Pengumpulan Data								
3	Kerja Praktek								
4	Konsultasi pada Pembimbing								
5	Penyusunan Laporan Kerja Praktek								

*Tabel II.1. Jadwal Kerja Praktik*

Kerja praktik di laksanakan dari bulan September sampai bulan November 2024, Waktu kerja praktik adalah hari Senin sampai hari Kamis dengan jam yang di sesuaikan dengan jadwal perkuliahan. Secara umum, kegiatan yang dilakukan selama kerja praktik adalah sebagai berikut

1. Minggu pertama: pengenalan lingkungan kerja praktik
2. Minggu kedua: melakukan analisis kebutuhan yang akan digunakan dalam evaluasi tata kelola sistem informasi
3. Minggu ketiga: melakukan analisis kebutuhan yang akan digunakan dalam evaluasi tata kelola sistem informasi
4. Minggu Keempat: Perancangan Audit Working Paper
5. Minggu kelima: Penyusunan pertanyaan
6. Minggu Keenam: konsultasi pada pembimbing
7. Minggu Ketujuh: konsultasi pada pembimbing
8. Minggu Kedelapan: penyusunan laporan kerja praktik

## **BAB III**

### **TEORI PENUNJANG KERJA PRAKTIK**

#### **III.1. Teori Penunjang**

Pelaksanaan kerja praktek di Tsirwah Indonesia penulis menggunakan pengetahuan yang diperoleh selama masa perkuliahan sebagai landasan teori. Pengetahuan dan teori yang digunakan antara lain:

1. Tata Kelola

Teori tentang tata kelola teknologi informasi diperoleh di mata kuliah SIF335 yaitu Perencanaan Sistem Informasi. Tata kelola memiliki fokus mengenai kerangka kerja dan praktiknya dalam pengelolaan sistem informasi.

2. SI Manajemen

Teori tentang sistem informasi manajemen di mata kuliah TIF314 yaitu Sistem Informasi Manajemen. Dalam mata kuliah ini, mahasiswa memahami bagaimana sistem informasi dapat digunakan untuk tujuan manajerial dan operasional dalam sebuah organisasi.

3. Strategi SI

Teori tentang Strategi SI diperoleh di mata kuliah SIF331 yaitu Perencanaan Strategis SI. Dalam mata kuliah ini mengajarkan mahasiswa untuk mampu merancang dan menerapkan strategi SI yang selaras dengan tujuan organisasi.

4. Pengembangan SI

Teori tentang Pengembangan SI diperoleh di mata kuliah yaitu Pengembangan Sistem Informasi. Dalam mata kuliah ini, mahasiswa memahami proses pembuatan, pengujian dan implementasi sistem informasi yang dapat mendukung pengambilan keputusan.

5. Proyek SI

Teori tentang proyek SI diperoleh di mata kuliah SIF330 yaitu Pengelolaan Proyek SI. Proyek SI ini mengajarkan mahasiswa untuk mengidentifikasi,



menganalisis dan mengelola risiko yang berkaitan dengan penggunaan SI dalam organisasi.

### **III.2. Pengertian Dasar Sistem Informasi**

#### **III.2.1. Pengertian Sistem**

Sistem merupakan sekumpulan elemen yang saling terhubung dan berinteraksi untuk mencapai tujuan tertentu. Sistem terdiri dari tiga komponen utama yaitu input, proses, dan output. Sebagai contoh, dalam konteks organisasi, sistem digunakan untuk mengolah berbagai sumber daya seperti manusia, teknologi, dan data menjadi informasi yang bermanfaat. (Lediwara, 2020).

#### **III.2.2. Pengertian Informasi**

Informasi adalah data yang telah diproses sehingga memiliki nilai dan relevansi bagi penggunaannya. Informasi yang baik harus memenuhi kriteria seperti akurasi, relevansi, kelengkapan, dan ketepatan waktu. Dalam dunia bisnis dan teknologi, informasi yang berkualitas tinggi memungkinkan organisasi untuk memahami kondisi saat ini dan merencanakan langkah strategis ke depan. (Lediwara, 2020)

#### **III.2.3. Pengertian Sistem Informasi**

Sistem informasi adalah kombinasi antara teknologi, manusia, dan proses yang dirancang untuk mengelola informasi secara efisien. Sistem ini membantu organisasi mengumpulkan, menyimpan, memproses, dan mendistribusikan informasi untuk mendukung operasional dan pengambilan keputusan. (Andry et al., 2022).

### **III.3. Evaluasi**

Evaluasi merupakan bagian dari sistem manajemen yaitu perencanaan, organisasi, pelaksanaan, monitoring dan evaluasi. Evaluasi sistem informasi dapat dilakukan dengan cara berbeda dan pada tingkatan berbeda, tergantung pada tujuan evaluasinya. Tujuannya adalah untuk menilai kemampuan teknis, pelaksanaan operasional, dan pendayagunaan sistem. Evaluasi dilakukan untuk mendefinisikan seberapa baik sistem berjalan. Tujuan evaluasi sistem informasi antara lain: menilai

kemampuan teknis dari sebuah sistem informasi. Dan menilai keberhasilan dan kegagalan pelaksanaan operasional sistem informasi (Saputera et al., 2020).

#### **III.4. Tata Kelola IT**

Tata kelola Teknologi Informasi adalah melakukan proses pemantauan dan pengendalian keputusan kapabilitas teknologi informasi (TI) dalam memastikan value delivery (mengirimkan nilai) kepada pemangku kepentingan utama dalam suatu organisasi (Sofa et al., 2020). Pentingnya Tata Kelola Teknologi Informasi adalah:

1. Terdapat perubahan peran Teknologi Informasi, dari efisiensi ke peran strategis dan ditangani oleh level korporat.
2. Beberapa proyek strategi Teknologi Informasi gagal dalam pelaksanaannya karena hanya ditangani oleh teknisi TI.
3. Keputusan kebijakan Teknologi Informasi di dewan direksi biasanya bersifat adhoc.
4. Teknologi Informasi merupakan pendorong utama proses transformasi bisnis yang berdampak pada organisasi dalam pencapaian misi, visi, dan tujuan strategis.
5. Pelaksanaan TI harus dapat terukur melalui matriks tata kelola TI.

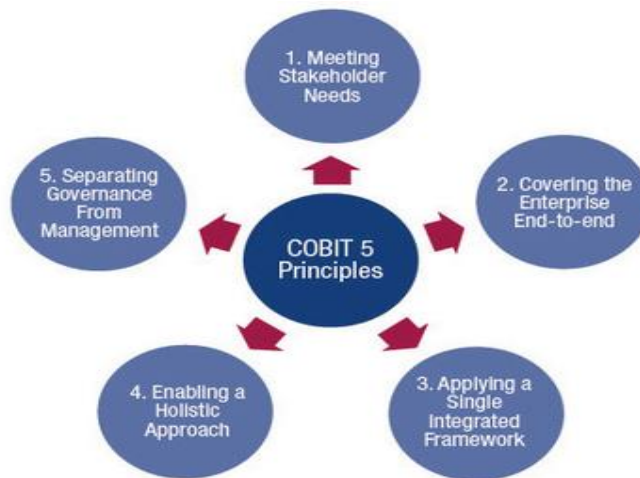
#### **III.5. Framework COBIT 5**

COBIT (*Control Objectives for Information and Related Technology*) merupakan pedoman yang digunakan untuk melakukan manajemen TI dibuat oleh *Information Systems Audit and Control Association* (ISACA) dan *IT Governance Institute* (ITGI). COBIT digunakan untuk memastikan penerapan teknologi informasi dapat mendukung tujuan serta goals yang ditetapkan suatu perusahaan dengan cara mengukur kualitas tatakelola teknologi informasi pada perusahaan terkait (Sari, 2021).

COBIT 5 menyediakan kerangka kerja yang lengkap. Terdapat 5 domain dan 37 proses pada COBIT 5 yang dapat digunakan untuk melakukan audit. Maka dari itu

COBIT 5 dianggap sesuai dan dapat membantu dalam proses audit teknologi informasi karena mencakup semua elemen pada teknologi informasi yang dipakai (Waruwu & Sundari, 2024).

COBIT 5 dikembangkan berdasarkan prinsip-prinsip COBIT 4.1 dan menggabungkan standar penilaian dan manajemen risiko TI dari ISACA, ITIL, dan ISO. Prinsip dasar COBIT 5 untuk mengelola organisasi di TI (ISACA, 2012) Penjelasan 5 prinsip COBIT 5 sebagaimana Gambar 3.1.



*Gambar III.1 Prinsip COBIT 5*

Keterangan gambar:

1. *Meeting Stakeholder Need*, pada prinsip ini memiliki lima proses berbeda, yang masing- masing mencakup langkah evaluasi, pemantauan, dan pelaporan (EDM).
2. *Covering the Enterprise End to end*, Area ini terdiri dari empat domain yang terkait dengan area fokus PERM (Perencanaan, Pembangunan, dan Pemantauan), dan menyediakan dukungan TI end-to-end. Padahal setiap proses memerlukan kegiatan perencanaan, pelaksanaan, pelaksanaan, dan pemantauan. Saat bekerja dengan TI di tingkat perusahaan, proses atau masalah tertentu yang ditawarkan biasanya ditempatkan di wilayah yang berbeda dari yang biasanya.

3. *Applying a Single Integrated Framework*, Cobit 5 adalah kerangka kerja yang bekerja terintegrasi dengan praktik yang baik dan standar TI lainnya untuk memberikan jaminan untuk setiap aktivitas TI.
4. *Enabling a Holistic Approach*, Sesuai dengan konsep tersebut, pengelolaan TI dapat diterapkan secara efektif serta efisien, dan terhubung dengan semua kategori.
5. *Separating Governance from Management*, Cobit 5 merupakan kerangka kerja yang mempunyai hubungan antar manajemen dengan staf teknis dan sejumlah perbedaan yang signifikan dalam struktur organisasi, struktur organisasi, dan tujuan. Enabler adalah faktor- faktor yang secara langsung ataupun tidak langsung menentukan keberhasilan atau tidaknya

COBIT 5 mempunyai lima Domain yang berbeda-beda, antara lain : Domain *Build, Acquire, and Implement* (BAI), *Domain Align, Plan, and Organize* (APO), Domain *Deliver, Service, and Support* (DSS), terakhir Domain *Evaluate, Direct and Monitor* (EDM) dan Domain *Monitor, Evaluate and Assess* (MEA) (M Rizky Astari & Bambang Sugiantoro, 2023).

### **III.6. Analisa Maturity Level**

*Maturity Level* untuk pengelolaan dan kontrol pada proses TI didasarkan pada metode evaluasi organisasi, sehingga dapat mengevaluasi sendiri, mulai dari level tidak ada (0) hingga optimis (5) (Andry et al., 2022). *Maturity Level* digunakan untuk mengidentifikasi peningkatan prioritas dalam suatu organisasi yang hendak dilakukan serta meningkatkan kesadaran pentingnya pengelolaan proses teknologi informasi (Sari, 2021).

Analisa Maturity Level dilakukan untuk penilaian tingkat kematangan atau penerapan proses-proses yang ada dalam domain DSS05. Metode perhitungan maturity level COBIT 5 akan digunakan sebagai tolak ukur dan penilaian sejauh mana penerapan domain dan proses dalam sistem informasi yang ada di Tsiwah Indonesia.

Berikut ini penjelasan yang dikutip dalam buku *Process Assessment Model (PAM)* (ISACA, 2013):

Skala	Maturity Level	
4,51 - 5,00	5	Di optimalisasi
3,51 - 4,50	4	Diatur
2,51 - 3,50	3	Ditetapkan
1,51 - 2,50	2	Dapat Diulang
0,51 - 1,50	1	Inisialisasi
0,00 - 0,50	0	Tidak Ada

*Gambar III.2 Analisa Maturity Levels*

- a. Level 0 *Incompleted Process*, dalam level proses ini perusahaan sama sekali tidak peduli terhadap pentingnya teknologi informasi untuk dikelola secara baik oleh manajemen.
- b. Level 1 *performed Process*, level proses ini perusahaan secara reaktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya.
- c. Level 2 *Managed Process*, Sudah mulai ada prosedur namun tidak seluruhnya terdokumentasi dan tidak seharusnya disosialisasikan kepada pelaksana. Belum ada pelatihan formal untuk mensosialisasikan prosedur tersebut.
- d. Level 3 *Established Process*, Kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan aktivitas sehari-hari.
- e. Level 4 *Predictable Process*, Kondisi dimana perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun objektif terhadap kinerja proses teknologi informasi. Proses diperbaiki terus menerus dan dibandingkan dengan praktik-praktik terbaik.
- f. Level 5 *Optimized Process*, Kondisi dimana perusahaan dianggap telah mengimplementasikan tata kelola manajemen teknologi informasi yang

mengacu pada praktik terbaik. Memudahkan perusahaan untuk beradaptasi terhadap perubahan.

### **III.7. Analisa Kesenjangan (*Gap Analysis*)**

Analisa kesenjangan bertujuan untuk mengidentifikasi perbedaan antara kondisi saat ini dengan kondisi yang diharapkan (Andry et al., 2022). Dalam tata kelola keamanan sistem informasi di Tsirwah Indonesia dengan menggunakan framework COBIT 5. Hal ini membantu dalam menemukan area yang perlu ditingkatkan serta diperbaiki agar sistem dapat lebih sesuai dengan standar COBIT 5.

### **III.8. DDoS (*Distributed Denial of Service*) Attack**

DDoS (*Denial of Service Attack*) adalah sebuah serangan yang melibatkan satu komputer atau satu jaringan. DDoS berfungsi untuk membanjiri salah satu server atau website dengan paket ICMP, TCP, UDP. Serangan ini bertujuan untuk membuat bandwidth server atau web menjadi overload sehingga server atau web tidak bisa lagi menanggulangi trafik yang masuk sampai akhirnya server atau web tersebut Down (Hamdani et al., 2023). Serangan DDoS melibatkan penggunaan sejumlah besar perangkat yang terinfeksi atau dikendalikan oleh penyerang untuk secara bersamaan membanjiri target dengan lalu lintas data, menyebabkan penurunan kinerja atau bahkan kegagalan sistem (Mamuriyah et al., 2024).

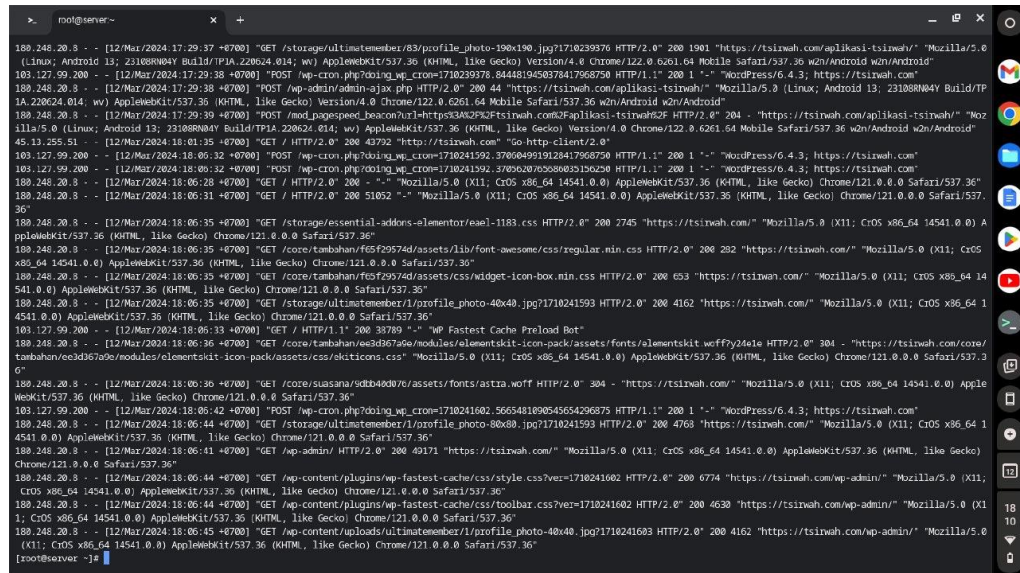
## BAB IV

### PELAKSANAAN PRAKTIK KERJA

#### IV.1. Input

Rencana evaluasi keamanan ini inisiatif dari penulis yang mendengar cerita dari salah satu pengurus Tsirwah yaitu kak Dewi Anggraini selaku Koordinator Divisi Jurnalistik yang mengatakan bahwa telah terjadi serangan siber beberapa waktu lalu. Kemudian penulis bertanya langsung kepada bapak Hafidz Ramdhani selaku Founder Tsirwah untuk melakukan penelitian mengenai evaluasi keamanan pada website Tsirwah Indonesia.

Dalam mempelajari metodologi evaluasi tata kelola sistem informasi yang akan dilakukan, diberikan gambaran mengenai permasalahan DDoS Attack yang terjadi pada tanggal 12 Maret 2024.



```
root@server:~# cat /var/log/nginx/access.log
188.248.20.8 - [12/Mar/2024:17:29:37 +0700] "GET /storage/ultimatember/83/profile_photo-190x190.jpg?1710239370 HTTP/2.0" 200 1901 "https://tsirwah.com/aplikasi-tsirwah/" "Mozilla/5.0 (Linux; Android 13; 2310880M4Y Build/TP1A.220624.014; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/122.0.6261.64 Mobile Safari/537.36 wv/Android wv/Android"
189.127.99.200 - [12/Mar/2024:17:29:38 +0700] "POST /wp-cron.php?doing_wp_cron=1710239378.8444819458378417668750 HTTP/1.1" 200 1 "-" "WordPress/6.4.3; https://tsirwah.com/"
188.248.20.8 - [12/Mar/2024:17:29:38 +0700] "POST /wp-admin/admin-ajax.php HTTP/2.0" 200 44 "https://tsirwah.com/aplikasi-tsirwah/" "Mozilla/5.0 (Linux; Android 13; 2310880M4Y Build/TP1A.220624.014; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/122.0.6261.64 Mobile Safari/537.36 wv/Android wv/Android"
188.248.20.8 - [12/Mar/2024:17:29:39 +0700] "POST /mod_pagespeed_beacon?url=https%3A%2F%2Ftsirwah.com%2Faplikasi-tsirwah%2F HTTP/2.0" 204 - "https://tsirwah.com/aplikasi-tsirwah/" "Mozilla/5.0 (Linux; Android 13; 2310880M4Y Build/TP1A.220624.014; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/122.0.6261.64 Mobile Safari/537.36 wv/Android wv/Android"
46.117.255.51 - [12/Mar/2024:18:01:35 +0700] "GET / HTTP/2.0" 200 43792 "http://tsirwah.com/" "Go-http-client/2.0"
189.127.99.200 - [12/Mar/2024:18:06:32 +0700] "POST /wp-cron.php?doing_wp_cron=1710241592.37080649919128417968750 HTTP/1.1" 200 1 "-" "WordPress/6.4.3; https://tsirwah.com/"
189.127.99.200 - [12/Mar/2024:18:06:32 +0700] "POST /wp-cron.php?doing_wp_cron=1710241592.37080649919128417968750 HTTP/1.1" 200 1 "-" "WordPress/6.4.3; https://tsirwah.com/"
188.248.20.8 - [12/Mar/2024:18:06:28 +0700] "GET / HTTP/2.0" 200 - "-" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:31 +0700] "GET / HTTP/2.0" 200 51052 "-" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:35 +0700] "GET /storage/essential-addons-elementor/ea-el-1183.css HTTP/2.0" 200 2745 "https://tsirwah.com/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:35 +0700] "GET /core/tambahan/f65f29574d/assets/lib/font-awesome/css/regular.min.css HTTP/2.0" 200 282 "https://tsirwah.com/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:35 +0700] "GET /core/tambahan/f65f29574d/assets/css/widget-icon-box.min.css HTTP/2.0" 200 693 "https://tsirwah.com/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:35 +0700] "GET /storage/ultimatember/1/profile_photo-40x40.jpg?1710241593 HTTP/2.0" 200 4162 "https://tsirwah.com/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
189.127.99.200 - [12/Mar/2024:18:06:13 +0700] "GET / HTTP/1.1" 200 38789 "-" "WP Fastest Cache Preload Bot"
188.248.20.8 - [12/Mar/2024:18:06:36 +0700] "GET /core/tambahan/ea3d367a6e/modules/elementskit/icon-pack/assets/fonts/elementskit-woff2y24ele HTTP/2.0" 304 - "https://tsirwah.com/core/tambahan/ea3d367a6e/modules/elementskit/icon-pack/assets/fonts/elementskit-woff2y24ele"
188.248.20.8 - [12/Mar/2024:18:06:36 +0700] "GET /core/suassan/sdb40d07e/assets/fonts/astia.woff HTTP/2.0" 304 - "https://tsirwah.com/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
189.127.99.200 - [12/Mar/2024:18:06:42 +0700] "POST /wp-cron.php?doing_wp_cron=1710241602.5665481890545654296875 HTTP/1.1" 200 1 "-" "WordPress/6.4.3; https://tsirwah.com/"
188.248.20.8 - [12/Mar/2024:18:06:44 +0700] "GET /storage/ultimatember/1/profile_photo-80x80.jpg?1710241593 HTTP/2.0" 200 4768 "https://tsirwah.com/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:41 +0700] "GET /wp-admin/ HTTP/2.0" 200 49171 "https://tsirwah.com/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:44 +0700] "GET /wp-content/plugins/wp-fastest-cache/css/style.css?ver=1710241602 HTTP/2.0" 200 6774 "https://tsirwah.com/wp-admin/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:44 +0700] "GET /wp-content/plugins/wp-fastest-cache/css/toolbar.css?ver=1710241602 HTTP/2.0" 200 4638 "https://tsirwah.com/wp-admin/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
188.248.20.8 - [12/Mar/2024:18:06:45 +0700] "GET /wp-content/uploads/ultimatember/1/profile_photo-40x40.jpg?1710241603 HTTP/2.0" 200 4162 "https://tsirwah.com/wp-admin/" "Mozilla/5.0 (X11; CrOS x86_64 14541.0.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36"
[root@server ~]#
```

Gambar IV.1. Screenshot DDoS Attack

## IV.2. Proses

Selama Kerja Praktik evaluasi tata kelola keamanan di Tsirwah Indonesia, kegiatan dimulai dengan pengenalan lingkungan kerja di Tsirwah Indonesia, melibatkan pemahaman keamanan sistem informasi. Selanjutnya, tahap eksplorasi dilakukan untuk mengidentifikasi permasalahan dan menerapkan evaluasi tata kelola keamanan Tsirwah Indonesia menggunakan *framework* COBIT 5. Hambatan mungkin melibatkan kesulitan menyesuaikan metodologi, atau kesulitan teknis, yang dapat diatasi dengan keterlibatan pemangku kepentingan, penggalian data efektif.

Terakhir, dalam tahap pelaporan hasil kerja evaluasi tata kelola keamanan sistem informasi, kegiatan mencakup penyusunan laporan dengan domain yang sesuai serta kapabilitas level dari keamanan sistem informasi yang ada di Tsirwah Indonesia. Potensi hambatan melibatkan kesulitan menyusun laporan yang jelas, kompleksitas evaluasi. Dengan solusinya adalah menggunakan format laporan terstruktur.

### IV.2.1. Eksplorasi

Tahap eksplorasi dimulai dengan melakukan eksplorasi mengenai metodologi yang akan digunakan dalam evaluasi tata kelola keamanan. Untuk mendukung pelaksanaan metodologi evaluasi tata kelola keamanan, diperlukan pula pengetahuan mengenai *framework* COBIT 5. Dengan demikian, pendalaman terhadap *framework* COBIT 5 pun dilakukan.

Seperti telah disebutkan sebelumnya, untuk melakukan evaluasi keamanan dari sebuah sistem informasi yang telah ada, diperlukan pula pengetahuan mengenai *framework* yang telah dikembangkan tersebut. Dengan demikian dilakukan eksplorasi terhadap *framework* COBIT 5 baik secara Domain maupun secara kapabilitas level. Eksplorasi Domain diperlukan untuk mengetahui Domain mana saja yang cocok untuk kebutuhan evaluasi tata kelola keamanan sistem informasi. Di sisi lain, eksplorasi kapabilitas level perlu dilakukan untuk mengetahui ada ditingkatan mana keamanan sistem informasi tersebut.



#### IV.2.2. Evaluasi Tata Kelola Keamanan Sistem Informasi

Setelah dipelajari lebih lanjut domain COBIT 5 yang cocok untuk tata kelola keamanan sistem informasi di Tsirwah Indonesia menggunakan domain DSS05 yang berfokus untuk mengevaluasi keamanan sistem. Berikut ini beberapa pernyataan dari domain tersebut:

Nama Kontrol	DSS05 Mengelola Layanan Keamanan					
Tujuan Audit	Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional.					
Sub Kontrol	DSS05.01 Melindungi dari malware					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Koordinasi ketika adanya perangkat lunak berbahaya dan menegakan prosedur untuk pencegahan					
2	Adanya alat perlindungan perangkat lunak					
3	Adanya perlindungan perangkat lunak secara terpusat					
4	Adanya evaluasi informasi secara berkala dari potensi ancaman baru					
6	Adanya pelatihan berkala mengenai melware dan penggunaan internet					
Sub kontrol	DSS05.02 Mengelola keamanan jaringan dan konektivitas					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Hanya orang-orang yang diberi otoritas untuk mengakses informasi					
2	Enkripsi informasi yang dikirim sesuai dengan klasifikasinya					
3	Konfigurasikan peralatan jaringan dengan cara yang aman					
4	Terapkan protokol keamanan yang disetujui untuk konektivitas jaringan					
6	Melaksanakan pengujian keamanan sistem secara berkala					
7	Menerapkan mekanisme penyaringan jaringan, seperti firewall					
Sub Kontrol	DSS05.03 Mengelola keamanan titik akhir					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5

1	Mengkonfigurasi sistem operasi dengan cara yang aman					
2	Menerapkan mekanisme penguncian perangkat					
3	Mengenkripsi informasi dalam penyimpanan sesuai dengan klasifikasinya					
4	Mengelola konfigurasi jaringan dengan cara yang aman					
5	Memberikan perlindungan fisik pada perangkat <i>endpoint</i>					
<b>Sub Kontrol</b>	<b>DSS05.04 Mengelola identitas pengguna dan akses logis</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis dan persyaratan proses					
2	Mengelola semua perubahan hak akses					
3	Memisahkan dan mengelola akun pengguna istimewa					
4	Melakukan tinjauan manajemen berkala terhadap semua akun					
5	Meengidentifikasi secara unik semua aktivitas pemrosesan informasi menurut pengguna					
<b>Sub Kontrol</b>	<b>DSS05.05 Mengelola akses fisik ke aset TI</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mengelola permintaan dan pemberian akses					
2	Batasi akses ke situs TI yang sensitif dengan menetapkan batasan perimeter					
3	Profil akses tetap terkini					
<b>Sub Kontrol</b>	<b>DSS05.06 Mengelola dokumen sensitif dan perangkat keluaran</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menetapkan hak akses pada dokumen sensitif					
2	Menetapkan inventaris dokumen sensitif dan perangkat <i>output</i>					
3	Menghancurkan informasi sensitif dan lindungi perangkat <i>output</i>					
4	Menetapkan perlindungan fisik yang tepat terhadap formulir khusus dan perangkat sensitif					
<b>Sub Kontrol</b>	<b>DSS05.07 Memantau infrastruktur untuk Keterangan kejadian terkait keamanan</b>					

No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mencatat peristiwa terkait keamanan yang dilaporkan oleh alat pemantauan keamanan infrastruktur					
2	Tinjau log peristiwa secara berkala untuk mengetahui potensi insiden					

*Tabel IV.1 Lembar Evaluasi Domain DSS 05*

Tabel kuesioner ini lalu diberikan kepada pihak Tsirwah Indonesia untuk diisi oleh pihak-pihak yang memiliki pemahaman mengenai keamanan sistem informasi di Tsirwah Indonesia.

#### **IV.2.3. Pelaporan Hasil Kerja Praktik**

Proses pelaporan hasil kerja praktek dilakukan pada tahap akhir kerja praktik di Tsirwah Indonesia. Pelaporan hasil kerja praktek dilakukan dengan presentasi dihadapan penguji kampus. Pelaporan hasil kerja praktik dilakukan pula dengan laporan kerja praktik.

### **IV.3. Pencapaian Hasil**

Adapun hasil yang dicapai dari kerja praktik di Tsirwah Indonesia ini berupa evaluasi tata kelola keamanan sistem informasi. Evaluasi tata kelola keamanan sistem informasi ini menggunakan *framework* COBIT 5 dengan domain DSS05 (*Manage Security* / Mengelola Layanan Keamanan).

#### **IV.3.1. Analisa Tingkat Kematangan**

Dari hasil jawaban kuisisioner narasumber di Tsirwah Indonesia yang diperoleh saat melakukan analisis tersebut. Analisis yang dilakukan pada tahap ini adalah untuk menilai tingkat kematangan tata kelola sistem informasi saat ini, akan tersedia jawaban dengan nilai 0-5 (Ishlahuddin, 2020). Berikut rumus untuk menghitung tingkat kematangan:

$$\text{Tingkat Kematangan Atribut} = \frac{\sum \text{bobot jawaban kuisisioner}}{\text{Jumlah Responden}}$$

*Gambar IV.2. Rumus Perhitungan Kuesioner*

### 1. Tingkat Kematangan Subdomain DSS05.01

Tingkat rata-rata kematangan pada subdomain DSS05.01 yang telah dicapai oleh Tsirwah indonesia telah tertuang dalam tabel berikut:

Subdomain	No	Tingkat Persetujuan				Current Maturity	Nilai Rata-rata
		R1	R2	R3	R4		
DSS05.01	1	5	5	4	4	4,50	3,75
	2	4	3	3	3	3,25	
	3	4	4	5	4	4,25	
	4	3	4	3	3	3,25	
	5	4	4	3	3	3,50	

*Tabel IV.2. Tingkat Kematangan Subdomain DSS05.01*

Dalam subdomain “DSS05.01 *Protect against malware*” terdapat 5 buah pernyataan dan ada 4 orang responden menghasilkan nilai rata-rata 3,75.

### 2. Tingkat Kematangan Subdomain DSS05.02

Tingkat rata-rata kematangan pada subdomain DSS05.02 yang telah dicapai oleh Tsirwah indonesia telah tertuang dalam tabel berikut

Subdomain	No	Tingkat Persetujuan				Current Maturity	Nilai Rata-rata
		R1	R2	R3	R4		
DSS05.02	1	5	5	4	5	4,75	3,85
	2	4	4	4	4	4,00	
	3	4	3	3	3	3,25	
	4	3	3	3	4	3,25	
	5	4	4	4	4	4,00	

*Tabel IV.3. Tingkat Kematangan Subdomain DSS05.02*

Dalam subdomain “DSS05.02 *Manage network and connectivity security*” terdapat 5 buah pernyataan dan ada 4 orang responden menghasilkan nilai rata-rata 3,85.

### 3. Tingkat Kematangan Subdomain DSS05.03

Tingkat rata-rata kematangan pada subdomain DSS05.03 yang telah dicapai oleh Tsirwah indonesia telah tertuang dalam tabel berikut:

Subdomain	No	Tingkat Persetujuan				Current Maturity	Nilai Rata-rata
		R1	R2	R3	R4		
DSS05.03	1	5	4	3	4	4,00	3,96
	2	4	4	4	4	4,00	
	3	4	4	3	3	3,50	
	4	3	4	4	4	3,75	
	5	5	5	4	4	4,50	
	6	5	5	3	3	4,00	

*Tabel IV.4. Tingkat Kematangan Subdomain DSS05.03*

Dalam subdomain “DSS05.03 *Manage endpoint security*” terdapat 6 buah pernyataan dan ada 4 orang responden menghasilkan nilai rata-rata 4,04.

#### 4. Tingkat Kematangan Subdomain DSS05.04

Tingkat rata-rata kematangan pada subdomain DSS05.04 yang telah dicapai oleh Tsirwah indonesia telah tertuang dalam tabel berikut:

Subdomain	No	Tingkat Persetujuan				Current Maturity	Nilai Rata-rata
		R1	R2	R3	R4		
DSS05.04	1	4	4	5	4	4,25	4,20
	2	5	4	4	4	4,25	
	3	4	5	5	5	4,75	
	4	4	4	3	3	3,50	
	5	5	4	4	4	4,25	

*Tabel IV.5. Tingkat Kematangan Subdomain DSS05.04*

Dalam subdomain “DSS05.04 *Manage user identity and logical access*” terdapat 5 buah pernyataan dan ada 4 orang responden menghasilkan nilai rata-rata 4,20.

#### 5. Tingkat Kematangan Subdomain DSS05.05

Tingkat rata-rata kematangan pada subdomain DSS05.05 yang telah dicapai oleh Tsirwah indonesia telah tertuang dalam tabel berikut:

Subdomain	No	Tingkat Persetujuan				Current Maturity	Nilai Rata-rata
		R1	R2	R3	R4		
DSS05.05	1	5	5	4	5	4,75	4,42

	2	5	4	4	4	4,25	
	3	4	5	4	4	4,25	

*Tabel IV.6. Tingkat Kematangan Subdomain DSS05.05*

Dalam subdomain “DSS05.05 *Manage physical access to IT assets*” terdapat 3 buah pernyataan dan ada 4 orang responden menghasilkan nilai rata-rata 4,42.

6. Tingkat Kematangan Subdomain DSS05.06

Tingkat rata-rata kematangan pada subdomain DSS05.06 yang telah dicapai oleh Tsirwah indonesia telah tertuang dalam tabel berikut:

Subdomain	No	Tingkat Persetujuan				Current Maturity	Nilai Rata-rata
		R1	R2	R3	R4		
DSS05.06	1	5	5	5	4	4,75	4,19
	2	5	4	4	4	4,25	
	3	4	5	4	4	4,25	
	4	4	4	3	3	3,50	

*Tabel IV.7. Tingkat Kematangan Subdomain DSS05.06*

Dalam subdomain “DSS05.06 *Manage sensitive documents and output devices*” terdapat 4 buah pernyataan dan ada 4 orang responden menghasilkan nilai rata-rata 4,19.

7. Tingkat Kematangan Subdomain DSS05.07

Tingkat rata-rata kematangan pada subdomain DSS05.07 yang telah dicapai oleh Tsirwah indonesia telah tertuang dalam tabel berikut:

Subdomain	No	Tingkat Persetujuan				Current Maturity	Nilai Rata-rata
		R1	R2	R4	R4		
DSS05.07	1	5	4	4	3	4,00	3,88
	2	4	4	3	4	3,75	

*Tabel IV.8. Tingkat Kematangan Subdomain DSS05.07*

Dalam subdomain “DSS05.07 *Monitor the infrastructure for security-related events*” terdapat 2 buah pernyataan dan ada 4 orang responden menghasilkan nilai rata-rata 3,88.

### IV.3.2. Ringkasan Tingkat Kematangan Domain DSS05

Ringkasan tingkat kematangan domain DSS05 dapat dilihat dari tabel dibawah ini:

Domain	Subdomain	Keterangan	Maturity Score	Keterangan
DSS05	DSS05.01	Protect against malware	3,75	3 - Established
	DSS05.02	Manage network and connectivity security	3,85	3 - Established
	DSS05.03	Manage endpoint security	3,96	3 - Established
	DSS05.04	Manage user identity and logical access	4,20	4 - Predictable
	DSS05.05	Manage physical access to IT assets	4,42	4 - Predictable
	DSS05.06	Manage sensitive documents and output devices	4,19	4 - Predictable
	DSS05.07	Monitor the infrastructure for security-related events	3,88	3 - Established

*Tabel IV.9. Ringkasan Tingkat Kematangan*

Jadi, tingkat kematangan COBIT 5 untuk masing-masing subdomain adalah sebagai berikut:

- Tingkat Kematangan 3 (Established): DSS05.01, DSS05.02, DSS05.03, DSS05.07
- Tingkat Kematangan 4 (Predictable): DSS05.03, DSS05.04, DSS05.05.

Berdasarkan tingkat kematangan COBIT 5, masing-masing sub domain memiliki tingkat kematangan yang berbeda, dapat dideskripsikan sebagai berikut:

1. Domain “DSS05.03 *Manage endpoint security*”, “DSS05.04 *Manage user identity and logical access*”, “DSS05.05 *Manage physical access to IT assets*” berada ditingkat kematangan 4 (Predictable). Pada tingkat ini, proses TI sudah mulai terstruktur dengan baik. Organisasi memiliki kebijakan dan prosedur yang jelas untuk mengelola TI. Proses-proses yang ada sudah terdokumentasi, tim TI memahami peran dan tanggung jawab mereka dan ada pelatihan untuk staf agar bisa menjalankan proses dengan baik.

Domain “DSS05.01 *Protect against malware*”, “DSS05.02 *Manage network and connectivity security*”, “DSS05.06 *Manage sensitive documents and output devices*” dan “DSS05.07 *Monitor the infrastructure for security-related events*”

berada ditingkatan kematangan 3 (Established). Kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan aktivitas sehari-hari. Pada tingkat ini, proses TI tidak hanya terstruktur, tetapi juga bisa diprediksi dan diukur. Artinya, organisasi dapat memperkirakan hasil dan kinerja dari proses yang dijalankan. Proses-proses dapat diukur dengan metrik yang jelas, ada analisis untuk meningkatkan efektivitas dan efisiensi dan tim dapat merencanakan dan mengantisipasi masalah yang mungkin muncul.

Secara Keseluruhan, analisis Maturity Level menunjukkan bahwa beberapa subdomain telah mencapai kematangan yang telah ditahap yang diharapkan (Tingkat Kematangan 4), meskipun sementara yang lainnya masih memerlukan peningkatan dan perbaikan (Tingkat Kematangan 3). Ini berarti Tsirwah telah mencapai tingkat prediktabilitas yang cukup tinggi dalam mengelola akses fisik ke akses IT, mengelola dokumen sensitif dan perangkat keluaran serta mengelola identitas pengguna dan akses logis.

#### IV.3.3. Analisis Kesenjangan (GAP Analysis)

Gap adalah jarak antara tingkat kapabilitas dengan tingkat yang diharapkan, untuk membandingkan tingkat kapabilitas yang diperoleh dengan tingkat yang diharapkan (Andry et al., 2022). Berikut ini tabel analisis kesenjangan:

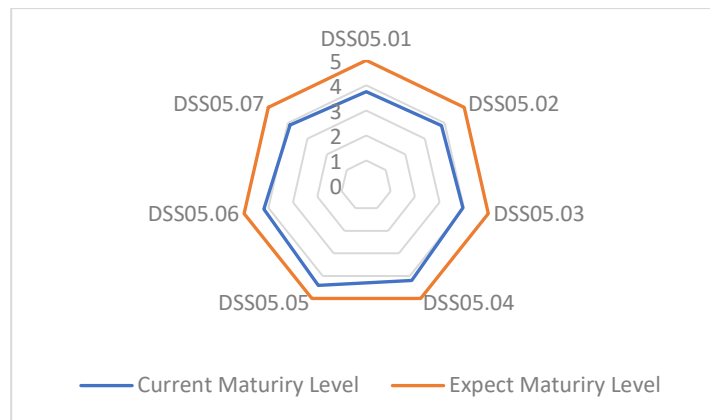
Domain	Subdomain	Current Maturity	Expect Maturity	Gap
DSS05	DSS05.01	3,75	5	1,25
	DSS05.02	3,85	5	1,15
	DSS05.03	3,96	5	1,04
	DSS05.04	4,2	5	0,8
	DSS05.05	4,42	5	0,58
	DSS05.06	4,19	5	0,81
	DSS05.07	3,88	5	1,12

*Tabel IV.10. Analisis Kesenjangan (GAP Analysis)*

Dari tabel dapat dilihat bahwa tingkat kematangan saat ini (*current maturity*) untuk setiap proses yang ada pada subdomain DSS05.01, DSS05.02, DSS05.03,



DSS05.04, DSS05.05, DSS05.06 dan DSS05.07 rata-rata berada disekitar level 3 (Established) dengan target pengelolaan TI berada pada level 5 (optimizing). Hal ini dapat dikatakan bahwa perusahaan telah memiliki sejumlah indikator yang dijadikan sebagai sasaran maupun objektif terhadap kinerja proses teknologi informasi.



*Gambar IV.3. Grafik Analisis Kesenjangan*

Dari gambar grafik IV.3 terlihat jelas bahwa terdapat kesenjangan (gap) antara nilai kematangan saat ini dengan nilai kematangan yang diharapkan. Dengan adanya kesenjangan (gap) tersebut di butuhkan rekomendasi agar nilai maturity level dapat meningkat sesuai dengan tingkat kematangan yang diharapkan.

#### **IV.3.4. Rekomendasi**

Setelah Maturity Level ditetapkan, maka akan dilakukan proses penyusunan rekomendasi. Rekomendasi yang dapat diberikan untuk meningkatkan tata kelola keamanan sistem informasi di Tsirwah Indonesia:

1. Melindungi dari Malware (DSS05.01): Pastikan setiap komputer/laptop yang digunakan untuk selalu melakukan pemindaian virus secara berkala, perbaharui antivirus yang digunakan untuk melindungi data-data dan informasi yang ada di Tsirwah Indonesia. Selain perlunya pelatihan minimal 1 atau 2 kali setiap tahun untuk tim IT agar dapat menjalankan dan mengikuti perkembangan teknologi informasi.

2. Mengelola keamanan jaringan dan konektivitas (DSS05.02): Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi melalui semua metode konektivitas, memastikan bahwa data yang diterima dan dikirim melalui jaringan akses yang aman.
3. Mengelola keamanan *endpoint* (DSS05.03): Pastikan bahwa semua *endpoint*, seperti laptop, desktop, server, dan perangkat mobile atau jaringan lainnya, diamankan sesuai dengan persyaratan keamanan dan privasi yang ditetapkan untuk informasi yang diproses, disimpan, atau dikirim.
4. Mengelola identitas pengguna dan akses logis (DSS05.04): Pastikan semua pengguna memiliki hak akses sesuai dengan kebijakan privasi dan kebutuhan bisnis. Koordinasikan dengan unit yang mengelola hak akses di Tsirwah Indonesia. Implementasikan prosedur standar untuk identifikasi, otentikasi dan otorisasi pengguna, serta lakukan pemantauan dan peninjauan akses secara berkala untuk memastikan kepatuhan dan keamanan.
5. Mengelola akses fisik ke aset TI (DSS05.05): Pastikan memilih layanan server yang aman dan terpercaya agar data-data serta informasi yang ada di Tsirwah Indonesia tetap aman. Pastikan yang bisa akses ke server hanya pihak-pihak tertentu saja. Jika ada pihak lain buatlah catatan khusus.
6. Mengelola dokumen sensitif dan perangkat keluaran (DSS05.06): Pastikan dokumen sensitif seperti formulir pendaftaran santri dan peserta pelatihan menulis. Pastikan hanya pihak-pihak yang terkait yang dapat mengakses dokumen tersebut.
7. Memantau infrastruktur untuk kejadian terkait keamanan (DSS05.07): Gunakan berbagai alat dan teknologi, seperti alat deteksi intrusi, untuk mengelola kerentanan dan memantau infrastruktur terhadap akses yang tidak sah. Pastikan bahwa alat, teknologi dan deteksi keamanan terintegrasi dengan pemantauan umum dan manajemen insiden.

## **BAB V**

### **PENUTUP**

#### **V.1. Kesimpulan dan saran mengenai pelaksanaan**

Berdasarkan penjelasan pada bab-bab sebelumnya maka dapat ditarik kesimpulan:

##### **V.1.1. Kesimpulan Pelaksanaan Kerja praktik**

1. Mahasiswa dapat mengaplikasikan ilmu yang diperoleh selama perkuliahan untuk menyelesaikan permasalahan di dunia nyata.
2. Mahasiswa dapat mengetahui ilmu dan keterampilan yang dibutuhkan untuk memasuki dunia kerja di era globalisasi, seperti:
  - a. Keterampilan berkomunikasi dan bekerja sama dengan orang lain.
  - b. Ilmu dasar mengenai bidang spesifik yang diperoleh selama perkuliahan. Misalnya ilmu dasar di bidang informatika, ilmu dasar di bidang ekonomi, dan sebagainya.
  - c. Keterampilan menganalisis permasalahan untuk dicari solusinya.
  - d. Ilmu pengetahuan umum.
  - e. Keterampilan mempelajari hal yang baru dalam waktu relatif singkat.
3. Mahasiswa menyadari pentingnya etos kerja yang baik, disiplin dan tanggung jawab dalam menyelesaikan suatu pekerjaan.
4. Mahasiswa memperoleh tambahan ilmu yang tidak diperoleh di proses perkuliahan. Pada kerja praktik yang dilakukan di Tsirwah Indonesia, mahasiswa mendapatkan pengetahuan tambahan pengetahuan di bidang Jurnalistik dan juga evaluasi tata kelola menggunakan framework COBIT 5 lebih luas lagi.

##### **V.1.2. Saran Pelaksanaan Kerja praktik**

Adapun saran mengenai pelaksanaan kerja praktik antara lain:

1. Perlu ditumbuhkan kebiasaan belajar secara mandiri (*self learning*) di kalangan mahasiswa, khususnya dalam mempelajari teknologi secara aplikatif. Salah satu fasilitas yang tersedia yang mendukung proses pembelajaran secara mandiri ini adalah koneksi internet yang cukup cepat.

2. Perlu adanya bimbingan secara lebih intensif bagi mahasiswa kerja praktik.
3. Jika memungkinkan, dalam pelaksanaan kerja praktek mahasiswa dapat dilibatkan dalam suatu proyek di mana mahasiswa dapat bekerja sama dengan pegawai lain.

## **V.2. Kesimpulan dan saran mengenai substansi**

Berikut kesimpulan dan saran mengenai substansi yang diamati selama kerja praktik di Tsirwah Indonesia:

### **V.2.1. Kesimpulan**

Setelah melalui proses Evaluasi Tata Kelola Keamanan Menggunakan *Framework* COBIT 5 di Tsirwah Indonesia, kesimpulan yang didapat sebagai berikut:

1. Evaluasi tata kelola keamanan sistem informasi di Tsirwah Indonesia menunjukkan tingkat kematangan bervariasi pada domain DSS05. Sebagian besar subdomain berada pada tingkat kematangan 3 (Established) dan beberapa mencapai tingkat 4 (Predictable), menunjukkan pengelolaan yang cukup baik, tetapi masih memerlukan peningkatan untuk mencapai tingkat kematangan optimal (5).
2. Terdapat gap antara tingkat kematangan saat ini dengan tingkat yang diharapkan. Hal ini menunjukkan kebutuhan akan peningkatan proses dan sistem untuk memenuhi standar terbaik.

### **V.2.1. Saran**

Setelah hasil Evaluasi Tata Kelola Keamanan Menggunakan *Framework* COBIT 5 di Tsirwah Indonesia, saran yang diajukan sebagai berikut:

1. Adanya tahapan lanjutan untuk mengevaluasi tata kelola di Tsirwah Indonesia baik sisi keamanan, pengelolaan layanan, proses pengembangan sistem dan sisi lainnya yang perlu dievaluasi.
2. Menyebarluaskan kuisioner kepada pengguna dan pemangku kepentingan terkait untuk mendapatkan umpan balik langsung terkait pengalaman

mereka dengan Sistem Informasi dan *framework* COBIT 5. Ini dapat memberikan wawasan lebih lanjut tentang kebutuhan pengguna, serta mengidentifikasi area di mana perbaikan atau peningkatan dibutuhkan.

## DAFTAR PUSTAKA

- Andry, J. F., Lee, F. S., Darma, W., Rosadi, P., & Ekklesia, R. (2022). Audit Sistem Informasi Menggunakan Cobit 5 Pada Perusahaan Penyedia Layanan Internet. *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi*, 8(1), 17. <https://doi.org/10.24014/rmsi.v8i1.14761>
- Doharma, R., Prawoto, A. A., & Andry, J. F. (2021). Audit Sistem Informasi Menggunakan Framework Cobit 5 (Studi Kasus: Pt Media Cetak). *JBASE - Journal of Business and Audit Information Systems*, 4(1). <https://doi.org/10.30813/jbase.v4i1.2730>
- Hamdani, F., Bella Fitriana, Y., & Oper, N. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST). *Media Online*, 3(6), 1296–1302. <https://doi.org/10.30865/klik.v3i6.830>
- ISACA. (2012). COBIT 5: Enabling Processes, ISBN 978-1-60420-250-2. In *Cobit 5*.
- ISACA. (2013). *Process Assessment Model (PAM): Using COBIT 5 of Enterprise IT*. <http://linkd.in/ISACAOOfficial>
- Ishlahuddin, A. (2020). *Analisis Tingkat Kematangan Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 : Studi Kasus Sekolah Tinggi XYZ*. 5, 33–44.
- Lediwara, N. (2020). Analisis IT Governance Menggunakan Framework Cobit 5 Domain DSS, MEA dan BAI. *Pseudocode*, 7(2), 97–104. <https://doi.org/10.33369/pseudocode.7.2.97-104>
- M Rizky Astari, & Bambang Sugiantoro. (2023). Evaluasi sistem informasi pondok pesantren sabilul hasanah banyuasin menggunakan framework cobit 5 domain deliver, service, and support. *INFOTECH : Jurnal Informatika & Teknologi*, 4(1), 1–15. <https://doi.org/10.37373/infotech.v4i1.416>
- Mamuriyah, N., Prasetyo, S. E., & Sijabat, A. O. (2024). Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, 6(1), 162–167. <https://doi.org/10.47233/jteksis.v6i1.1124>
- Saputera, S. A., Sunardi, D., Syafrizal, A., & Samsidi, P. (2020). Evaluasi Sistem Informasi Akademik Menggunakan Metode Mccall. *Journal of Technopreneurship and Information System (JTIS)*, 3(2), 9–16. <https://doi.org/10.36085/jtis.v3i2.878>
- Sari, N. L. (2021). Pengukuran Maturity Level Cobit 5 Dan Domain Dss (Deliver, Service, and Support) Pada Regulasi Sandbox Ojk Klaster Aggregator. *JATISI*

(*Jurnal Teknik Informatika Dan Sistem Informasi*), 8(2), 561–572.  
<https://doi.org/10.35957/jatisi.v8i2.843>

Sofa, K., Suryanto, T. L. M., & Suryono, R. R. (2020). Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 5 Pada Dinas Pekerjaan Umum Kabupaten Tanggamus. *Jurnal Teknologi Dan Sistem Informasi*, 1(1), 39–46.  
<https://doi.org/10.33365/jtsi.v1i1.50>

Waruwu, G., & Sundari, J. (2024). Audit Teknologi Informasi Menggunakan Cobit 5 Studi Kasus PT. Global Network Dharma Jaya. *Infomatek*, 26(1), 69–74.  
<https://doi.org/10.23969/infomatek.v26i1.13333>

Wijaya, S. S. H., & Aziz, R. . A. (2019). Audit Sistem Informasi Pada Lampung Post Menggunakan Metode Framework COBIT 5. *Jurnal Informatika*, 19(2), 116–126.

**LAMPIRAN A**  
**BERITA ACARA WAWANCARA**

Hari/Tanggal : Sabtu, 26 November 2024

Jam : 20.00 WIB

Narasumber : Hafidz Ramdhani (Founder Tsirwah Indonesia)

Media : Google Meet

Pertanyaan	Jawaban
1. Masalah apa saja yang pernah terjadi di Tsirwah Indonesia	1. Belum lama ini kami mendapatkan serangan siber berupa DdoS Attack pada tanggal 12 Maret 2024, akibatnya pengguna tidak dapat mengakses website Tsirwah sehingga aktivitas di Tsirwah Indonesia di nonaktifkan terlebih dahulu. Alhamdulillah atas izin Allah, kami bisa menanggapi website dan membuka kembali aktivitas setelah selesai libur lebaran.
2. Berapa lama waktu untuk pemulihan dari serangan cyber tersebut?	2. itu saya lupa sih mas, tapi kalau salah gak lebih dari 5 hari mas.
3. Sudah orang lain yang melakukan penelitian di Tsirwah Indonesia?	3. Kalau untuk penelitian belum ada, tapi kalau untuk liputan pernah. Liputan tentang Hari Santri Nasional, kami diliput oleh platform Antara News

Pewawancara

Hanif Ibrahim

Narasumber



Hafidz Ramdhani



Minggu, Oktober 21, 2024

Tampilkan Tampilan Sesi dan Sesi Lain

**APLIKASI PESANTREN DIGITAL**  
SUPER LENGKAP  
for You!

ALUMNUS & INDORE

PERHIMPUNAN & KELUARGA

SARAF KEMAHANTHAN

GASTI TAMPILAN

ARTIKEL TERBARU

ARTIKEL TERBARU

media sedang melakukan presentasi

Dennis

Havidz

Anda

media 2 lainnya

**LAMPIRAN B**  
**LEMBAR KERJA EVALUASI DOMAIN DSS 05**  
**TSIRWAH INDONESIA**

Narasumber : Hendry Yoga  
 Jabatan : Tim IT Tsirwah  
 Pilih Tingkat Persetujuan :

1. Sangat Tidak Setuju
2. Tidak Setuju
3. Cukup Setuju
4. Setuju
5. Sangat Setuju

Nama Kontrol	DSS05 Mengelola Layanan Keamanan					
Tujuan Audit	Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional.					
Sub Kontrol	DSS05.01 Melindungi dari malware					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Koordinasi ketika adanya perangkat lunak berbahaya dan menegakan prosedur untuk pencegahan					X
2	Adanya alat perlindungan perangkat lunak				X	
3	Adanya perlindungan perangkat lunak secara terpusat				X	
4	Adanya evaluasi informasi secara berkala dari potensi ancaman baru			X		
6	Adanya pelatihan berkala mengenai melware dan penggunaan internet				X	
Sub kontrol	DSS05.02 Mengelola keamanan jaringan dan konektivitas					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Hanya orang-orang yang diberi otoritas untuk mengakses informasi					X
2	Enkripsi informasi yang dikirim sesuai dengan klasifikasinya				X	
3	Konfigurasikan peralatan jaringan dengan cara yang aman				X	
4	Terapkan protokol keamanan yang disetujui untuk konektivitas jaringan			X		

5	Menerapkan mekanisme penyaringan jaringan, seperti firewall				X	
<b>Sub Kontrol</b>	<b>DSS05.03 Mengelola keamanan titik akhir</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman					X
2	Terapkan mekanisme penguncian perangkat				X	
3	Enkripsi informasi dalam penyimpanan sesuai dengan klasifikasinya				X	
4	Kelola konfigurasi jaringan dengan cara yang aman			X		
5	Melindungi integritas sistem					x
6	Memberikan perlindungan fisik pada perangkat <i>endpoint</i>					x
<b>Sub Kontrol</b>	<b>DSS05.04 Mengelola identitas pengguna dan akses logis</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis dan persyaratan proses				X	
2	Mengelola semua perubahan hak akses					X
3	Memisahkan dan mengelola akun pengguna istimewa				X	
4	Melakukan tinjauan manajemen berkala terhadap semua akun				X	
5	Meengidentifikasi secara unik semua aktivitas pemrosesan informasi menurut pengguna					X
<b>Sub Kontrol</b>	<b>DSS05.05 Mengelola akses fisik ke aset TI</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mengelola permintaan dan pemberian akses				X	
2	Batasi akses ke situs TI yang sensitif dengan menetapkan batasan perimeter					X
3	Profil akses tetap terkini					X
<b>Sub Kontrol</b>	<b>DSS05.06 Mengelola dokumen sensitif dan perangkat keluaran</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menetapkan hak akses pada dokumen sensitif					X
2	Menetapkan inventaris dokumen sensitif dan perangkat <i>output</i>					X

3	Hancurkan informasi sensitif dan lindungi perangkat <i>output</i>				X	
4	Tetapkan perlindungan fisik yang tepat terhadap formulir khusus dan perangkat sensitif				X	
<b>Sub Kontrol</b>	<b>DSS05.07 Memantau infrastruktur untuk Keterangan kejadian terkait keamanan</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mencatat peristiwa terkait keamanan yang dilaporkan oleh alat pemantauan keamanan infrastruktur					X
2	Tinjau log peristiwa secara berkala untuk mengetahui potensi insiden				X	

**LEMBAR KERJA EVALUASI DOMAIN DSS 05**  
**TSIRWAH INDONESIA**

Narasumber : Dimas Surya  
 Jabatan : Koor. Divisi IT  
 Pilih Tingkat Persetujuan :

1. Sangat Tidak Setuju
2. Tidak Setuju
3. Cukup Setuju
4. Setuju
5. Sangat Setuju

Nama Kontrol	DSS05 Mengelola Layanan Keamanan					
Tujuan Audit	Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional.					
Sub Kontrol	DSS05.01 Melindungi dari malware					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Koordinasi ketika adanya perangkat lunak berbahaya dan menegakan prosedur untuk pencegahan					X
2	Adanya alat perlindungan perangkat lunak			X		
3	Adanya perlindungan perangkat lunak secara terpusat				X	
4	Adanya evaluasi informasi secara berkala dari potensi ancaman baru				X	
6	Adanya pelatihan berkala mengenai melware dan penggunaan internet				X	
Sub kontrol	DSS05.02 Mengelola keamanan jaringan dan konektivitas					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Hanya orang-orang yang diberi otoritas untuk mengakses informasi					X
2	Enkripsi informasi yang dikirim sesuai dengan klasifikasinya				X	
3	Konfigurasikan peralatan jaringan dengan cara yang aman			X		
4	Terapkan protokol keamanan yang disetujui untuk konektivitas jaringan			X		

5	Menerapkan mekanisme penyaringan jaringan, seperti firewall				X	
<b>Sub Kontrol</b>	<b>DSS05.03 Mengelola keamanan titik akhir</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman				X	
2	Terapkan mekanisme penguncian perangkat				X	
3	Enkripsi informasi dalam penyimpanan sesuai dengan klasifikasinya				X	
4	Kelola konfigurasi jaringan dengan cara yang aman				X	
5	Melindungi integritas sistem					X
6	Memberikan perlindungan fisik pada perangkat <i>endpoint</i>					X
<b>Sub Kontrol</b>	<b>DSS05.04 Mengelola identitas pengguna dan akses logis</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis dan persyaratan proses				X	
2	Mengelola semua perubahan hak akses				X	
3	Memisahkan dan mengelola akun pengguna istimewa					X
4	Melakukan tinjauan manajemen berkala terhadap semua akun				X	
5	Meengidentifikasi secara unik semua aktivitas pemrosesan informasi menurut pengguna				X	
<b>Sub Kontrol</b>	<b>DSS05.05 Mengelola akses fisik ke aset TI</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mengelola permintaan dan pemberian akses					X
2	Batasi akses ke situs TI yang sensitif dengan menetapkan batasan perimeter				X	
3	Profil akses tetap terkini					X
<b>Sub Kontrol</b>	<b>DSS05.06 Mengelola dokumen sensitif dan perangkat keluaran</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menetapkan hak akses pada dokumen sensitif					X
2	Menetapkan inventaris dokumen sensitif dan perangkat <i>output</i>				X	

3	Hancurkan informasi sensitif dan lindungi perangkat <i>output</i>					X
4	Tetapkan perlindungan fisik yang tepat terhadap formulir khusus dan perangkat sensitif				X	
<b>Sub Kontrol</b>	<b>DSS05.07 Memantau infrastruktur untuk Keterangan kejadian terkait keamanan</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mencatat peristiwa terkait keamanan yang dilaporkan oleh alat pemantauan keamanan infrastruktur				X	
2	Tinjau log peristiwa secara berkala untuk mengetahui potensi insiden				X	

## LEMBAR KERJA EVALUASI DOMAIN DSS 05

### TSIRWAH INDONESIA

Narasumber : Daniel  
Jabatan : Tim IT Tsirwah  
Pilih Tingkat Persetujuan :

6. Sangat Tidak Setuju
7. Tidak Setuju
8. Cukup Setuju
9. Setuju
10. Sangat Setuju

Nama Kontrol	DSS05 Mengelola Layanan Keamanan					
Tujuan Audit	Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional.					
Sub Kontrol	DSS05.01 Melindungi dari malware					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Koordinasi ketika adanya perangkat lunak berbahaya dan menegakan prosedur untuk pencegahan				X	
2	Adanya alat perlindungan perangkat lunak			X		
3	Adanya perlindungan perangkat lunak secara terpusat				X	
4	Adanya evaluasi informasi secara berkala dari potensi ancaman baru			X		
6	Adanya pelatihan berkala mengenai malware dan penggunaan internet			X		
Sub kontrol	DSS05.02 Mengelola keamanan jaringan dan konektivitas					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Hanya orang-orang yang diberi otoritas untuk mengakses informasi					X
2	Enkripsi informasi yang dikirim sesuai dengan klasifikasinya				X	
3	Konfigurasi peralatan jaringan dengan cara yang aman			X		
4	Terapkan protokol keamanan yang disetujui untuk konektivitas jaringan				X	



5	Menerapkan mekanisme penyaringan jaringan, seperti firewall				X	
<b>Sub Kontrol</b>	<b>DSS05.03 Mengelola keamanan titik akhir</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman				X	
2	Terapkan mekanisme penguncian perangkat				X	
3	Enkripsi informasi dalam penyimpanan sesuai dengan klasifikasinya			X		
4	Kelola konfigurasi jaringan dengan cara yang aman				X	
5	Melindungi integritas sistem				X	
6	Memberikan perlindungan fisik pada perangkat <i>endpoint</i>			X		
<b>Sub Kontrol</b>	<b>DSS05.04 Mengelola identitas pengguna dan akses logis</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis dan persyaratan proses				X	
2	Mengelola semua perubahan hak akses				X	
3	Memisahkan dan mengelola akun pengguna istimewa					X
4	Melakukan tinjauan manajemen berkala terhadap semua akun			X		
5	Meengidentifikasi secara unik semua aktivitas pemrosesan informasi menurut pengguna				X	
<b>Sub Kontrol</b>	<b>DSS05.05 Mengelola akses fisik ke aset TI</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mengelola permintaan dan pemberian akses					X
2	Batasi akses ke situs TI yang sensitif dengan menetapkan batasan perimeter				X	
3	Profil akses tetap terkini				X	
<b>Sub Kontrol</b>	<b>DSS05.06 Mengelola dokumen sensitif dan perangkat keluaran</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menetapkan hak akses pada dokumen sensitif				X	
2	Menetapkan inventaris dokumen sensitif dan perangkat <i>output</i>				X	

3	Hancurkan informasi sensitif dan lindungi perangkat <i>output</i>				X	
4	Tetapkan perlindungan fisik yang tepat terhadap formulir khusus dan perangkat sensitif			X		
<b>Sub Kontrol</b>	<b>DSS05.07 Memantau infrastruktur untuk Keterangan kejadian terkait keamanan</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mencatat peristiwa terkait keamanan yang dilaporkan oleh alat pemantauan keamanan infrastruktur			X		
2	Tinjau log peristiwa secara berkala untuk mengetahui potensi insiden				X	

**LEMBAR KERJA EVALUASI DOMAIN DSS 05**  
**TSIRWAH INDONESIA**

Narasumber : Dion  
 Jabatan : Tim IT Tsirwah  
 Pilih Tingkat Persetujuan :

1. Sangat Tidak Setuju
2. Tidak Setuju
3. Cukup Setuju
4. Setuju
5. Sangat Setuju

Nama Kontrol	DSS05 Mengelola Layanan Keamanan					
Tujuan Audit	Minimalkan dampak bisnis dari kerentanan dan insiden keamanan informasi operasional.					
Sub Kontrol	DSS05.01 Melindungi dari malware					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Koordinasi ketika adanya perangkat lunak berbahaya dan menegakan prosedur untuk pencegahan					X
2	Adanya alat perlindungan perangkat lunak				X	
3	Adanya perlindungan perangkat lunak secara terpusat				X	
4	Adanya evaluasi informasi secara berkala dari potensi ancaman baru			X		
6	Adanya pelatihan berkala mengenai malware dan penggunaan internet				X	
Sub kontrol	DSS05.02 Mengelola keamanan jaringan dan konektivitas					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Hanya orang-orang yang diberi otoritas untuk mengakses informasi					X
2	Enkripsi informasi yang dikirim sesuai dengan klasifikasinya				X	
3	Konfigurasikan peralatan jaringan dengan cara yang aman				X	
4	Terapkan protokol keamanan yang disetujui untuk konektivitas jaringan			X		

5	Menerapkan mekanisme penyaringan jaringan, seperti firewall				X	
<b>Sub Kontrol</b>	<b>DSS05.03 Mengelola keamanan titik akhir</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Konfigurasi sistem operasi dengan cara yang aman					X
2	Terapkan mekanisme penguncian perangkat				X	
3	Enkripsi informasi dalam penyimpanan sesuai dengan klasifikasinya				X	
4	Kelola konfigurasi jaringan dengan cara yang aman			X		
5	Melindungi integritas sistem					x
6	Memberikan perlindungan fisik pada perangkat <i>endpoint</i>					x
<b>Sub Kontrol</b>	<b>DSS05.04 Mengelola identitas pengguna dan akses logis</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menjaga hak akses pengguna sesuai dengan fungsi bisnis dan persyaratan proses				X	
2	Mengelola semua perubahan hak akses					X
3	Memisahkan dan mengelola akun pengguna istimewa				X	
4	Melakukan tinjauan manajemen berkala terhadap semua akun				X	
5	Meengidentifikasi secara unik semua aktivitas pemrosesan informasi menurut pengguna					X
<b>Sub Kontrol</b>	<b>DSS05.05 Mengelola akses fisik ke aset TI</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mengelola permintaan dan pemberian akses				X	
2	Batasi akses ke situs TI yang sensitif dengan menetapkan batasan perimeter					X
3	Profil akses tetap terkini					X
<b>Sub Kontrol</b>	<b>DSS05.06 Mengelola dokumen sensitif dan perangkat keluaran</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Menetapkan hak akses pada dokumen sensitif					X
2	Menetapkan inventaris dokumen sensitif dan perangkat <i>output</i>					X

3	Hancurkan informasi sensitif dan lindungi perangkat <i>output</i>				X	
4	Tetapkan perlindungan fisik yang tepat terhadap formulir khusus dan perangkat sensitif				X	
<b>Sub Kontrol</b>	<b>DSS05.07 Memantau infrastruktur untuk Keterangan kejadian terkait keamanan</b>					
No	Pernyataan	Tingkat Persetujuan				
		1	2	3	4	5
1	Mencatat peristiwa terkait keamanan yang dilaporkan oleh alat pemantauan keamanan infrastruktur					X
2	Tinjau log peristiwa secara berkala untuk mengetahui potensi insiden				X	