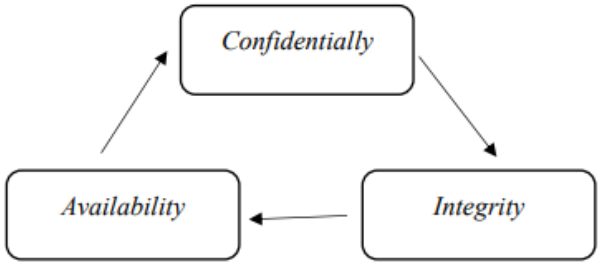
# BAB II
# TINJAUAN PUSTAKA

## 2.1 Keamanan Komputer

Keamanan komputer adalah proses pencegahan dan pendeteksian penipuan dalam sistem informasi, dimana informasi itu sendiri tidak memiliki arti fisik [16]. Tiga prinsip dari sumber daya komputer yaitu *Confidentiality, Integrity*, dan *Availablity* (CIA), dapat digambarkan dalam segitiga CIA seperti Gambar 2.1 [17]:




Gambar 2.1 Segitiga CIA

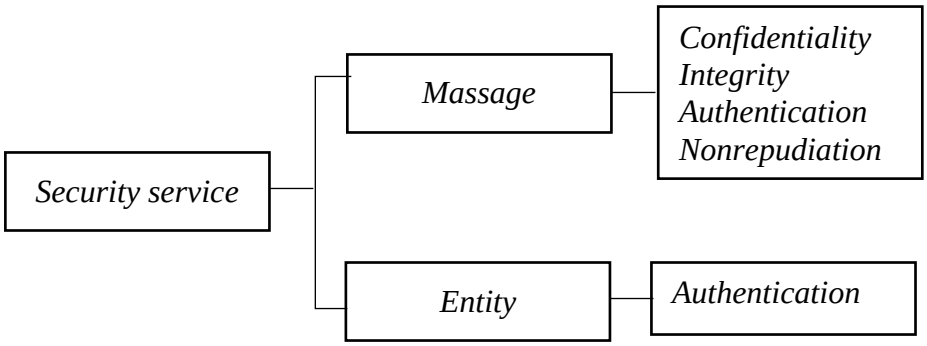
Gambar 2.1 merupakan penjelasan mengenai segitiga CIA, antara lain:

1. *Confidentiality* (Kerahasiaan), memiliki 2 pengertian yaitu kerahasiaan data dan *privacy*.
   a. Kerahasian data adalah jaminan data rahasia, seseorang tidak dapat mengubah data tersebut.
   b. Privasi menjamin bahwa individu hanya memiliki kendali atas informasi tentang diri sendiri. Informasi tersebut dapat dikumpulkan atau disimpan dengan dan kepada siapa informasi tersebut dapat dibagikan.
2. *Integrity* (Integritas), memiliki 2 konsep yaitu integritas data dan integritas sistem.
   a. Integritas data menjamin data dan program dapat berubah dengan cara yang spesifik dan resmi.

b. Integritas sistem menjamin sistem untuk melakukan fungsi yang diinginkan dalam keadaan tidak terganggu dan bebas dari pihak yang tidak berkepentingan.

3. *Availability* (Ketersediaan) adalah jaminan sistem yang berkerja dengan benar serta layanan pengguna tidak akan terganggu.

Berikut 5 layanan pada keamanan jaringan, dapat dilihat pada Gambar 2.2:




Gambar 2.2 Layanan Keamanan jaringan

Berikut Gambar 2.2 di atas merupakan penjelasan dari layanan jaringan.

1. Kerahasiaan pesan merupakan pengirim dan penerima mengharapkan kerahasiaan. Pesan yang dikirim hanya dapat diterima oleh penerima yang dituju.
2. Integritas pesan merupakan informasi harus sampai pada penerima samam dengan yang dikirim, karena semakin banyak informasi yang dipertukarkan melalui internet, maka integritas sangat penting.
3. Otentikasi pesan adalah layanan yang bukan dari bagian intgritas pesan. Dalam otentikasi pesan, penerima harus memverifikasi identitas pengirim dan penipu untuk tidak mengirimkan pesan tersebut.
4. *Nonrepudiation* pesan berarti pengirim tidak dapat menolak pengiriman pesan sebenarnya yang sudah dikirim.
5. Otentikasi Entitas berarti pengguna diautentikasi sebelum mendapat akses sumber daya sistem.

a. Keamanan Aplikasi

Keamanan aplikasi melindungi dan meningkatkan dari pencurian dan pembajakan data atau kode pada aplikasi. Berikut jenis keamanan aplikasi, yaitu:

1. Autentikasi, prosedur otentikasi menentukan pengguna yang berhak mempunyai akses.
2. Otorisasi, hanya dapat dilakukan setelah proses otentikasi berhasil. Sistem memvalidasi ruang lingkup otoritas pengguna saat menggunakan aplikasi.
3. Enkripsi, sebuah proses yang mencegah pengguna tidak bertanggung jawab membaca data sensitif pengguna aplikasi.
4. *Logging*, merekam informasi akses aplikasi.
5. Pengujian keamanan aplikasi, proses untuk memastikan bahwa semua proses keamanan berkerja dengan baik.

b. Sistem Keamanan Data

Keamanan data adalah proses melindungi informasi digital dari kerusakan, pencurian, atau akses yang tidak sah. Ini mencakupkan semua hal seperti *software*, *hardware*, alat penyimpanan, perangkat pengguna, manajemen akses, dan prosedural Universitas. Beberapa jenis keamanan data antara lain [18]:

1. Enkripsi, sebuah proses yang mencegah data pengguna aplikasi sensitif dibaca oleh pengguna yang tidak bertanggung jawab.
2. Pembersihan data, tata kelola keamanan data yang efesien untuk menghapus tanggung jawab dan potensi kesalahan data.
3. Kamuflase data, suatu gambaran enkripsi menjadikan data tidak dapat digunakan apabila disadap oleh peretas. Keaslian pesan hanya terlihat oleh orang yang mengetahui kodenya.

## 2.2 Serangan

Serangan keamanan dapat menyebabkan kerusakan yang signifikan, termasuk kerugian finansial, kerusakan reputasi, dan hilangnya data penting. Cara untuk megatasi serangan keamanan, Universitas harus menerapkan sistem keamanan yang ketat, melakukan peninjauan berulang, serta memberi pembelajaran

mengenai keamanan untuk memangkas dampak akibat serangan. Berikut beberapa jenis serangan *cyber*, antara lain [19]:

a. *Malware*

*Malware* atau *malicious software* adalah serangan komputer dengan program bawaan yang dirancang untuk mendapatkan informasi atau bahkan mendapatkan akses ke informasi korban. Berikut adalah jenis-jenis *malware,* yaitu:

1. *Ransomware* adalah serangan di mana korban dipaksa membayar sejumlah uang untuk mendapatkan akses ke informasi penting korban.
2. *Spyware* adalah perangkat lunak yang mengirimkan semua data dari komputer ke peretas yang menginstal perangkat lunak tersebut.
3. *Keylogger* memiliki prinsip yang sama dengan *spyware* tetapi hanya mengirimkan data yang dimasukkan melalui perangkat *input.*
4. *Trojan* adalah salah satu *malware* yang paling umum, karena dapat menambahkan aplikasi berbahaya ke aplikasi yang tanpa disadari telah terinfeksi oleh pengguna. Komputer yang terinfeksi kemudian dapat mengakses sebagian besar data, tergantung pada seberapa banyak akses yang diperoleh oleh *Trojan.*
5. Virus menginfeksi aplikasi atau *file* dan hanya tumbuh atau menyebar ketika aplikasi atau *file* tersebut dibuka.

b. *Phishing*

Serangan ini menggunakan pesan-pesan yang menipu kepada korban, sehingga korban tidak merasa terancam dengan bocornya informasi yang diberikan. Biasanya, serangan *phishing* dikirim melalui email atau media sosial atau bahkan pesan teks yang dikenal dengan istilah smishing dan melalui telepon yang dikenal dengan istilah *phishing*. Serangan ini dapat dikerjakan oleh pihak tidak bertanggung jawab, akibatnya korban masuk ke dalam *website,* pengguna dialihkan ke berbagai serangan kejahatan dunia maya lainnya. Kedua situs tersebut meminta informasi pribadi, otorisasi pembayaran, halaman palsu, dan lainnya. Beberapa serangan *phishing* yang terkenal adalah *spear phishing, whaling,* dan *angler phishing.*

c. *Man-in-the-Middle*

Serangan ini dilakukan pada jaringan yang tidak aman dan tidak terenkripsi. Peretas mencoba mengarahkan semua lalu lintas jaringan ke komputer atau perangkat bekas. Besarnya kerugian korban tergantung pada informasi apa yang diterima korban. Jika korban menggunakan rekening bank, ada kemungkinan nama pengguna, kata sandi dan informasi dibagikan kepada pelaku.

d. *Distributed Denial of Service* atau *Denial of Service*

*Denial of Service* (DOS) adalah serangan *server* yang dimaksudkan untuk menghancurkan atau menonaktifkan sistem target, sehingga komputer tidak dapat dijalankan fungsinya. Sedangkan *Distributed Denial of Service* **(**DDOS**)** merupakan serangan *denial of service* yang memanfaatkan beberapa server atau komputer untuk mengeksplotasi server target di jaringan.

Perbedaan antara DoS dan DDoS adalah jumlah perangkat yang digunakan untuk serangan pada waktu yang bersamaan. Tujuan serangan ini bukan untuk mencuri data, melainkan untuk melemahkan *server*, yang menciptakan celah untuk kemungkinan serangan *cyber* lainnya di *server*.

e. *Domain name system spoofing*

*Domain name system* (DNS) *spoofing* adalah serangan peretas yang mengalihkan lalu lintas *web* ke situs *web* palsu. Halaman ini terlihat identik dengan halaman yang dimaksud korban. Tetapi setiap informasi yang dimasukkan korban di situs web palsu dikirim langsung ke peretas, memberikan akses ke akun anda kepada penjahat dunia maya. Peretas juga dapat menggunakan DNS *spoffing* untuk menyabotase sistem dengan mengarahkan pengunjung ke situs *web*.

f. *Cross-site scripting*

*Cross-site scripting* (XSS) adalah kejahatan ancaman situs *web* untuk mengeksploitasi kerentanan dalam formulir entri situs *web*. Saat penyerang menemukan kerentanan XSS di sebuah situs *web*, penyerang mengeksploitasinya dengan memasukkan *script* yang salah satunya dirancang untuk menjebak korban

[20]. Jika korban tertangkap, situs bisa diambil alih. Serangan XSS terbagi dalam dua macam, yaitu:

1. Permanen

Serangan ini biasanya disebut *stored* XSS, yang biasanya ditemukan di halaman web tempat pelanggan dapat misalnya, mengetikkan *script* ke dalam kotak pencarian halaman.

2. Tidak secara permanen

Serangan XSS ini sering disebut sebagai XSS tercermin, dimana penyerang dapat memasukkan *script* yang dapat disimpan dalam *database website*. *Script* yang dimasukkan dikembalikan ke *server* aplikasi *web* korban, misalnya dengan menampilkan pesan kesalahan yang dapat terlihat di program klien lain.

g. *Padding oracle on downgraded legacy encryption*

*Padding oracle on downgraded legacy encryption* (POODLE) adalah serangan yang mengeksploitasi kerentanan dalam protokol SSL 3.0 (CVE-2014-3566). Kerentanan ini memungkinkan penyerang mendengarkan komunikasi terenkripsi SSLv3. Kerentanan tidak lagi ada di protokol *Transport Layer Security* (TLS) penerus *Secure Socket Layer* (SSL). Penyerang dapat mencuri data rahasia yang dikirimkan, misalnya kata sandi atau cookie sesi, lalu menyamar sebagai pengguna.

Kerentanan POODLE mepengaruhi *cipher suite* yang berisi *cipher blok* serta *cipher simetris*, seperti algoritma AES atau DES. *Cipher blok* mengenkripsi data dalam blok dengan panjang tetap, seperti 8 Byte atau 16 Byte [21]. Solusi yang disarankan untuk mencegah serangan POODLE adalah menonaktifkan SSL versi 3.0 pada HTTPS, atau SSL versi 3.0 masih diperlukan dapat menggunakan mekanisme `TLS_FALLBACK_SCSV`.

h. SQL *injection*

SQL *injection* merupakan teknik serangan yang mengekspoilitasi kode dengan memodifikasi *backend* SQL dengan menambahkan pernyataan, dengan mencoba memanipulasi parameter pada URL target dengan memasukan tanda petik (‘) [22]. SQL *injection* memungkinkan peretas untuk mendapatkan akses ke sistem *database*

tanpa otentikasi dan dapat menghapus atau mengubah semua data yang disimpan dalam *database*. Ketika kerentanan itu terjadi dan tidak ada cadangan *database*-nya itu sangat berbahaya. Keamanan data tersebut harus dicadangkan di penyimpanan eksternal atau *cloud*. Efek yang ditimbulkan dari SQL *injection*, yaitu:

1. SQL *injection* memungkinkan akses ke sistem tanpa memiliki akun. Hal ini berlaku baik pengguna biasa maupun administrator.
2. SQL *injection* memungkinkan seseorang dapat membobol *database*, mengubah, menghapus, atau bahkan menambahkan data ke dalamnya.
3. *Hacker* tidak hanya mengubah data tetapi juga menanamkan akun yang tidak dikenal. Oleh karena itu, jika system sudah diperbaiki dan peretas masih memiliki akun cadangan, dapat *login* tanpa harus injeksi SQL lagi.
4. Basis data itu sendiri mungkin dimatikan sehigga server web yang tidak dapat melayani pengguna dengan baik.

i. *Penetration Testing*

Pengujian penetrasi berbasis modul CEH adalah prosedur penilaian keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber risiko dan bagian pengujian keamanan informasi. Pengujian simulasi serangan dilakukan dalam bentuk skenario yang dilakukan oleh *hacker, cracker,* dan lain-lain. Tujuan untuk mengidentifikasi dan memahami serangan terhadap sistem dan kemungkinan konsekuensi dari kelemahan sistem. Metode pengujian penetrasi terbagi dalam tiga kategori:

1. *Black-box* adalah jenis pengujian penetrasi yang mirip dengan peretas sungguhan, dimana penguji mendapatkan nama dan informasi dari jaringan serta penguji harus mendapatkan sendiri informasi lainnya.
2. *White-box* merupakan jenis pengujian yang merupakan kebalikan dari pengujian *black-box*, karena informasi sudah diketahui terlebih dahulu dan infrastruktur seperti apa yang akan diuji.
3. *Grey-box* merupakan kombinasi dari data terbatas dan pengujian internal, selain itu semua program diperiksa kesalahannya. Simulasi yang digunakan pada

*grey-box* didasarkan pada pengujian *black-box* dan pengetahuan yang ada, sehingga dapat dianalisis secara menyeluruh.

## 2.3 *Information System Security Assessment Framework*

Kerangka penilaian keamanan sistem informasi (ISSAF) merupakan kerangka acuan dan tujuan penggunaannya meliputi tahapan menginformasikan, evaluasi dan melaporkan hasil pengujian sistem keamanan pada domain yang di tes dan analisis hasilnya [23]. ISSAF memiliki 3 pendekatan, yaitu:

1. *Planning and preparation* merupakan tahap awal yang terdiri dari penyiapan jaringan target dan pengumpulan informasi untuk uji penetrasi.
2. *Assessment* merupakan tahap pengujian suatu sistem informasi yang terdiri dari tahapan sebagai berikut:
    a. Pengumpulan informasi mengacu terkait sistem informasi target, seperti IP *address*, nama domain, dan lain sebagainya.
    b. Pemetaan jaringan adalah melakukan langkah untuk mencari informasi contohnya *port* yang terbuka, bentuk ancaman, dan lain-lain.
    c. Identifikasi kerentanan adalah identifikasi kelemahan sistem informasi.
    d. *Penetration testing* adalah menguji sistem keamanan target.
3. *Reporting* merupakan tahap dimana suatu laporan dibuat berdasarkan hasil yang diperoleh pada tahap sebelumnya.

Berikut merupakan *tools* yang digunakan pada metode ISSAF, yaitu:

1. Whois adalah layanan untuk mengetahui informasi seperti, domain, tanggal registrasi, tanggal expired, nama server dan lain sebagainya.
2. Dnsrecon adalah *tools* yang ditulis dengan bahasa pemrograman Python. *Tool* ini digunakan untuk recon DNS saat melakukan *information gathering.*
3. Nmap adalah aplikasi *open source* untuk mengeksplorasi keamanan jaringan. Nmap dikembangkan pada tanggal 1 September 1997 oleh Fyodor Vaskovich. Nmap melakukan deteksi jaringan menggunakan teknik seperti, *port scanning, ping scanning, ping TCP ACK, ICMP, IP, UDP*, dan *TCP SYK.*

4. Vega adalah *tools open source* untuk mendeteksi celah kerentanan keamanan *website* atau informasi sensitif yang diungkapkan secara tidak sengaja. Vega dikembangkan oleh subgraph di Montreal.
5. Owasp Zap adalah *tools vulnerability* untuk mendeteksi celah kerentanan *website*. Owasp Zap diciptakan oleh organisasi Owasp, *tools* ini dikembangkan terus sehingga siapa saja dapat mengembangkan *tools* tersebut.

## 2.4 Sistem Informasi Akademik

Sistem Informasi Akademik (Siakad) merupakan suatu sistem pengelolaan dan pengolahan data yang berkaitan dengan aktifitas akademik mahasiswa, dosen dan pegawai. Siakad digunakan untuk mengelola proses seperti mengatur proses kemahasiswaan, proses belajar mengajar antara dosen dan mahasiswa, keutuhan dokumen, dan kegiatan registrasi akademik pada saat melakukan kegiatan pengelolaan akademik. Siakad dirancang khusus untuk memenuhi kebutuhan layanan pendidikan yang terkomputerisasi, sehingga menaikkan kemampuan dan mutu.

Unit Pelaksanaan Teknis yang ditugaskan untuk mengelola Siakad di Untirta adalah Pusat Data dan Informasi (Pusdainfo). Pusdainfo Untirta memiliki sekitar 33 layanan teknologi informasi yang dapat mendukung layanan akademik dan administrasi. Berikut layanan TI tersebut:

a. Sistem Informasi Akademik (Siakad).
b. Sistem Pembelajaran Daring (Spada).
c. Sistem Informasi Tugas Akhir (Sista)
d. Sistem informasi Kinerja Untirta (Sikita).
e. e-administrasi.

## 2.5 Audit Sistem Informasi

Audit sistem informasi merupakan metode pengumpulan serta penilaian untuk menentukan apakah sistem yang berisi *asset* dapat dilindungi. Kredibilitas data dianggap konsisten dengan tujuan Universitas apabila mendapat penerapan

sumber dayanya yang baik. Berikut merupakan tujuan untuk audit sistem informasi [24]:

a. Keamanan aset, seperti *software*, *hardware* dan sumber daya dijamin dengan sistem penanganan intern untuk menghindari penyimpangan.
b. Melindungi kredibilitas data, seperti data-data yang lengkap.
c. Pengaruh teknologi, Universitas memiliki kewajiban dalam proses mengambil kesimpulan. TI dinyatakan efesien apabila dapat melengkapi kebutuhan jumlah pengguna dan sumber daya yang minimum.
d. Ekonomi adalah aspek keuangan. Dalam ilmu ekonomi, kerugian dihitung dalam satuan moneter.

## 2.6 *IT Governance*

Tata kelola TI adalah proses pengelolaan organisasi secara keseluruhan, seperti proses struktur organisasi digunakan sebagai perpanjangan TI dalam organisasi untuk mengembangkan tujuan dan strategi organisasi [25]. Tata kelola TI terdiri dari lima bagian, yaitu:

1. Penyelarasan strategis adalah penyelarasan perencanaan bisnis dan TI. Penyelarasan strategi ditunjukkan untuk mendefinisikan, mempertahankan dan memvalidasi posisi nilai TI dalam operasional perusahaan.
2. Penciptaan nilai merupakan proses yang dirancang agar informasi yang dikomunikasikan menghasilkan keuntungan dengan biaya yang lebih optimal.
3. Manajemen sumber daya untuk meningkatkan dan mengatur pengelolaan TI yang tepat seperti aplikasi, informasi, dan infrastruktur.
4. Manajemen risiko adalah proses manajemen tingkat risiko yang meningkatkan transparansi risiko yang terjadi dalam suatu perusahaan.
5. Pengukuran kinerja mengacu pada evaluasi dan pengukuran perilaku sistem secara berkala.

## 2.7 *Control Objective for Information and Related Technology*

COBIT adalah kerangka TI untuk melakukan penilaian guna mengoptimalkan dan menyeimbangkan manfaat, tingkat risiko, dan penggunaan

sumber daya. COBIT merupakan kumpulan praktik tata kelola TI dirancang untuk mendukung pelaksanaan manajemen dalam menghubungkan kesenjangan antara risiko TI.

Tahun 1996 pertama kali COBIT diluncurkan dengan versi 1 hanya focus di area pengujian. COBIT berkembang tahun 1998 menjadi versi 2 fokus di domain proses. Versi 3 berevolusi tahun 2000, yang menambahkan pedoman operasional yang fokus terhadap manajemen. Manajemen TI merupakan tambahan penting terhadap berubahnya kerangka versi COBIT 4.0/4.1 yang dirilis tahun 2005-2007. Tahun 2012, ISACA merilis versi 5 ini mencakup cakupan yang lebih luas dibandingkan versi sebelumnya dan membahas mengenai tata kelola TI, khususnya tata kelola TI di Universitas [26].

### 2.7.1 Prinsip COBIT 5

Prinsip dan dasar COBIT 5 dapat berguna bagi Universitas, baik komersial, nirlaba, atau publik. ISACA dan ITGI memiliki kerangka COBIT 5 yang berisi lima prinsip dalam mengimplementasikan bagian pengelolaan pada suatu Universitas. Dibawah ini merupakan lima prinsipnya:

1. Pemenuhan kebutuhan *stakeholder*
2. Meliputi bisnis dari awal sampai akhir
3. Penggunaan kerangka terpadu
4. Mengaktifkan pendekatan holostik
5. Pemisahan administrasi dan manajemen

Menurut COBIT 5, berikut merupakaan perbedaan antara tata kelola dan manajemen:

a. Tata kelola

Tata kelola menentukan bahwa kualitas, ketentuan, dan prioritas pemangku kepentingan dinilai dan diidentifikasi untuk mencapai tujuan yang diakui. Khususnya dalam organisasi yang besar dan kompleks, tugas administratif tertentu dapat ditugaskan ke tingkat yang sesuai dalam struktur organisasi.

b. Manajemen

Manajemen mendefinisikan, melaksanakan, dan mengendalikan kegiatan sebagaimana diarahkan oleh otoritas untuk mencapai tujuan. Universitas dapat menciptakan manajemen efektif yang memaksimalkan pemodalan pemangku kepentingan dan pengguna TI.

### 2.7.2 Model Referensi Proses

Model referensi proses merupakan penghubung antar model proses sebelumnya, pada COBIT 5 dibagi 5 domain dengan 37 proses manajemen, 5 domain tersebut adalah [27]:

1. *Evaluate, direct and monitor*

Proses EDM terkait tujuan manajemen penanggung jawab seperti pembentukan nilai, mengoptimalkan risiko dan sumber daya, memberikan hasil konsultasi serta pemantauan TI. Evaluasi, pengarahan, dan pemantauan (EDM) mencakup 5 subdomain dan metode pengelolaan utamanya:

a. Menentukan penyusunan dan perlindungan tata kelola manajemen (EDM01).
b. Menentukan manfaat keluaran (EDM02).
c. Pengelolaan risiko (EDM03).
d. Mengoptimalkan sumber daya (EDM04).
e. Menjelaskan penanggung jawab kepentingan (EDM05).

2. *Align, plan and organise*

Proses APO menyelaraskan, merencanakan, mengatur strategi dan taktik untuk identifikasi tentang bagaimana TI akan mencapai tujuan bisnisnya dengan sebaik-baiknya. Berikut ini adalah subdomain prosesnya.

a. Pengelolaan manajemen IT (APO01).
b. Pengelolaan strategi (APO02).
c. Pengelolaan arsitektur Universitas (APO03).
d. Pengelolaan inovasi (APO04).
e. Pengelolaan dokumen (APO05).
f. Pengelolaan anggaran dan manajemen biaya (APO06).

g. Pengelolaan sumber daya manusia (APO07).
h. Pengelolaan hubungan (APO08).
i. Pengelolaan perjanjian layanan (APO09).
j. Pengelolaan pemasok (APO10).
k. Manajemen mutu (APO11).
l. Pengelolaan risiko (APO12).
m. Pengelolaan keamanan (APO13).

3. *Build, acquire and implement*

Proses BAI membangun tata kelola untuk menghasilkan solusi layanan. Strategi TI dijalankan untuk mengidentifikasi, mengembangkan serta mengintegrasikan solusi TI ke dalam proses memperoleh tujuan bisnisnya. Berikut adalah subdomain dari prosesnya:

a. Pengelolaan program dan project (BAI01).
b. Pengelolaan persyaratan (BAI02).
c. Pengelolaan manajemen dan pengembangan solusi identitas (BAI03).
d. Pengelolaan ketersediaan dan kapabilitas (BAI04).
e. Pengelolaan aktivasi perubahan (BAI05).
f. Pengelolaan perubahan (BAI06).
g. Pengelolaan penerimaan dan transformasi perubahan (BAI07).
h. Pengelolaan pengetahuan (BAI08).
i. Pengelolaan asset (BAI09).
j. Pengelolaan konfigurasi (BAI10).

4. *Deliver, service and support*

Proses DSS mencakup strategi yang digunakan untuk memastikan bagaimana TI dapat memberi peran terbaik terhadap tujuan Universitas. Penerapan strategi harus diatur, dihubungkan, dan dikelola dari berbagai sudut pandang. Berikut ini adalah subdomain prosesnya:

a. Pengelolaan operasi (DSS01).
b. Pengelolaan layanan insiden dan manajemen (DSS02).
c. Pengelolaan masalah (DSS03).
d. Pengelolaan keberlanjutan (DSS04).

e. Pengelolaan layanan keamanan (DSS05).
f. Pengelolaan pengendalian proses (DSS06).

5. *Monitor, evaluate and assets*

Proses MEA memastikan kualitas seluruh proses TI dan kepatuhan terhadap persyaratan manajemen, seperti pemantauan pengendalian internal dan eksternal, peraturan manajemen, dan tata kelola. Berikut ini adalah subdomain prosesnya:

a. Memonitoring, mengevaluasi kinerja, melakukan penyesuaian (MEA01).
b. Memonitoring dan mengevaluasi sistem pengendalian internal (MEA02).
c. Memonitoring dan mengevaluasi persyaratan eksternal (MEA03).

### 2.7.3 *Capability Level*

Kapabilitas level adalah proses kemampuan untuk mencapai tingkat kemampuan yang ditentukan oleh atribut proses. Untuk menginterprestasikan tingkat kemampuan, dapat diasumsikan bahwa setiap subproses memiliki nilai bobot untuk tingkat kemampuan, seperti terlihat di Tabel 2.1.

Tabel 2.1 Jawaban Nilai dan Tingkat Kapabilitas

| Nilai | Jawaban | Nilai Kapabilitas | Tingkat Kapabilitas |
|---|---|---|---|
| 0,00-0,50 | A | 0,00 | 0 (*incomplate process*) |
| 0,51-1,50 | B | 1,00 | 1 (*perfomed process*) |
| 1,51-2,50 | C | 2,00 | 2 (*managed process*) |
| 2,51-3,50 | D | 3,00 | 3 (*established process*) |
| 3,51-4,50 | E | 4,00 | 4 (*predectable process*) |
| 4,51-5,00 | F | 5,00 | 5 (*optimising process*) |

Berdasarkan Tabel 2.1, aspek fungsional model peniliaan formatif mencakup enam tingkatan fungsional. Keenam level ini berisi indikator atribut proses, untuk mengasumsikan bobot tingkat kapabilitas.

### 2.7.4 Perhitungan *Capability Level*

Perhitungan untuk rekapitulasi jawaban kuesioner menggunakan perhitungan yang dirumuskan pada Persamaan (2.1).

$$C = \frac{H}{JR}\ x\ 100\% \qquad (2.1)$$

Berdasarkan Persamaan (2.1), nilai untuk rekapitulasi kuesioner dari hasil total jawaban responden dibagi dengan jumlah responden. Perhitungan nilai *capability level* menggunakan perhitungan yang dirumuskan pada Persamaan (2.2).

$$NK = \frac{(LPxNka)+(LPxNkb)+(LPxNkc)+(LPxNkd)+(LPxNke)+(LPxNkf)}{100} \quad (2.2)$$

Berdasarkan persamaan (2.2), nilai *capability* diperoleh dari hasil level presentase dikali dengan nilai kematangan proses. Analisis kesenjangan adalah teknik umum untuk mengidentifikasi dan mengelola kesenjangan yang terjadi selama perencanaan transisi antara keadaan awal dan keadaan target. Analisis kesenjangan adalah sebuah alat atau teknik yang sering digunakan dalam konteks perencanaan strategis. Hal ini melibatkan evaluasi keadaan atau tujuan yang diinginkan dibandingkan dengan keadaan saat ini dan memahami kesenjangan antara keduanya [28]. Tingkat kesenjangan menggunakan perhitungan yang dirumuskan pada Persamaan (2.3)

$$Tingkat\ kesenjangan = Kondisi\ yang\ diharapkan - Kondisi\ saat\ ini \quad (2.3)$$

Berdasarkan Persamaan (2.3), tingkat kesenjangan ditentukan dari kondisi yang diharapkan dengan kondisi saat ini. Analisis kesenjangan membantu mengidentifikasi kesenjangan yang besar dan penyebabnya.

### 2.7.5 Diagram *Responsible, Accountable, Consulted, and Informed*

Diagram *responsible, accountable, consulted, and informed* (RACI) merupakan matriks dari seluruh aktivitas mengambil keputusan yang dilaksanakan Universitas untuk setiap peran dalam proses [29].

1. Bertanggung jawab mendeskripsikan siapa yang akan mengerjakan pekerjaan. Artinya seseorang bertanggung jawab dalam menjalankan kegiatan operasional untuk melengkapi kebutuhan serta mencapai hasil yang diharapkan.
2. Akuntabel mendeskripsikan siapa yang berkewajiban atas keberhasilan pekerjaan. Berarti mengambil tanggung jawab penuh atas pekerjaan yang diselesaikan.
3. Konsultasi mendeskripsikan pihak yang akan memberi pendapat. Berarti yang berkewajiban atas pengumpulan data.

4. Informasi mendeskripsikan pihak yang akan memperoleh data. Mengacu pihak yang berkewajiban mendapatkan data yang sesuai, untuk memverifikasi pekerjaan yang diselesaikan.

## 2.8 Kajian Pustaka

Penelitian mengenai audit keamanan menggunakan *penetration testing* serta layanan manajemen menggunakan COBIT 5 telah banyak dilakukan oleh berbagai pihak. Penelitian tersebut dibuktikan oleh karya tulis yang dipublikasikan di jurnal. Berikut penelitian yang penulis gunakan sebagai referensi.

Penelitian pertama membahas mengenai evaluasi keamanan *website*. Metode yang digunakan yaitu pentest dengan memanfaatkan kerangka ISSAF. Hasil pengujian memperoleh 18 kerentanan yang ditemukan di *website* tersebut [11]. Penelitian kedua membahas evaluasi TI. Penelitian ini memanfaatkan kerangka COBIT 2019 proses BAI11. Hasilnya tingkat kemampuan yaitu level 1 (*perfomed*) sedangkan tingkat kematangan nya level 2 (*managed projects*) [12].

Penelitian ketiga membahas menganalisa keamanan *webserver*, Metode yang digunakan yaitu *penetration testing* dengan domain *information gathering, vulnerability assessment, gaining* dan *maintaining*, serta *clearing track.* Hasil pengujian memperoleh 10 kerentanan, ditemukan beberapa *port* yang terbuka dan dalam mensimulasikan ancaman, berhasil memperoleh nama pengguna dan kata sandi [13]. Penelitian keempat membahas mengaudit Siakad, penelitian ini memanfaatkan kerangka COBIT 5 proses APO12, APO13, serta DSS05. Hasil dari penelitian tingkat kapabilitas adalah APO12 yaitu level 1, APO13 level 2, dan DSS05 level 2, artinya telah melaksanakan dan mengimplementasikan proses TI hingga memperoleh tujuan [14].

Penelitian kelima membahas pengujian penetrasi aplikasi *web* menggunakan serangan injeksi SQL. Penelitian ini menggunakan metode *black-box* dengan *framework Open Web Application Security Project* (OWASP). Hasil pengujian terhadap 10 situs dilakukan, 80% *web* yang di uji memiliki kelemahan terhadap serangan SQL injeksi [15].

Penelitian selanjutnya membahas evaluasi tata kelola keamanan TI. Penelitian ini menerapkan kerangka COBIT 5 dan ISO 27002 dengan subdomain APO12, APO13, dan DSS05. Hasil dari penelitian ini menunjukkan bahwa nilai kapabilitas dari subdomain yang di uji *as is* pada level 2 (*managed process*) dengan tingkat kemampuan *to be* berada pada level 3 (*established process*) dengan hasil nilai kesenjangan yaitu 1.13, 1.10, dan 0.97 [30].

Berdasarkan penelitian tersebut, terlihat bahwa menganalisis dan mensimulasikan dengan *penetration testing* menggunakan *framework* ISSAF, dapat mengidentifikasi kerentanan dan memeriksa layanan *website* dapat disusupi atau tidak. Selain itu terlihat bahwa analisis manajemen menggunakan kerangka COBIT 5 dapat melihat tingkat kapabilitas manajeman keamanan dan kesenjangan yang diakibatkannya.