BAB II
TINJAUAN PUSTAKA

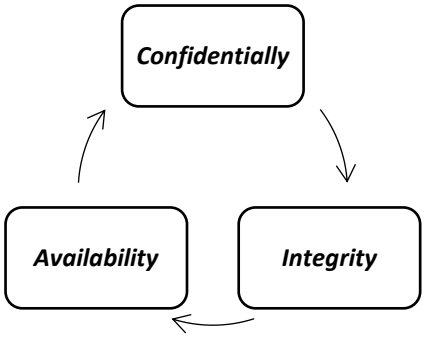
2.1 Layanan Teknologi Informasi

Layanan teknologi informasi adalah sarana yang disediakan oleh industri maupun organisasi kepada penggunanya untuk menyampaikan nilai atau manfaat tanpa adanya risiko tertentu [16]. Layanan teknologi informasi merupakan campuran dari teknologi informasi, orang, dan proses.

Layanan teknologi informasi yang menghadap pelanggan secara langsung menunjang proses bisnis satu atau lebih pelanggan dan target tingkat layanannya wajib ditetapkan dalam *Service Level Agreement* (SLA). Layanan teknologi informasi yang lain disebut sebagai layanan pendukung (*supporting services*). Layanan tersebut tidak digunakan secara langsung oleh bisnis, tetapi diperlukan oleh penyedia layanan untuk menyediakan layanan yang berhadapan langsung dengan pelanggan [17].

2.2 Keamanan Informasi

Keamanan informasi merupakan sebuah proses pengamanan aset informasi terhadap ancaman dan kerentanan [18]. Tujuan utama keamanan informasi ialah melindungi kerahasiaan, integritas, serta ketersediaan informasi. Keamanan jaringan bertujuan untuk menjaga kerahasiaan, integritas, dan aksesibilitas jaringan komputer dan data yang dikirimkan dalam media komunikasi. Pada keamanan informasi, terdapat prinsip utama yang dijelaskan pada Gambar 2.1.



Gambar 2.1 Prinsip Utama dalam Keamanan Informasi

Pada Gambar 2.1, dijelaskan bahwa terdapat tiga prinsip utama pada keamanan informasi, yaitu kerahasiaan (*Confidentiality*), integritas (*Integrity*), dan ketersediaan (*Availability*) atau sering disebut CIA *triad*.

1. Kerahasiaan berkaitan dengan perlindungan informasi dari pengguna dan program yang tidak sah di dunia digital. Kerahasiaan dibagi kedalam dua pengertian yaitu kerahasiaan data dan *privacy*. Kerahasiaan data merupakan adanya jaminan bahwa informasi rahasia atau informasi privat tidak dapat diubah atau diganti oleh seseorang yang tidak memiliki otoritas. Sementara itu, *privacy* merupakan adanya jaminan bahwa seseorang hanya mengendalikan informasi yang terkait dengan dirinya, dapat dikumpulkan atau disimpan dan oleh siapa serta untuk siapa informasi tersebut dapat dibuka.
2. Integritas berkaitan dengan akurasi, kualitas, konsistensi, dan kelengkapan data selama seluruh siklus hidupnya. Integritas dibagi kedalam dua konsep yaitu integritas data dan sistem. Integritas data merupakan jaminan sebuah informasi dan program dapat berubah dengan cara yang spesifik dan terotorisasi. Sementara itu, integritas sistem merupakan jaminan sebuah sistem melakukan fungsi yang diinginkan dalam suatu keadaan yang terhindar dari campur tangan pihak yang tidak terotorisasi.
3. Ketersediaan berkaitan dengan aksesibilitas data. Ketersediaan berarti data selalu tersedia saat pengguna resmi meminta atau menggunakannya [19]. Ketersediaan merupakan adanya jaminan bahwa sistem bekerja dengan benar dan layanan kepada pihak pengguna yang memiliki otoritas tidak terganggu [20].

Terdapat beberapa pembagian jenis keamanan informasi, yaitu *physical security*, *personal security*, *operational security*, *communications security*, dan *network security* [21].

2.3 *Website*

Website pada dasarnya merupakan kumpulan dokumen yang berisi data serta informasi yang dapat diakses melalui internet. Selain itu, *website* bisa berjalan di berbagai macam *platform* serta termasuk aplikasi yang ringan untuk digunakan

[13]. *Website* saat ini menjadi sumber informasi utama dan digunakan untuk berbagai kegiatan [15]. Setiap tahun, semakin banyak aplikasi berbasis web. Seiring dengan waktu dan semakin kompleksnya layanan dan aplikasi web dalam berbagai bidang, permintaan layanan web dari pengguna terus bertambah. Pada kuartal pertama tahun 2020, ada sekitar 367 juta nama domain. Masing-masing *website* ini dapat dianggap sebagai aplikasi web statis atau dinamis [6].

Pertumbuhan *website* di Indonesia sendiri terus bertambah secara signifikan. Fenomena ini terus bertambah sebanding dengan jumlah pengguna layanan internet di Indonesia yang meningkat dari tahun ke tahun. Berbagai macam *website* yang kerap diakses oleh pengguna di Indonesia antara lain: mesin pencari, *e-commerce*, forum sosial, dan portal berita [22].

2.4 Kerentanan dan Serangan Keamanan Informasi

Pelanggaran terhadap keamanan layanan teknologi informasi telah menyebabkan masalah besar bagi pelanggan, bisnis, dan perusahaan selama beberapa tahun terakhir [6]. Hal tersebut dikarenakan jaringan komputer bersifat publik dan global yang pada dasarnya tidak aman [8]. Pada sebuah layanan teknologi informasi tidak jarang menyimpan data-data pengguna terlebih lagi data yang bersifat pribadi seperti tanggal lahir, nomor telepon, serta data penting lainnya [23]. Ketika sebuah data terkirim dari satu terminal asal menuju ke terminal tujuan, data tersebut akan melewati beberapa terminal lain yang berarti akan memberi peluang untuk pengguna internet lain untuk mengambil data tersebut [9].

Kerentanan atau *vulnerability* adalah kelemahan dalam produk atau sistem yang berpotensi memungkinkan penyerang merusak kerahasiaan, integritas, atau ketersediaan produk atau sistem tersebut. Penyerang dapat mengeksploitasi kerentanan yang ada di perangkat lunak, *firewall*, protokol jaringan, jaringan nirkabel, sistem operasi, dan web *server*. Dari kerentanan tersebut, penyerang dapat melakukan serangannya.

Pada saat ini, serangan terhadap keamanan informasi semakin bervariasi. Berdasarkan data lalu lintas internet yang dihimpun dari *Indonesian Security Incident Response Team on Internet Infrastructure* (Id-SIRTII) pada tahun 2021, terdapat 10 serangan teratas beberapa diantaranya adalah *MyIoBot*, serangan *trojan*,

dan *Denial of Service* (DoS) [7]. Serangan tersebut dapat dibagi menjadi tiga jenis: serangan berbasis kelemahan perangkat keras, serangan *bug* berbasis perangkat lunak, dan serangan berbasis kerentanan dalam jaringan komputer.

Serangan berbasis kelemahan perangkat keras lebih sulit dicegah dikarenakan alat berbasis perangkat lunak saja tidak cukup untuk mendeteksi dan mencegah serangan terkait perangkat keras. Virus *Trojan* sering kali menjadi akar penyebab serangan perangkat keras. Varian perangkat lunak berbahaya ini menyebabkan penggunaan sumber daya komputer yang berlebihan, mengurangi kinerja, dan menyebabkan sistem mati dengan mengonsumsi daya yang berlebihan. Contoh serangan berbasis kelemahan perangkat keras adalah *Trojan*, *Rowhammer*, *logic bomb* dan *Malware*.

Serangan *bug* berbasis perangkat lunak disebabkan oleh kesalahan yang ada dalam perangkat lunak. Beberapa penyebab diantaranya adalah kesalahan yang terdapat pada *input* validasi, akses kendali, otentikasi, dan direktori. Selain itu, penyebab kesalahan perangkat lunak juga dapat disebabkan oleh masalah *Structured Query Language* (SQL), *Cross-site scripting* (XSS), komponen yang memiliki kerentanan, layanan web dan *Application Programming Interface* (API) yang bermasalah, dan pengujian keamanan perangkat lunak yang tidak tepat. Contoh serangan *bug* berbasis perangkat lunak adalah SQL *Injection*, XSS, dan *Buffer overflow*.

Serangan berbasis kerentanan dalam jaringan komputer disebabkan kerentanan dalam protokol jaringan, seperti *Transmission Control Protocol* (TCP), *Internet Protocol* (IP), *Address Resolution Protocol* (ARP), *Dynamic Host Configuration Protocol* (DHCP), dan *Domain Name System* (DNS). Misalnya, karena tidak ada struktur untuk mengontrol keakuratan dan kerahasiaan paket saat membawanya melalui jaringan menggunakan IP, informasi dalam paket dapat diekspos dan diubah selama pengiriman. Demikian pula, karena respons DNS tidak diverifikasi, penyerang dapat membuat *server* palsu, dan pengguna mungkin terhubung ke *server* palsu ini, bukan ke *server* yang sebenarnya.

Penyerang juga dapat mengirim permintaan berlebihan ke *server* DNS, membuatnya tidak tersedia untuk pengguna yang sah. Selain itu, penyerang dapat menangkap informasi selama transportasi data karena konfigurasi perangkat

jaringan yang tidak lengkap atau salah, termasuk sakelar, *router*, dan titik akses nirkabel. Contoh serangan berbasis kerentanan dalam jaringan komputer adalah DoS (*Denial of Services*), MiTM (*Man in The Middle*), dan *Spoofing* [19]. Berikut beberapa penjelasan terkait kerentanan dan serangan keamanan informasi.

a. *Distributed Denial of Service* (DDoS)

Distrributed Denial of Service (DDoS) merupakan salah satu serangan jaringan dimana penyerang berusaha membuat sumber daya jaringan tidak tersedia untuk pengguna sementara waktu. Serangan ini biasa dilakukan dengan membanjiri perangkat target. Serangan dilakukan dari beberapa komputer sekaligus menuju target yang disebut sebagai *zombie* atau *botnet*. DDoS memiliki tipe serangan, diantaranya adalah UDP *Flood*, ICMP *Flood*, dan SYN *Flood* [24].

Perubahan ukuran data menuju target serangan dapat meningkatkan level serangan serta menyebabkan peningkatan konsumsi daya listrik begitu juga dengan beban CPU pada *router* yang dilewati data tersebut. Teknik mitigasi yang biasa dilakukan untuk mengurangi dampak dari serangan DDoS adalah dengan *blackholing* untuk penyediaan *upstreams* atau pemberitahuan perubahan jalur [25].

b. SQL *injection*

SQL *injection* adalah salah satu metode untuk mengeksploitasi aplikasi *website* dengan menggunakan data yang disediakan atau diselipkan ke dalam kueri SQL. Serangan SQL *injection* dapat menyebabkan *server* mengembalikan data yang seharusnya dibatasi, menjalankan perintah *Data Definition Language* (DDL) yang menghapus atau mengubah objek *database*, atau sekadar menghapus data dari tabel.

SQL *injection* berkerja dengan cara memasukkan kueri SQL atau perintah (*command*) sebagai *input* yang dimungkinkan melalui halaman web atau *command prompt*. Halaman web akan mengambil parameter dari pengguna kemudian membuat kueri SQL tembus ke dalam *database*. Cara ini membuat SQL *injection* dapat dikatakan pula sebagai aktivitas yang mengelabui kueri pada *database*, sehingga pengguna yang tidak diautentikasi dapat mengetahui serta mengambil data dan informasi yang berada dalam *database* [26].

c. *Cross Site Scripting* (XSS)

Cross Site Scripting (XSS) merupakan serangan injeksi kode dengan memasukkan skrip berbahaya. Perbedaan utama antara SQL *Injection* dan XSS adalah teknologi dasar yang menjadi sasaran serangan. SQL *Injection* menyuntikkan kode SQL berbahaya, sedangkan serangan XSS menyuntikkan JavaScript [27]. Skrip yang sudah diinjeksi ini bisa dijalankan dengan hampir seluruh *client-side script*. Serangan ini dapat menimbulkan berbagai ancaman keamanan. Hal tersebut termasuk pencurian identitas, akses ke informasi yang bersifat sensitif dan terbatas, perubahan fungsionalitas web, serta ancaman dari serangan DoS [28].

d. DNS *spoofing*

DNS *spoofing* merupakan salah satu teknik serangan *Man in The Middle Attack* (MiTM). DNS *spoofing* merupakan proses memalsukan paket DNS pada jaringan DNS dengan mengubah alamat domain menjadi alamat palsu. Metode ini mengeksploitasi *server* yang memiliki kerentanan untuk memodifikasi data yang disimpan yang kemudian akan digunakan oleh sistem yang menjadi target [29]. DNS *Spoofing* dapat mengalihkan web yang memiliki konten positif dengan web yang memiliki konten negatif.

2.5 *Vulnerability Assessment*

Vulnerability Assessment merupakan proses mendefinisikan, mengidentifikasi, dan mengklasifikasikan celah keamanan (kerentanan) pada komputer, jaringan, atau infrastruktur komunikasi. Selain itu, *vulnerability assessment* dapat memperkirakan keefektifan tindakan pencegahan yang diusulkan dan mengevaluasi keefektifan aktualnya setelah diterapkan. Hasil kegiatan *vulnerability assessment* dapat digunakan untuk menentukan tingkat kematangan keamanan suatu *website*.

Tingkat kematangan ini dapat digunakan untuk mengukur sejauh mana penerapan kendali keamanan telah diterapkan pada suatu *website*, sehingga dapat diambil tindakan korektif untuk menghadapi ancaman yang dapat ditimbulkan oleh kerentanan keamanan pada *website* [15]. Berikut adalah beberapa *tool* yang dapat digunakan untuk melakukan *vulnerability assessment*.

a. Nmap

Network Mapper atau biasa disebut dengan Nmap merupakan salah satu *tool* yang digunakan dalam melakukan audit keamanan jaringan serta melakukan eksplorasi jaringan. Nmap bersifat *open source* dan bekerja lebih optimal di sistem operasi Linux daripada Windows. Nmap dapat melakukan pemindaian jaringan dengan teknik *port scanning*, *ping scannning*, *ping scan* TCP SYN, *ping scan* TCP ACK, *ping scan* UDP, *ping scan* ICMP, dan *ping scan* IP [30].

b. Nessus

Nessus merupakan salah satu tool *vulnerability scanner* untuk keamanan jaringan yang wajib digunakan oleh administrator sistem. Nessus adalah *software scanning*, yang dapat digunakan untuk mengaudit keamanan suatu sistem, seperti kerentanan, kesalahan konfigurasi, *patch* keamanan yang belum diterapkan, *password default*, dan DoS. Nessus berfungsi untuk memantau lalu lintas jaringan. Karena Nessus berfungsi juga untuk mendeteksi kerentanan atau cacat pada suatu sistem, Hal tersebut menjadikan Nessus sebagai salah satu alat yang andal dalam melakukan audit keamanan suatu sistem [15].

Tool Nessus memiliki sistem penilaian yang disebut *Common Vulnerability Scoring System* (CVSS). CVSS adalah metode penilaian untuk menilai kerentanan pada pengujian sistem. CVSS diklasifikasikan berdasarkan *score* pada tingkat penilaian yaitu *None, Low, Medium, High,* dan *Critical* [31]

2.6 Forensik Jaringan

Forensik jaringan adalah salah satu bagian dari forensik digital, dimana bukti dari jaringan ditangkap kemudian diinterpretasikan berdasarkan pengetahuan dari serangan jaringan. Bukti yang digunakan untuk melakukan forensik jaringan salah satunya adalah *log* jaringan saat serangan terjadi. Forensik jaringan dapat memberikan beberapa informasi, diantaranya adalah IP *address* penyerang, lokasi penyerang, jenis paket yang terkirim, dan beban CPU.

Tujuan dari forensik jaringan adalah untuk menemukan penyerang serta merekonstruksi kejadian pada saat serangan melalui analisis bukti penyusupan [25]. Forensik jaringan adalah tentang mencari tahu bagaimana keamanan dilanggar dan mengambil tindakan yang tepat untuk masa depan [32]. Forensik jaringan menjadi

perangkat yang sangat penting dalam melindungi keamanan serta mencari tahu pelanggaran keamanan yang dapat berdampak kepada suatu individu, perusahaan, maupun lembaga pemerintahan.

2.7 Manajemen Layanan Teknologi Informasi

Manajemen layanan teknologi informasi atau *Information Technology Service Management* (ITSM) merupakan sebuah implementasi dan pengelolaan layanan teknologi informasi berkualitas yang memenuhi kebutuhan bisnis. Manajemen layanan teknologi informasi dilakukan oleh penyedia layanan teknologi informasi melalui perpaduan yang tepat antara orang, proses, dan teknologi informasi. Manajemen layanan teknologi informasi harus dilakukan secara efektif dan efisien. Mengelola teknologi informasi dari perspektif bisnis memungkinkan kinerja tinggi organisasi dan penciptaan nilai [17].

Fokus ITSM adalah mengelola siklus hidup penuh layanan teknologi informasi. Ruang lingkupnya biasanya tidak mencakup manajemen proyek atau program, dan juga tidak mencakup pengembangan aplikasi atau perangkat lunak. Namun, proses ITSM harus dirancang dan diimplementasikan dengan cara yang selaras dan terintegrasi dengan manajemen proyek dan program serta proses pengembangan aplikasi dan perangkat lunak.

Pada ITSM terdapat beberapa kerangka kerja. Kerangka kerja tersebut menjelaskan praktik terbaik yang dapat digunakan organisasi teknologi informasi untuk mengimplementasikan dan terus meningkatkan kemampuan ITSM mereka. Banyak organisasi mengadopsi dan mengadaptasi praktik terbaik dari berbagai kerangka kerja dalam upaya mengembangkan serangkaian proses yang memenuhi kebutuhan mereka. Kerangka ITSM yang paling umum digunakan adalah: *Information Technology Infrastructure Library* (ITIL), *Control Objectives for Information and Related Technology* (COBIT), dan *Microsoft Operations Framework* (MOF). Kerangka kerja khusus vendor meliputi *IBM Tivoli Unified Process* dan *HP Service Management Framework* [33].

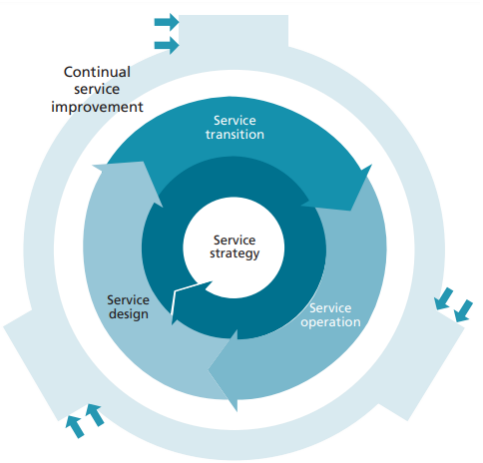
2.8 ITIL V3 *Service Operation*

Information Technology Infrastructure Library (ITIL) adalah salah satu aplikasi terbaik untuk manajemen layanan teknologi informasi. ITIL menawarkan pendekatan sistematis guna memberikan layanan teknologi informasi yang bermutu. ITIL membantu penyedia layanan dalam memberikan panduan tentang penyediaan layanan teknologi informasi yang bermutu, serta proses, fungsi, dan kemampuan lain yang dibutuhkan untuk mendukungnya. Digunakan oleh ratusan organisasi di seluruh dunia, ITIL membagikan panduan aplikasi terbaik yang berlaku untuk seluruh jenis organisasi yang menyediakan layanan teknologi informasi [17].

ITIL dikembangkan pada tahun 1980-an dan 1990-an oleh *Central Computer and Telecommunications Agency* (CCTA), yang saat ini bernama *Office of Government Commerce* (OGC), di bawah kontrak dengan Pemerintah Inggris. Semenjak saat itu, ITIL tidak hanya menawarkan kerangka kerja berbasis praktik terbaik untuk manajemen TI, namun juga pendekatan serta filosofi yang dibagikan oleh orang-orang yang bekerja dengannya dalam aplikasi. ITIL sudah mengalami dua kali perubahan. Perubahan pertama dilakukan pada tahun 2000-2002 (ITIL V2), dan yang kedua dilakukan pada tahun 2007 (ITIL V3). ITIL didukung oleh *IT Service Management Forum* (itSMF), sebuah organisasi nirlaba yang diakui secara internasional yang didedikasikan untuk menunjang pengembangan ITSM [34].

Perubahan kedua ITIL pada tahun 2007 diterbitkan sebagai tanggapan atas kemajuan signifikan dalam teknologi dan tantangan yang muncul bagi penyedia layanan teknologi informasi. Model serta arsitektur baru seperti *outsourcing*, layanan bersama, komputasi utilitas, komputasi awan, virtualisasi, layanan web, serta perdagangan seluler telah tersebar luas di dalam teknologi informasi. Pendekatan berbasis proses ITIL ditambah dengan siklus hidup layanan untuk mengatasi tantangan manajemen layanan tambahan ini.

Kerangka kerja ITIL didasarkan pada lima tahap siklus hidup yang dijelaskan pada Gambar 2.2.



Gambar 2.2 Siklus Hidup Layanan ITIL [17]

Gambar 2.2 merupakan siklus hidup layanan ITIL. Siklus hidup pada kerangka kerja ITIL v3 menggunakan desain *hub-and-spoke*, dengan *service strategy* di *hub*, kemudian *service design, transisition*, dan *operation* di siklus hidup bergulir atau jari-jari. *Continual service improvement* meliputi serta menunjang seluruh tahapan siklus hidup layanan.

Setiap tahap siklus hidup memengaruhi yang lain serta bergantung pada masukan dan umpan balik mereka. Menggunakan metode ini, serangkaian pemeriksaan dan keseimbangan yang konstan sepanjang siklus hidup layanan memastikan layanan dapat beradaptasi dan merespons secara efektif saat permintaan bisnis berubah seiring dengan kebutuhan bisnis. Siklus hidup layanan, memiliki publikasi utama membagikan panduan tentang aplikasi terbaik di tiap tahap. Panduan ini mencakup prinsip-prinsip utama, proses serta aktivitas yang dibutuhkan, organisasi dan peran, teknologi, tantangan terkait, aspek penentu keberhasilan, serta risiko.

Pada panduan inti ITIL, terdapat 26 proses dan empat fungsi yang dijelaskan. Definisi proses adalah sekumpulan aktivitas terstruktur yang ditujukan untuk mencapai tujuan tertentu. Suatu proses mengambil satu atau lebih *input* spesifik dan mengubahnya menjadi *output* tertentu. Sedangkan definisi fungsi adalah tim atau sekelompok orang dan alat atau sumber daya lain yang digunakan untuk melakukan satu atau lebih proses atau aktivitas. Proses dan fungsi berjalan sepanjang siklus hidup layanan tetapi sebagian besar dimiliki oleh satu tahap siklus hidup [35].

Perbedaan kerangka kerja ITIL dengan yang lain seperti COBIT 5, ITIL memiliki 5 domain sedangkan COBIT hanya memiliki 4 domain. Perbedaan

lainnya, pada ITIL proses dijelaskan dan dikelola pada setiap aktivitas dan *flowchart*. Penggunaan ITIL diharapkan dapat memberikan arahan untuk organisasi dalam pengunaan teknologi informasi yang efektif dan efisien. Selain itu, ITIL menjelaskan bagaimana merencanakan, merancang, dan mengimplementasikan fungsi manajemen layanan secara efektif. Sementara itu, COBIT berfokus pada apa yang perlu dilakukan untuk memastikan tata kelola yang baik dari semua proses teknologi infomasi terkait, termasuk proses manajemen layanan informasi. COBIT memberikan panduan, kerangka kerja, dan alat untuk mencapai tingkat kepatuhan dan kinerja yang diinginkan untuk proses teknologi informasi yang diperlukan untuk memenuhi kebutuhan bisnis [36].

Service operation merupakan salah satu domain yang termasuk dalam kerangka kerja ITIL v3. Domain ini menjelaskan praktik terbaik untuk mengelola layanan di lingkungan yang didukung. *Service operation* mencakup panduan untuk mencapai efektivitas dan efisiensi dalam penyampaian dan dukungan layanan untuk memastikan nilai bagi pelanggan, pengguna, dan penyedia layanan. Tujuan strategis pada akhirnya diwujudkan melalui layanan operasi, menjadikan *service operation* sebagai kemampuan yang kritis.

Service operation memberikan panduan untuk menjaga stabilitas dalam operasi layanan dan memungkinkan perubahan dalam desain, skala, cakupan, dan tingkat layanan. Organisasi diberikan panduan terperinci tentang proses, metode, dan alat yang dapat digunakan untuk dua perspektif *main control*, yaitu reaktif dan proaktif. Manajer dan praktisi diberikan pengetahuan yang memungkinkan mereka untuk membuat keputusan yang lebih baik di berbagai bidang seperti manajemen ketersediaan layanan, kendali permintaan, optimalisasi pemanfaatan kapasitas, penjadwalan operasional, pencegahan atau penyelesaian insiden layanan, dan manajemen masalah.

a. Proses dalam *service operation*

Pada *service operation*, terdapat sejumlah proses utama yang harus terhubung bersama untuk menyediakan struktur dukungan teknologi informasi yang efektif secara keseluruhan. S*ervice operation* memiliki lima proses utama:

1. *Event management*

Event management mengelola *event* sepanjang siklus hidupnya. Siklus hidup ini melibatkan koordinasi aktivitas untuk mendeteksi peristiwa, memahaminya, dan menentukan tindakan kendali yang sesuai.

2. Incident management

Incident management berfokus pada pemulihan layanan yang secara tidak terduga terdegradasi atau terganggu kepada pengguna secepat mungkin untuk meminimalkan dampak bisnis.

3. *Problem management*

Problem management mencakup analisis akar penyebab untuk mengidentifikasi dan menyelesaikan akar penyebab insiden, dan aktivitas proaktif untuk mengidentifikasi dan mencegah masalah atau insiden di masa depan. Hal ini termasuk juga pembuatan catatan atau *database* kesalahan yang diketahui, yang mendokumentasikan akar penyebab dan solusi untuk memungkinkan diagnosis dan resolusi yang lebih cepat jika insiden lebih lanjut terjadi.

4. *Request fulfilment*

Request fulfilment adalah proses untuk mengelola siklus hidup semua permintaan layanan. Permintaan layanan dikelola sepanjang siklus hidupnya, dari permintaan awal hingga pemenuhan, menggunakan catatan atau tabel pemenuhan permintaan terpisah untuk mencatat dan melacak statusnya.

5. *Access management*

Access management merupakan proses pemberian hak kepada pengguna yang berwenang untuk menggunakan layanan sambil membatasi akses ke pengguna yang tidak berwenang. Hal ini bergantung pada kemampuan untuk secara akurat mengidentifikasi pengguna yang berwenang kemudian mengelola kemampuan mereka untuk mengakses layanan sesuai kebutuhan untuk peran organisasi atau fungsi kerja spesifik mereka.

b. Fungsi dalam *service operation*

Proses saja tidak mengarah pada operasi layanan yang efektif. Infrastruktur yang stabil dan staf yang terampil juga diperlukan. *Service operation* bergantung

pada berbagai fungsi untuk melakukan tugas operasional supaya hal tersebut dapat tercapai. Fungsi mencakup kelompok individu terampil yang melakukan satu atau lebih proses dan aktivitas siklus hidup layanan. Ada empat fungsi utama dalam operasi layanan:

1. *Service desk*

   Service desk adalah titik kontak tunggal bagi pengguna jika terjadi gangguan layanan, untuk permintaan layanan, atau bahkan untuk beberapa kategori *Request for Change* (RFC). *Service desk* adalah titik komunikasi bagi pengguna dan titik koordinasi untuk berbagai kelompok dan proses teknologi informasi.

2. *Technical management*

   Technical management menyediakan keterampilan teknis terperinci dan sumber daya yang diperlukan untuk mendukung operasi berkelanjutan dari layanan teknologi informasi dan pengelolaan infrastruktur teknologi informasi. *Technical management* juga memainkan peran penting dalam merancang, menguji, merilis, dan meningkatan layanan teknologi informasi. Pada organisasi kecil dimungkinkan untuk mengelola keahlian ini dalam satu departemen, tetapi organisasi yang lebih besar biasanya dibagi menjadi beberapa departemen teknis khusus.

3. *IT operations management*

   IT operations management menjalankan kegiatan operasional sehari-hari yang diperlukan untuk mengelola layanan teknologi informasi dan infrastruktur teknologi informasi pendukung. Hal ini dilakukan sesuai dengan standar kinerja yang ditetapkan selama *service design*. Di beberapa organisasi ini merupakan satu departemen terpusat, sementara di organisasi lain terdapat beberapa kegiatan serta staf terpusat dan beberapa disediakan oleh departemen terdistribusi atau khusus. *IT operations management* memiliki dua sub-fungsi yang unik dan umumnya berbeda secara organisasi. Kedua sub-fungsi tersebut, adalah:

   a. *IT operations control*. Ini biasanya dikelola oleh *shift* operator yang memastikan bahwa tugas operasional rutin dilakukan. Kendali operasi teknologi informasi juga menyediakan aktivitas pemantauan

dan pengendalian terpusat, biasanya melalui jembatan operasi atau pusat operasi jaringan.

b. *Facilities management*. Ini mengacu pada pengelolaan lingkungan fisik teknologi informasi, biasanya pusat data atau ruang komputer. Di banyak organisasi, manajemen teknis dan aplikasi ditempatkan bersama dengan operasi teknologi di pusat data besar.

4. *Application management*

Application management bertanggung jawab untuk mengelola aplikasi sepanjang siklus hidupnya. Fungsi manajemen aplikasi mendukung dan memelihara aplikasi operasional dan juga memainkan peran penting dalam merancang, menguji, dan meningkatkan aplikasi yang merupakan bagian dari layanan TI.

ITIL memandang manajemen aplikasi secara berbeda dari pengembangan aplikasi. Di dalam TI, pengembangan aplikasi biasanya difokuskan pada aktivitas internal untuk merancang, membangun, menguji, dan menyebarkan solusi teknologi informasi yang sedang dibangun di dalam organisasi TI. *Application management* mengambil pandangan yang jauh lebih luas yang mengakui kemampuan di pasar saat ini untuk mendapatkan aplikasi dari banyak sumber selain organisasi teknologi informasi internal. Selain itu, ini juga berfokus pada pengelolaan dan pemeliharaan aplikasi yang berkelanjutan yang terjadi setelah aplikasi diterapkan.

2.9 Layanan Teknologi Informasi di Untirta

UPT Data dan Informasi Untirta memiliki layanan teknologi informasi yang dapat membantu pelayanan akademik serta administrasi di Untirta. Terdapat sekitar 33 layanan teknologi informasi yang dimiliki UPT Data dan Informasi Untirta [11]. Layanan ini digunakan untuk mempermudah dalam akses serta efesiensi dalam kebutuhan akademik maupun administrasi universitas dimana saja dan kapan saja.

Beberapa layanan teknologi informasi tersebut diantaranya adalah Sistem Informasi Akademik (SIAKAD)**,** Sistem Informasi Kinerja (SIKITA) Untirta, Sistem Pembelajaran Daring (SPADA), Sistem Informasi Tugas Akhir (SISTA), e-Administrasi, dan Solusi Laporan Terkini Antar Sivitas (SULTANS). Layanan

Untirta yang sering digunakan untuk kebutuhan akademik adalah SIAKAD dan SPADA, sedangkan layanan yang sering digunakan untuk kebutuhan administrasi adalah e-Administrasi.

2.10 *Maturity Model*

Maturity model merupakan alat yang digunakan untuk mengukur seberapa baik kinerja atau proyek sesuatu organisasi atau perusahaan dan seberapa jauh organisasi tersebut melakukan perbaikan berkelanjutan. Tidak seperti alat pengukur yang digerakkan oleh tujuan lainnya, *maturity* model dapat mengevaluasi data kualitatif untuk menentukan lintasan dan kinerja jangka panjang perusahaan. Model bertujuan untuk melihat apakah perusahaan semakin matang, yang berarti mereka terus-menerus menguji, tumbuh, dan berkembang. Model dapat menentukan tingkat efektivitas yang berbeda dan dapat menunjukkan posisi seseorang, tim, proyek, atau perusahaan saat ini dalam model.

Maturity model merupakan hal yang penting, karena memberikan pemantauan kinerja yang fleksibel yang dapat mengungkapkan informasi berharga tentang kesehatan dan potensi perusahaan. Sementara model tidak memperbaiki inefisiensi itu sendiri, model tersebut dapat mengidentifikasi area di mana organisasi tidak beroperasi pada standar dan memungkinkan mereka untuk menentukan strategi yang dapat meningkatkan operasi dan proses mereka [37].

Pada ITIL sendiri terdapat *maturity model* yang didasarkan pada lima tingkat *maturity*. Definisi tingkat kematangan ini selaras dengan definisi COBIT dan CMMI [38].

a. Level 1 (*Initial*)

Pada level ini, proses atau fungsi bersifat *ad hoc*, tidak terorganisir atau kacau. Terdapat bukti bahwa organisasi sudah menyadari bahwa masalah tersebut ada serta perlu ditangani. Akan tetapi, tidak terdapat prosedur standar ataupun kegiatan manajemen proses atau fungsi. Pada level ini, proses atau fungsi dianggap tidak terlalu berarti, dengan sedikit sumber daya yang dialokasikan untuk itu di dalam organisasi. Selain itu, terdapat pendekatan *ad hoc* yang cenderung diterapkan secara individual ataupun bersumber pada tiap kasus. Seluruh pendekatan untuk manajemen tidak terorganisir dengan baik.

b. Level 2 (*Repeatable*)

Pada level ini, proses atau fungsi mengikuti pola yang teratur. Mereka sudah berkembang ke tahap di mana prosedur serupa diiringi oleh orang yang berbeda melaksanakan tugas yang sama. Pelatihan bersifat informal, tidak terdapat komunikasi terkait prosedur standar dan tanggung jawab diserahkan kepada individu. Terdapat tingkat ketergantungan yang tinggi pada pengetahuan individu dan oleh sebab itu kesalahan mungkin terjadi. Secara umum, aktivitas yang berkaitan dengan proses atau fungsi tidak terkoordinasi, tidak teratur, dan mengarah pada efisiensi proses atau fungsi.

c. Level 3 (*Defined*)

Pada level ini, proses atau fungsi sudah diakui dan prosedur sudah distandarisasi, didokumentasikan, serta dikomunikasikan lewat pelatihan. Prosedur tersebut tidak mutakhir, namun merupakan formalisasi dari aplikasi yang sudah ada. Akan tetapi, hal tersebut diserahkan kembali kepada individu untuk mengikuti ataupun tidak sehingga dari hal tersebut penyimpangan dapat terjadi. Proses memiliki pemilik proses, tujuan serta target formal dengan sumber daya yang dialokasikan dan fokus pada efisiensi dan efektivitas.

d. Level 4 (*Managed*)

Pada level ini, proses atau fungsi saat ini sudah sepenuhnya diakui dan diterima di segala teknologi informasi. Level ini berpusat pada layanan dan memiliki target yang didasarkan pada tujuan serta sasaran bisnis. Hal tersebut sepenuhnya ditentukan, dikelola, serta menjadi *pre-emptive*, dengan antarmuka dan dependensi yang terdokumentasi dan mapan ke proses teknologi informasi lainnya. Proses atau fungsi dipantau dan diukur. Kepatuhan terhadap prosedur serta tindakan yang diambil dipantau dan diukur. Proses atau fungsi terus ditingkatkan dan menunjukkan aplikasi terbaik. Otomatisasi dan peralatan semakin banyak digunakan guna menciptakan operasi yang efisien.

e. Level 5 (*Optimized*)

Pada level ini, praktik kerja unggulan diikuti serta diotomatisasi. Sebuah proses perbaikan terus-menerus mandiri didirikan, yang saat ini sudah menciptakan pendekatan *pre-emptive*. Teknologi informasi digunakan secara terintegrasi guna mengotomatisasi alur kerja, menyediakan peralatan untuk meningkatkan mutu dan

daya guna, serta memungkinkan organisasi bisa menyesuaikan diri dengan cepat. Proses atau fungsi mempunyai tujuan serta sasaran strategis yang sejalan dengan bisnis strategis dan tujuan teknologi informasi secara keseluruhan.

Perhitungan nilai *maturity* menggunakan perhitungan yang dirumuskan pada Persamaan (2.1).

$$Maturity\ Level = \frac{Total\ Bobot}{Total\ Responden} \quad (2.1)$$

Pada Persamaan (2.1), nilai *maturity* diperoleh dari hasil total bobot dibagi dengan total responden. Total bobot merupakan jumlah n dikali dengan parameter (n × parameter), dimana n adalah jumlah tanggapan untuk setiap parameter. Sedangkan total responden adalah jumlah orang yang menjadi responden [39].

2.11 Analisis Kesenjangan

Analisis kesenjangan atau *gap analysis* merupakan teknik umum untuk penemuan dan pengelolaan kesenjangan yang dihasilkan selama perencanaan transisi antara keadaan awal dan keadaan target. Analisis kesenjangan adalah sebuah alat atau teknik yang sering digunakan dalam konteks perencanaan strategis. Hal tersebut berkaitan dengan penilaian keadaan atau target yang diinginkan terhadap keadaan saat ini, dengan tujuan untuk memahami kesenjangan antara keduanya [40].

Tingkat kesenjangan menggunakan perhitungan yang dirumuskan pada Persamaan (2.2).

$$Tingkat\ Kesenjangan = Tingkat\ harapan\ - Tingkat\ maturity \quad (2.2)$$

Berdasarkan Persamaan (2.2), tingkat kesenjangan diperoleh dari tingkat harapan dikurangi dengan tingkat *maturity.* Analisis kesenjangan dapat membantu untuk mengetahui bagian-bagian yang memiliki kesenjangan yang besar serta penyebab dari kesenjangan tersebut.

2.12 Kajian Pustaka

Penelitian tentang evaluasi keamanan menggunakan *vulnerability assessment* serta evaluasi manajemen menggunakan ITIL v3 telah dilakukan oleh berbagai pihak. Penelitian tersebut telah dibuktikan melalui karya tulis jurnal yang

telah dipublikasikan. Penelitian-penelitian tersebut dijadikan referensi oleh penulis pada penelitian ini.

Penelitian sebelumnya membahas analisis celah keamanan aplikasi *web learning* pada universitas ABC dengan *vulnerability assessment*. Metode yang digunakan pada penelitian ini adalah *Vulnerability Assesment and Penetration Testing* (VAPT) *Life Cycle*. Hasil analisis didapatkan bahwa *Overall Risk Level Web* Aplikasi berada pada level *High* sehingga diharuskan untuk melakukan perbaikan serta evaluasi sistem [13].

Penelitian selanjutnya membahas *vulnerability assessment* dan analisis model kematangan pada web di pendidikan tinggi di Indonesia. *Vulnerability assessment* dilakukan dengan menggunakan *tools* Nessus dan Skipfish pada beberapa universitas di Jakarta. Hasil penilaian didapatkan 60% dari 33 situs memiliki kematangan dibawah angka 3 yang berarti tingkat kerentanan pada situs web tersebut masih tinggi [15].

Penelitian selanjutnya membahas penggunaan Wireshark dan Nessus untuk analisis SSL/TLS pada keamanan data pengguna *website* Badan Meteorologi Klimatologi dan Geofisika (BMKG). Pengujian dilakukan dengan menggunakan metode penelusuran paket data dengan aplikasi Wireshark dan metode pemindaian *website* berupa *vulnerability assessment* dengan aplikasi Nessus. Hasil menggunakan metode penelusuran paket data didapatkan bahwa web *server* sudah diverifikasi sertifikat SSL/TLS dan *server public key* dengan protokol TLS 1.2 sehingga dapat melindungi data pengguna menggunakan enkripsi client dan *server* menggunakan algoritma hash SHA256. Sementara hasil analisis pemindaian berupa vulnerability assessment menunjukkan level risiko keseluruhan adalah medium [22].

Penelitian selanjutnya membahas evaluasi *maturity level* pada manajemen layanan teknologi informasi di perusahaan *24Slides*. Penelitian tersebut menggunakan *framework* ITIL v3 domain *service operation* untuk mengukur *maturity level*, analisis kesenjangan, serta merumuskan rekomendasi perbaikan. Kuesioner dilakukan pada tiga responden dan kuesioner yang digunakan adalah kuesioner berbasis *Universities and Colleges Information Systems Association*

(UCISA). Hasil penelitian didapatkan skor rata-rata *maturity level* yang bernilai 2,6 dan masuk dalam kategori *repeatable* dengan kesenjangan sebesar 0,8 [14].

Penelitian selanjutnya membahas pengukuran tingkat kematangan ITSM menggunakan *framework* ITIL pada layanan teknologi informasi STMIK Mikroskil. Penelitian tersebut menggunakan *framework* ITIL v3 domain *service operation* untuk mengukur *maturity level*. Kuesioner yang digunakan juga merupakan kuesioner berbasis UCISA. Selain itu terdapat dokumentasi ISO 9001: 2008 yang telah dibuat oleh departemen IT. Hasil penelitian didapatkan *maturity level* dengan nilai rata-rata 2,01 dan masuk dalam kategori *repeatable*. Walaupun sudah ada dokumentasi ISO 9001:2008 terkait tahapan *service operation*, namun belum mengikuti detail proses *framework* ITIL [41].

Penelitian selanjtnya membahas audit tata kelola layanan teknologi informasi di Institusi X. Pada penelitian tersebut, untuk mengukur *maturity level* digunakan *framework* COBIT, sedangkan untuk rekomendasi digunakan *framework* ITIL v3 domain *service operation*. Hasil penelitian didapatkan nilai yang diperoleh dari audit manajemen tata kelola teknologi informasi pada Instansi X adalah 3,19 dan terletak pada level 3 (*Established Process*) [42].

Berdasarkan penelitian tersebut, dapat diketahui bahwa analisis celah keamanan dengan *vulnerability assessment* khususnya menggunakan tool *nessus* dapat mengetahui celah keamanan yang terdapat pada sebuah layanan teknologi informasi khususnya layanan *website*. *Vulnerability assessment* juga dapat mengevaluasi celah keamanan dalam suatu layanan sehingga dapat dilakukan perbaikan pada layanan tersebut. Selain itu juga, dapat diketahui bahwa analisis manajemen dengan *framework* ITIL v3 dapat mengetahui celah keamanan yang terdapat pada sebuah layanan teknologi informasi khususnya layanan *website*.