# BAB IITINJAUAN PUSTAKA

## Penelitian Terdahulu

Penelitian terdahulu berisi tentang kajian penelitian yang mirip, Terkait dan mendukung penelitian saat ini. Di bawah ini adalah 3 penelitian sebelumnya yang digunakan untuk referensi dalam penelitian ini :

### 2.1.1 Pembuatan Standard Operating Procedure (SOP) Service Desk Berdasarkan Kerangka Kerja ITIL V3 dengan Menggunakan Metode Analisis Gap Layanan (Studi Kasus : PT XYZ , Tangerang)

Penelitian yang dilakukan oleh (Annisa Rachmi et al., 2014). Pada penelitian tersebut membahas tentang pembuatan Standard Operating Procedure (SOP) dengan menggunakan metode Analisis Gap Layanan. Penelitian ini melakukan identifikasi terkait kebutuhan dengan Analisis Gap dan membuat beberapa section yang diperlukan untuk Service Desk. Selain itu penelitian ini juga berhasil membuat SOP dengan struktur organisasi *service desk* PT XYZ, kebijakan eskalasi, *Service Level Agreement*, instrument pendukung SOP yang berupa *form-form* mengacu dalam *best practice* yang digunakan dan usulan desain pembuatan aplikasi *knowledge base*. Dari penulisan terdauhulu penulis merancang SOP yang hanya berfokus dengan domain *Service Operation* dan proses yang berpusat dengan *event-management, dan incident-management*.

### 2.1.2 Pembuatan Prosedur Operasional Standar Insiden pada *Government Resources Management System* Kota Surabaya Berdasarkan ITIL V3

Penelitian ini dilakukan oleh (Rizky et al., 2017). Pada penelitian tersebut membahas tentang pembuatan Prosedur Operasional Standar dengan mengacu pada insiden yang terjadi pada pada *Goventment Resources Management System* kota Surabaya dan membagi fokus SOP dengan beberapa bagian yang sesuai dengan insiden terkait. Dari hasil penelitian tersebut menjabarkan beberapa bagian untuk membuat SOP yang ideal bagi objek penulisan tersebut antara lain Penggalian data yang dibagi beberapa tahapan, membuat analisa kondisi kekinian dengan kondisi ideal, melakukan Analisa kesenjangan, dan terakhir adalah pembuatan SOP yang sesuai dan telah di validasi dan verifikasi oleh pihak terkait.

### 2.1.3 Pembuatan Dokumen SOP Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja ISO 27002:2013 (Studi Kasus : CV Cempaka Tulungagung)

Penelitian ini dilakukan oleh (Indra Dheni et al., 2017). Pada penelitian tersebut membahas tentang pembuatan Prosedur Operasional Standar dengan mengacu pada keamanan informasi tata kelola IT yang ada pada CV Cempaka Tulungagung dan membagi fokus SOP dengan beberapa bagian keamanan teknologi informasi yang terkait. Dari hasil penelitian perancangan SOP menggunakan kerangka kerja ISO / IEC 27002:2013 yang berisikan panduan kekinian penerapan keamanan informasi menggunakan bentuk kontrol khusus untuk mencapai tujuan kontrol yang ditetapkan. Di akhir pembahasan penelitian dijelaskan bahwa tidak mengharuskan bentuk-bentuk kontrol yang tertentu dan memberikan kebebasan kepada pengguna ISO / IEC 27002 untuk memilih control yang sesuai dengan kebutuhannya. Maka penelitian terdahulu menghasilkan beberapa rancangan dokumen SOP untuk beberapa fungsi seperti Prosedur pengelolaan hak akses, Prosedur pengelolaan password, Prosedur *backup and restore,* Prosedur perawatan hardware, Prosedur keamanan kabel, Prosedur pengelolaan dan pengembangan SDM.

### 2.1.4 PEMBUATAN STANDARD OPERATING PROCEDURE(SOP) DOMAIN SERVICE DESK BERDASARKAN KERANGKAKERJA ITIL V3

Penelitian ini dilakukan oleh (Haris & Ariandi, 2019). Pada penelitian tersebut membahas tentang pembuatan Prosedur Operasional Standar dengan menggunakan framework ITIL V3 yang berfokus pada domain *service operation* yang mengarah pada layanan *service desk.* Pada penelitian yang dilakukan di dalam PT Sugih Rahayu Bahagia (SRB) memfokuskan pada satu proses saja yaitu *incident management* dengan mengadopsi metode PDCA *(Plan, Do, Check, Act).* Dalam pembahasannya SOP yang ada dalam perusahaan tersebut hanya berupa slide gambar dan tidak terlalu efisien terhadap keberlangsungan kinerja pelayanan serta operasi perusahaan. Dari permasalahan tersebut peneliti ingin menganalisa kekurangan yang ada serta melakukan peningkatan SOP dalam hal layanan. Hasil akhir yang didapatkan adalah SOP yang memiliki langkah awal untuk mengenali insiden dalam layanan teknologi informasi, memberikan ancuan langkah dalam penanganan hingga memulihkan layanan teknologi informasi kembali normal dalam penggunaannya. Maka penelitian terdahulu menghasilkan beberapa rancangan dokumen SOP untuk beberapa fungsi seperti Prosedur pengelolaan hak akses, Prosedur pengelolaan password, Prosedur *backup and restore,* Prosedur perawatan hardware, Prosedur keamanan kabel, Prosedur pengelolaan dan pengembangan SDM.

### 2.1.5 Perencanaan SOP Manajemen Insiden DPMPTSP Kabupaten OKI Menggunakan Framework ITIL V3

Penelitian ini dilakukan oleh (Julian & Sutabri, 2023). Pada penelitian tersebut membahas tentang pembuatan Prosedur Operasional Standar pada Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu (DPMPTSP) dengan menggunakan framework ITIl V3 yang berfokus pada domain *service operation* dengan proses *incident management* saja*.* Dalam pembahasannya DPMPTSP memanfaatkan aplikasi Bidang Pengaduan Kebijakan Dan Pelaporan layanan untuk masyaratakat. Untuk bidang pengaduan ini telah di sediakan aplikasi berbasis website yang dapat mendukung proses bisnis yang dilakukan, seperti menerima pengaduan dari masyarakat, atau untuk menerima dan mengumpulkan Survey Kepuasan Masyarakat(SKM). Dalam pemanfaatan aplikasi tersebut tidak adanya SOP yang mengakibatkan tidak adanya alur yang jelas dan tidak adanya prioritas dalam aktivitas yang dilakukan selama penggunaan aplikasi, selain itu juga tidak adanya IT Staff atau yang dikenal dengan seseorang yang bertanggung jawab dalam pemeliharaan aplikasi, yang mengakibatkan menumpuknya insiden yang terjadi dan tidak tersinkronnya terhadap kebutuhan bisnis dari DPMPTSP. Dari permasalahan tersebut peneliti ingin menyarnakan untuk memaksimalkan penggunaan aplikasi dengan menambah *IT Department* sekaligus menyusun SOP yang berfokus pada penanganan insiden yang terjadi. Hasil akhir yang didapatkan adalah perancangan SOP penanganan insiden, eskalasi, hingga penutupan insden dengan menyarankan untuk menambah IT Department yang khusus untuk mengatasi permasalahan yang terjadi.

### 2.1.6 Hasil Penelitian Terdahulu

Dalam Penelitian terdahulu menghasilkan banyak perbandingan dengan beberapa aspek dari pembuatan Standard Operasional Prosedur.

**2.1.6 Tabel Penelitian Terdahulu**

Tabel 1 Tabel Penelitian Terdahulu

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Judul Penelitian** | **Kelebihan** | **Kekurangan** |
| 1 | Pembuatan Standard Operating Procedure (SOP) Service Desk Berdasarkan Kerangka Kerja ITIL V3 dengan Menggunakan Metode Analisis Gap Layanan (Studi Kasus : PT XYZ , Tangerang) | 1. Hasil akhir dari pembuatan dokumen SOP tersebut adalah terdiri dari 4 prosedur (2 prosedur baru dan 2 prosedur diperbarui), beberapa kebijakan, dan form untuk melengkapi dokumen SOP. Seluruh isi dokumen SOP akan dibukukan terpisah menjadi buku produk dan diserahkan kepada pihak terkait, yaitu Service Desk Manager dan Kepala Divisi TI PT XYZ2. Pengaruh yang didapatkan dari penelitian ini adalah terciptanya dokumen Standard Operating Procedure (SOP) untuk layanan service desk PT XYZ yang dibuat berdasarkan proses-proses yang ada di dalam kerangka kerja ITIL V3 yang terkait dengan fungsi service desk. Dokumen SOP tersebut juga dibuat berdasarkan kebutuhan dan kebijakan oleh pihak-pihak terkait yang memiliki kewenangan untuk mendefinisikan informasi yang dimuat ke dalam dokumen SOP. | 1. Tidak dijelaskan secara rinci mengenai metode yang digunakan dalam pengumpulan data. Hanya disebutkan bahwa metode yang digunakan adalah wawancara, simulasi SOP, dan survey, namun tidak dijelaskan bagaimana proses pengumpulan data dilakukan secara detail.2. Tidak dijelaskan secara rinci mengenai proses verifikasi dan validasi SOP yang telah dibuat. Hanya disebutkan bahwa proses verifikasi dan validasi dilakukan menggunakan metode wawancara dan simulasi SOP, namun tidak dijelaskan bagaimana proses tersebut dilakukan secara detail.3. Tidak dijelaskan secara rinci mengenai hasil dari pengujian SOP yang telah dilakukan. Hanya disebutkan bahwa pengujian SOP dilakukan dengan dua skenario, namun tidak dijelaskan hasil dari pengujian tersebut secara detail.4. Tidak dijelaskan secara rinci mengenai dampak dari implementasi SOP yang telah dibuat terhadap kinerja layanan service desk PT XYZ. Hanya disebutkan bahwa diharapkan dapat meningkatkan efektivitas dan efisiensi layanan service desk, namun tidak dijelaskan secara detail mengenai dampak yang terjadi setelah implementasi SOP tersebut. |
| 2 | Pembuatan Prosedur Operasional Standar Insiden pada *Government Resources Management System* Kota Surabaya Berdasarkan ITIL V3 | 1. Menggunakan metodologi yang sistematis dan terstruktur, sehingga memudahkan dalam pengumpulan data dan analisis data yang dilakukan. 2. Memberikan usulan penambahan aktor dan role yaitu service desk sebagai single point of contact dengan pengguna, yang dapat meningkatkan efektivitas dan efisiensi dalam penanganan insiden. 3. Memberikan usulan penjelasan matrix prioritas, penambahan aktivitas untuk menangani insiden major, dan adanya penambahan aktivitas rekapitulasi log insiden yang harus dilakukan setiap tiga bulan sekali, sehingga dapat meningkatkan kualitas pengelolaan insiden. 4. Mengacu pada standar acuan ITIL V3 dalam melakukan analisis kondisi kekinian dan kondisi ideal, sehingga dapat memastikan bahwa hasil penelitian sesuai dengan standar internasional. 5. Memberikan rekomendasi yang jelas dan terukur, sehingga dapat diimplementasikan oleh Bina Program GRMS untuk meningkatkan kualitas pengelolaan insiden. | 1. Tidak dilakukan pengujian atau simulasi terhadap dokumen SOP yang dihasilkan, sehingga belum dapat dipastikan efektivitas dan efisiensi dari implementasi SOP tersebut. 2. Tidak dilakukan analisis terhadap faktor-faktor yang mempengaruhi keberhasilan implementasi SOP, seperti faktor organisasi, teknologi, dan lingkungan. 3. Tidak dilakukan survei atau wawancara kepada pengguna atau pelanggan GRMS untuk mengetahui kepuasan terhadap pengelolaan insiden yang dilakukan. 4. Tidak dilakukan perbandingan dengan pengelolaan insiden pada organisasi serupa atau sejenis, sehingga belum dapat diketahui sejauh mana pengelolaan insiden pada GRMS sudah memenuhi standar industri. 5. Tidak dilakukan analisis terhadap biaya dan manfaat dari implementasi SOP yang diusulkan, sehingga belum dapat dipastikan apakah implementasi SOP tersebut layak dari segi ekonomi. 6. Tidak dilakukan analisis terhadap risiko dan kendala yang mungkin terjadi selama implementasi SOP, sehingga belum dapat dipastikan apakah implementasi SOP tersebut dapat dilakukan dengan lancar dan tanpa hambatan. |
| 3 | Pembuatan Dokumen SOP Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja ISO 27002:2013 (Studi Kasus : CV Cempaka Tulungagung) | 1. Penelitian ini memberikan kontribusi pada pengembangan keamanan aset informasi pada perusahaan CV Cempaka Tulungagung dengan menghasilkan dokumen SOP keamanan aset informasi yang mengacu pada kontrol kerangka kerja ISO 27002:2013. 2. Penelitian ini menggunakan metode analisis risiko FMEA untuk mengidentifikasi risiko keamanan aset informasi pada perusahaan CV Cempaka Tulungagung. Dengan demikian, perusahaan dapat mengambil tindakan mitigasi yang tepat untuk mengurangi risiko tersebut. 3. Penelitian ini memberikan rekomendasi mitigasi risiko terkait pengelolaan hak akses sistem atau pengaturan username dan password pegawai, serta risiko pada perangkat keras maupun jaringan yang dimiliki. 4. Penelitian ini memberikan pemetaan dari perancangan SOP dengan formulir dan instruksi yang digunakan pada setiap prosedur, sehingga memudahkan pelaksanaan SOP. 5. Penelitian ini memberikan kontribusi pada pengembangan ilmu pengetahuan dan teknologi, khususnya pada bidang keamanan informasi dan manajemen risiko. | 1. Penelitian ini hanya dilakukan pada satu perusahaan yaitu CV Cempaka Tulungagung, sehingga hasil penelitian tidak dapat digeneralisasi untuk perusahaan lain. 2. Penelitian ini hanya menggunakan metode analisis risiko FMEA, sehingga tidak mempertimbangkan faktor-faktor lain yang dapat mempengaruhi keamanan aset informasi seperti faktor sosial, politik, dan ekonomi. 3. Penelitian ini tidak mempertimbangkan faktor-faktor internal perusahaan seperti budaya organisasi, kebijakan manajemen, dan sumber daya manusia yang dapat mempengaruhi keamanan aset informasi. 4. Penelitian ini tidak melakukan pengujian terhadap efektivitas implementasi SOP keamanan aset informasi yang telah dibuat, sehingga tidak dapat diketahui sejauh mana SOP tersebut dapat mengurangi risiko keamanan aset informasi pada perusahaan. 5. Penelitian ini tidak mempertimbangkan faktor-faktor eksternal seperti peraturan dan undang-undang yang berlaku terkait keamanan aset informasi, sehingga SOP yang dibuat mungkin tidak sesuai dengan peraturan dan undang-undang yang berlaku. |
| 4 | PEMBUATAN STANDARD OPERATING PROCEDURE(SOP) DOMAIN SERVICE DESK BERDASARKAN KERANGKAKERJA ITIL V3 | 1. Menggunakan metode observasi dan metode PDCA (Plan, Do, Check, Act) yang terbukti efektif dalam mengidentifikasi permasalahan dan meminimalisir kesalahan serta kerugian pengeluaran yang dilakukan serta penanggulangan keadaan yang terjadi saat terjadi kejadian. 2. Menghasilkan panduan kerja *incident* management yang berbasis framework ITIL V3 yang membantu dalam menetapkan proses pencatatan, penanganan, dan penyelesaian insiden. 3. Panduan kerja yang telah dihasilkan dapat digunakan untuk mengenali insiden layanan IT dan memberikan acuan langkah dalam melakukan tindakan penanganan hingga memulihkan layanan IT kembali secara normal, sesuai dengan proses *incident* management pada ITIL V3. 4. Dokumen rencana *incident* management yang dihasilkan dapat secara langsung digunakan sebagai panduan dalam menangani insiden layanan IT. 5. Jurnal ini memberikan informasi yang cukup detail tentang proses pengelolaan insiden pada PT Sugih Rahayu Bahagia (SRB) dan memberikan solusi untuk meningkatkan pengelolaan insiden tersebut dengan menggunakan framework ITIL V3. | 1. Tidak dijelaskan secara rinci mengenai hasil evaluasi atau pengukuran efektivitas dari implementasi SOP berbasis ITIL V.3 pada PT Sugih Rahayu Bahagia (SRB). 2. Tidak dijelaskan secara rinci mengenai kendala atau hambatan yang dihadapi selama proses pembuatan SOP berbasis ITIL V.3 pada PT Sugih Rahayu Bahagia (SRB). 3. Tidak dijelaskan secara rinci mengenai bagaimana proses implementasi SOP berbasis ITIL V.3 pada PT Sugih Rahayu Bahagia (SRB) dilakukan, termasuk bagaimana pelatihan dan sosialisasi dilakukan kepada karyawan. 4. Tidak dijelaskan secara rinci mengenai bagaimana SOP berbasis ITIL V.3 pada PT Sugih Rahayu Bahagia (SRB) dapat diintegrasikan dengan sistem manajemen layanan IT yang sudah ada di perusahaan. 5. Tidak dijelaskan secara rinci mengenai bagaimana SOP berbasis ITIL V.3 pada PT Sugih Rahayu Bahagia (SRB) dapat diadopsi oleh perusahaan lain yang memiliki karakteristik dan kebutuhan yang berbeda. |
| 5 | Perencanaan SOP Manajemen Insiden DPMPTSP Kabupaten OKI Menggunakan Framework ITIL V3 | adanya identifikasi kesenjangan antara kondisi saat ini dengan kondisi ideal berdasarkan ITIL V3. Hal ini memungkinkan untuk mengetahui area yang perlu diperbaiki dan diatur dengan SOP yang lebih jelas dan terstruktur, seperti SOP penanganan insiden, eskalasi insiden, dan penutupan insiden. Dengan adanya SOP yang lebih jelas dan terstruktur, diharapkan dapat meminimalisir kesalahan yang dapat terjadi dan meningkatkan kinerja operasional DPMPTSP Kabupaten Ogan Komering Ilir dalam memberikan layanan kepada masyarakat. Selain itu, penelitian ini juga memberikan panduan dan pedoman manajemen insiden standar internasional yang dapat diterapkan oleh instansi lain yang memiliki layanan berbasis TI. | 1. Penelitian ini hanya dilakukan pada satu instansi, yaitu DPMPTSP Kabupaten Ogan Komering Ilir, sehingga hasilnya tidak dapat digeneralisasi untuk instansi lain yang memiliki karakteristik dan kondisi yang berbeda. 2. Penelitian ini hanya fokus pada manajemen insiden dan tidak membahas aspek lain dari manajemen layanan TI, seperti manajemen perubahan, manajemen kapasitas, dan manajemen keamanan. 3. Penelitian ini hanya menggunakan ITIL V3 sebagai acuan, sementara saat ini sudah ada versi terbaru dari ITIL, yaitu ITIL 4. Hal ini dapat mempengaruhi relevansi dan aktualitas rekomendasi yang diberikan. 4. Penelitian ini hanya menggunakan metode deskriptif kualitatif, sehingga tidak dilakukan analisis statistik untuk menguji hipotesis atau mengukur tingkat signifikansi dari hasil penelitian. |

## Teknologi Informasi

Teknologi informasi adalah proses yang mencakup segala sesuatu yang berhubungan dengan penggunaan komputer untuk memproses informasi dan penggunaan alat untuk mentransfer data dari satu perangkat ke perangkat lainnya. (Bessen, 2017) melampirkan bahwa TI telah diadopsi secara luas di banyak industry sejak tahun 1970-an, namum se iring berjalannya waktu investasi TI di dalam perusahaan semakin bergeser ke dalam perangkat lunak dan khususnya aplikasi khusus saja.

## Information Technology Service Management (ITSM)

*IT Service Management* atau dikenal dengan Manajemen Layanan Teknologi Informasiadalah suatu tata kelola yang menyelaraskan antara proses bisnis dengan organisasi yang memfokuskan dalam area layanan teknologi informai. Manajemen Layanan Teknologi Informasi (MLTI) memiliki peran untuk mengukur tingkat pelayanan yang ada dalam organisasi tersebut. Dalam karyanya (Riche, 2018) mengungkapkan bahwa Manajemen Layanan Teknologi Informasi mengadopsi suatu pendekatan yang melibatkan penggunaan alat yang dikenal sebagai *IT Infrastructure Library* (ITIL). Konsep Manajemen Layanan Teknologi Informasi timbul dari pengakuan bahwa teknologi informasi memiliki keterkaitan yang kuat dengan berbagai layanan yang tersedia di dalam lingkungan organisasi.

## Information Technology Infrastructure Library(ITIL)

*Information Technology Infrastructure Library* (ITIL) merupakan *framework* yang menggambarkan *best practice* dalam penerapan manajemen layanan teknologi informasi (Annisa Rachmi et al., 2014). Dalam kerangka kerja ITIL merupakan suatu solusi yang di perlukan untuk meningkatkan layanan teknologi informasi yang ada di dalam organisasi. *Framework* ITIL memiliki beberapa bagian yaitu :

* *Service Strategy* : *Service Strategy* adalah membuat manajemen layanan yang lebih baik dalam organisasi dengan menyelaraskan strategi layanan IT yang konsisten.
* *Service Design* : *Service Design* memberikan panduan bagi organisasi TI untuk merancang layanan TI secara sistematis sebagai praktik terbaik dan mengimplementasikan ITSM.
* *Service Transition* : *Service Transition* adalah mengembangkan kemampuan untuk memindahkan hasil desain layanan TI yang diubah ke dalam produksi.
* *Service Operation* : *Service Operation* mencakup semua kegiatan operasional sehari-hari dalam mengelola layanan TI. Banyak tahapan panduan tentang cara mengelola layanan TI secara efisien dan efektif dan memastikan tingkat kinerja pengguna.
* *Continual Service Improvement* :Tahapan terakhir adalah melakukan perbaikan yang efektif secara terus – menerus dengan beberapa Langkah seperti Proses perbaikan, Pengukuran Layanan, dan Pelaporan Layanan.



Gambar 1 ITIL Life-Cycle

**Gambar 2.4 ITIL *Life-Cycle***

## Service Operation

*Service Operation* mengacu pada aktivitas dan proses yang terlibat dalam mengelola dan memberikan layanan TI dalam suatu organisasi, *Service Operation* berfokus pada operasi sehari-hari dan dukungan layanan teknologi informasi untuk memastikan pengiriman yang efektif dan efisien kepada pelanggan(Muharman Lubis et al., 2020). (Muharman Lubis et al., 2020) juga mengutarakan bahwa *Service Operation* sangat penting untuk menjaga stabilitas dan ketersediaan layanan teknologi informasi, mengurangi gangguan, dan memastikan bahwa kebutuhan dan harapan pelanggan terpenuhi. *Service operation* juga memiliki beberapa proses didalamnya yaitu :

* *Incident Management* (Manajemen Insiden): Proses ini berfokus pada menangani insiden dan gangguan dalam layanan teknologi informasi. Tujuan utamanya adalah mengembalikan layanan ke kondisi normal secepat mungkin setelah gangguan terjadi dan mengurangi dampak buruknya pada bisnis.
* *Problem Management*, juga dikenal sebagai "Manajemen Masalah", adalah proses yang bertujuan untuk menemukan sumber utama dari satu atau lebih peristiwa dan mengambil tindakan yang dapat mencegah masalah tersebut muncul kembali. Ini menghasilkan peningkatan keandalan dan kualitas layanan.
* *Event Management* (Manajemen Peristiwa): Proses ini mengawasi dan mengelola peristiwa dalam lingkungan teknologi informasi. Peristiwa dapat berupa kejadian biasa atau tidak biasa, seperti log masuk, pengingat kontrak, atau peringatan kegagalan sistem.
* *Request Fulfillment*, juga dikenal sebagai Pemenuhan Permintaan, adalah proses yang menangani permintaan rutin pengguna, seperti permintaan akses, perubahan data, atau informasi. Tujuan utamanya adalah memastikan permintaan ini diproses dengan cepat dan efektif.
* *Management Access* (Manajemen Akses): Prosedur ini bertanggung jawab untuk memastikan bahwa pengguna memiliki akses yang tepat untuk menggunakan layanan teknologi informasi. Ini mencakup pengelolaan identitas, autentikasi, otorisasi, dan tindakan terkait lainnya.
* *IT Operations Control* (Kontrol Operasi IT): Proses ini berkonsentrasi pada pengawasan harian, pelaporan, dan kegiatan operasional IT. Ini mencakup pemantauan kinerja, penjadwalan tugas rutin, dan koordinasi aktivitas operasional lainnya.
* *Facilities Management* (Manajemen Fasilitas): Mengelola fasilitas fisik yang mendukung layanan teknologi informasi, seperti pusat data, ruang server, dan lingkungan lainnya, adalah bagian dari proses manajemen fasilitas.
* *Application Management* (Manajemen Aplikasi): Proses ini berkaitan dengan pengelolaan dan perawatan aplikasi di bidang teknologi informasi. Ini mencakup koordinasi dengan tim pengembang aplikasi, mengelola siklus hidup aplikasi, dan mengelola pembaruan.

Adapaun beberapa fungsi dari domain *Service Operation* didalamnya meliputi :

* *Service Desk* : Berfungsi sebagai *single point of contact* (SPOC) antara pengguna dan penyedia layanan. Fungsi ini juga memberikan dukungan dan informasi yang diperlukan, serta menerima laporan masalah, permintaan, dan pertanyaan pengguna.
* *Technical Management*: Fungsi ini berfokus pada manajemen infrastruktur teknis yang mendukung layanan teknologi informasi. Manajemen teknik bertanggung jawab untuk merencanakan, mengimplementasikan, dan mengelola infrastruktur teknologi informasi seperti jaringan, perangkat keras, dan perangkat lunak.
* *IT Operations Management*: Fungsi ini mengawasi kinerja, penjadwalan pekerjaan, manajemen kapasitas, dan tugas-tugas harian lainnya untuk memastikan layanan TI berjalan dengan baik.
* *Application Management*: Fungsi ini bertanggung jawab atas manajemen dan dukungan aplikasi yang digunakan dalam layanan teknologi informasi. Ini termasuk pemeliharaan aplikasi, pengembangan, pemecahan masalah, dan kolaborasi dengan tim pengembang untuk memastikan aplikasi memenuhi kebutuhan bisnis.
* *IT Facilities Management*: Fungsi ini menangani manajemen fasilitas fisik yang mendukung layanan teknologi informasi, seperti pusat data dan ruang server. Manajemen fasilitas teknologi informasi bertanggung jawab atas pemeliharaan, keamanan, dan efisiensi operasional fasilitas tersebut.

## Event Management

*Event Management* adalah serangkaian aktivitas untuk *scanning* pesan abnormal dari infrastruktur teknologi informasi dan melakukan sesuatu untuk mencegah hal yang buruk terjadi dan mempengaruhi pengguna (Irsad et al., 2022). Dalam tahapan sebelum melakukan *scanning,* Perusahaan harus lebih dulu menentukan batas atau *limit* dari *Event* yang terkait dengan aplikasi atau program. Juga dalam tinjauan Pustaka sebelumnya yang dilakukan oleh (Irsad et al., 2022) *tools* dalam *Event Management* dapat menerima pesan yang nantinya dapat di identifikasi dan memutuskan tindakan apa yang harus diambil, apakah mengabaikannya atau diteruskan kepada manajemen layanan atau staff teknologi informasi yang terkait. Menurut *framework* ITIL V3 aktifitas di dalam *Event Management* memiliki beberapa poin seperti :

* *Event Occurs : Event occurs* (peristiwa terjadi) dalam *framework Service Operation* dari ITIL V3 adalah kejadian yang terjadi selama operasi layanan IT. Ini meliputi peristiwa seperti perubahan konfigurasi, masalah kinerja, atau kegagalan sistem. Pada tahap ini, tim *Service Operation* akan mendeteksi, mencatat, dan mengklasifikasikan peristiwa tersebut. Tujuannya adalah memantau lingkungan operasional, mengidentifikasi perubahan yang signifikan, dan merespons dengan cepat jika ada dampak negatif pada layanan. Dengan memahami dan mengelola peristiwa yang terjadi, tim dapat mengoptimalkan kinerja layanan dan mengurangi gangguan bagi pengguna akhir.
* *Event notification : Event Notification* adalah semakin bermakna data yang dikandungnya dan semakin tepat sasaran penggunannya, maka semakin mudah untuk membuat keputusan tentang *event* tersebut. Operator seringkali dihadapkan pada pesan kesalahan berkode dan tidak tahu bagaimana meresponsnya atau apa yang harus dilakukan dengan pesan tersebut. Data yang diperloeh memberikan peran serta tanggung jawab yang jelas serta didokumentasikan selama *service design* dan *transition service*. Jika peran dan tanggung jawab tidak didefinisikan dengan jelas, dalam keadaan siaga tidak ada yang tahu siapa yang melakukan apa dan hal ini dapat menyebabkan banyak hal yang terlewatkan atau upaya yang terduplikasi.
* *Event detection : Event detection* (deteksi peristiwa) dalam framework *Service Operation* dari ITIL V3 adalah proses mengidentifikasi, memantau, dan melaporkan peristiwa yang terjadi selama operasi layanan teknologi informasi. Ini melibatkan penggunaan alat dan teknologi untuk mendeteksi indikasi peristiwa, seperti perubahan konfigurasi, kegagalan layanan, atau kejadian tak terduga lainnya. Dengan *event* *detection*, tim *Service Operation* dapat merespons dengan cepat, mengambil tindakan yang diperlukan, dan mengurangi dampak negatif pada layanan. Penerapan *event* detection memungkinkan pengelolaan proaktif, pemantauan real-time, serta pemulihan yang cepat dalam menghadapi peristiwa yang mempengaruhi operasi layanan teknologi informasi.
* *Event logged : Event logged* (pencatatan peristiwa) dalam framework *Service Operation* dari ITIL V3 melibatkan pencatatan secara terstruktur dan sistematis semua peristiwa yang terjadi selama operasi layanan teknologi informasi. Ini termasuk informasi seperti waktu, deskripsi, pengaruh, dan tindakan yang diambil. Pencatatan peristiwa memungkinkan analisis dan pemantauan yang efektif, membantu mengidentifikasi pola dan tren, serta memfasilitasi evaluasi pasca-peristiwa. Dengan *event logging*, tim *Service Operation* dapat melacak dan mengelola peristiwa dengan lebih baik, mengambil keputusan yang lebih baik, dan meningkatkan responsivitas terhadap perubahan atau masalah yang muncul selama operasi layanan IT.
* *First - level event correlation and filtering : First level event correlation and filtering* (korelasi dan penyaringan peristiwa tingkat pertama) dalam framework *Service Operation* dari ITIL V3 adalah proses menghubungkan dan menganalisis peristiwa yang terjadi untuk mengidentifikasi pola, keterkaitan, dan hubungan penyebab-akibat. Dalam tahap ini, peristiwa yang relevan diambil, disaring, dan digabungkan menjadi kejadian yang lebih signifikan. Hal ini membantu dalam mengurangi kebisingan, fokus pada peristiwa yang penting, dan memahami dampaknya terhadap layanan teknologi informasi. *First-level event correlation and filtering* memungkinkan respons yang lebih efisien dan efektif terhadap perubahan dan masalah yang terjadi dalam operasi layanan IT.
* *Significance of events : Significance of events (signifikansi peristiwa)* dalam framework *Service Operation* dari ITIL V3 adalah penilaian terhadap pentingnya peristiwa yang terjadi selama operasi layanan IT. Ini melibatkan evaluasi dampaknya terhadap layanan, pelanggan, dan bisnis secara keseluruhan. Dengan memahami signifikansi peristiwa, tim *Service Operation* dapat memberikan prioritas yang tepat, mengalokasikan sumber daya dengan bijaksana, dan mengambil tindakan yang sesuai. Evaluasi signifikansi peristiwa juga membantu dalam mengidentifikasi tren, pola, dan masalah potensial yang mempengaruhi operasi layanan IT. Dengan memperhatikan signifikansi peristiwa, respons dan penanganan insiden dapat dioptimalkan untuk menjaga kontinuitas layanan yang efektif.
* *Second level event correlation :  Second-level event correlation* (korelasi peristiwa tingkat kedua) dalam framework *Service Operation* dari ITIL V3 adalah proses lanjutan untuk menghubungkan dan menganalisis peristiwa yang terkumpul dari tingkat pertama. Ini melibatkan penggabungan, pemodelan, dan korelasi lebih lanjut untuk mengidentifikasi pola yang lebih kompleks, mengungkapkan hubungan sebab-akibat yang lebih dalam, serta memahami dampaknya terhadap layanan IT secara holistik. Dengan *second-level event correlation*, tim *Service Operation* dapat memiliki pemahaman yang lebih lengkap tentang masalah dan perubahan yang sedang terjadi, memfasilitasi pemecahan masalah yang lebih efektif, dan meningkatkan kecepatan dan kualitas respons terhadap peristiwa yang mempengaruhi operasi layanan IT.
* *Further action required ? : Further action required* (tindakan lanjutan yang diperlukan) dalam proses *event management* dalam framework *Service Operation* dari ITIL V3 mengacu pada langkah tambahan yang harus diambil setelah peristiwa atau masalah terdeteksi. Ini melibatkan evaluasi lebih lanjut, pemecahan masalah mendalam, dan tindakan proaktif untuk mencegah atau mengurangi dampak negatif. Tindakan lanjutan yang diperlukan dapat mencakup pemanggilan tim respons, penerapan solusi sementara, pemantauan lanjutan, atau perencanaan langkah-langkah pemulihan. Dengan mengenali dan menindaklanjuti tindakan lanjutan yang diperlukan, tim *Service Operation* dapat merespons dengan cepat, meminimalkan downtime, dan memastikan kelancaran operasi layanan IT secara keseluruhan.
* *Response Selection : Response selection* (pemilihan respons) dalam proses *event management* dalam framework *Service Operation* dari ITIL V3 adalah tahap di mana tim *Service Operation* memilih tindakan yang tepat untuk merespons peristiwa yang terjadi. Ini melibatkan evaluasi dan pemilihan respons yang sesuai dengan tingkat kepentingan, urgensi, dan dampak peristiwa terhadap layanan IT. *Respons* dapat mencakup tindakan perbaikan sementara, eskalasi ke tim yang lebih tinggi, atau pengambilan tindakan pemulihan. Dengan melakukan response selection yang tepat, tim *Service Operation* dapat merespons dengan cepat dan efektif terhadap peristiwa, mengurangi dampak negatif, dan memastikan kelancaran operasi layanan IT.
* *Review actions : Review actions* (meninjau tindakan) dalam proses *event management* dalam framework *Service Operation* dari ITIL V3 adalah tahap di mana tim *Service Operation* mengevaluasi dan memeriksa tindakan yang telah diambil sebagai respons terhadap peristiwa. Ini melibatkan analisis efektivitas tindakan, identifikasi perbaikan yang mungkin, dan pembelajaran dari pengalaman. Dengan melakukan *review actions* secara sistematis, tim dapat meningkatkan keputusan dan tindakan di masa depan, mengoptimalkan proses respons, dan mencegah terulangnya peristiwa serupa. *Review actions* membantu dalam pengembangan kontinu dan peningkatan kualitas layanan IT dalam jangka panjang.
* *Close event : Close event* (menutup peristiwa) dalam proses *event management* dalam framework *Service Operation* dari ITIL V3 adalah tahap terakhir di mana peristiwa dianggap selesai dan dicatat sebagai penyelesaian. Ini melibatkan penilaian dan konfirmasi bahwa peristiwa telah ditangani dengan sukses, layanan telah pulih, dan tidak ada dampak yang berkelanjutan. *Close event* juga mencakup pencatatan informasi terkait, evaluasi kualitas respons, dan pengarsipan data terkait peristiwa. Dengan menutup peristiwa secara tepat, tim *Service Operation* dapat melengkapi siklus penanganan peristiwa, melacak kejadian masa lalu, dan memastikan rekam jejak yang lengkap dalam manajemen layanan IT.



Gambar 2 Arus proses Event-Management

**Gambar 2.5 Arus proses *Event-Management***

## Incident Management

*Incident Management* adalah suatu proses yang ada di dalam bagian ITIL V3 Service Operation(Irsad et al., 2022). *Incident* dapat di definisikan sebagai gangguan atau penurunan kualitas layanan TI (Palilingan & Batmetan, 2018). Menurut *framework* ITIL V3 aktifitas di dalam *Incident Management* memiliki beberapa poin seperti :

* Idenfitikasi *Incident Management* mengacu pada langkah awal dalam mengenali dan mengidentifikasi kejadian atau insiden yang memerlukan respons. Ini melibatkan pemantauan sistem dan lingkungan untuk mendeteksi indikasi potensi masalah, pelanggaran keamanan, atau peristiwa yang tidak diinginkan. Identifikasi yang efektif memungkinkan tim *incident* management untuk merespons dengan cepat, mengambil tindakan pencegahan atau mitigasi yang sesuai, serta meminimalkan dampak negatif. Dengan memahami dan mengidentifikasi *incident* dengan tepat, proses *incident* management dapat dilakukan dengan lebih efisien dan efektif untuk menjaga kelancaran operasional dan keamanan.
* *Incident Logging* dalam proses *incident management* melibatkan pencatatan detail lengkap tentang setiap insiden atau kejadian yang terjadi. Hal ini bertujuan untuk mencatat informasi penting seperti waktu kejadian, deskripsi insiden, pihak terkait, langkah-langkah yang diambil, dan hasil tindakan. Dengan pencatatan insiden yang akurat, tim *incident management* dapat memiliki rekaman yang terperinci dan dapat dijadikan referensi untuk analisis pasca-insiden, perbaikan proses, dan perencanaan kejadian mendatang. *Incident* logging juga membantu dalam pelaporan kejadian kepada pihak berwenang dan untuk keperluan audit atau penilaian keamanan.
* *Incident categorization* (kategori insiden) dalam proses *incident* management di dalam domain *Service Operation* dari framework ITIL v3 adalah tahap di mana insiden diklasifikasikan berdasarkan atribut dan karakteristiknya. Ini melibatkan pengelompokan insiden ke dalam kategori yang telah ditentukan sebelumnya, seperti perangkat keras, perangkat lunak, jaringan, atau aplikasi. Categorization membantu dalam pemahaman yang lebih baik tentang jenis insiden yang terjadi, memudahkan pelaporan, pemantauan, dan analisis data. Dengan kategori insiden yang jelas, tim Service Operation dapat mengalokasikan sumber daya secara efisien, merujuk pada kejadian serupa di masa lalu, dan mengidentifikasi tren atau pola yang relevan untuk meningkatkan manajemen insiden di masa mendatang.
* *Incident Priority* adalah melibatkan evaluasi dampak bisnis, kebutuhan pelanggan, serta konsekuensi operasional dalam menentukan prioritas penanganan. *Incident priority* membantu dalam alokasi sumber daya dengan bijaksana, memastikan insiden yang memiliki dampak besar atau mengancam bisnis mendapatkan perhatian segera, sementara insiden yang memiliki dampak rendah diberikan prioritas yang lebih rendah. Dengan menggunakan *incident priority*, tim *incident management* dapat merespons dengan cepat dan efektif, mengoptimalkan waktu dan sumber daya yang tersedia.
* *Initial diagnosis* (diagnosis awal) dalam proses *incident management* di dalam domain *Service Operation* dari framework ITIL v3 2011 adalah tahap di mana tim melakukan evaluasi awal terhadap insiden yang dilaporkan. Ini melibatkan identifikasi gejala, analisis informasi yang tersedia, dan penentuan penyebab yang mungkin. Initial diagnosis membantu dalam pemahaman awal tentang sifat insiden, memungkinkan prioritas yang tepat, dan memandu langkah-langkah respons selanjutnya. Dengan melakukan diagnosis awal yang efektif, tim dapat mengambil tindakan yang tepat, mengurangi waktu pemulihan, dan meminimalkan dampak negatif pada layanan IT dan pengguna akhir. *Incident Escalation* adalah tindakan untuk meningkatkan tingkat penangan *Incident*.
* *Incident escalation* (eskaklasi insiden) dalam proses *incident* management di dalam domain *Service Operation* dari framework ITIL v3 2011 adalah langkah yang diambil ketika insiden tidak dapat ditangani oleh tim saat ini. Ini melibatkan peningkatan tingkat eskalasi kepada tim yang lebih tinggi, seperti tim spesialis atau manajemen, untuk memperoleh bantuan dan kepemimpinan tambahan dalam menyelesaikan insiden. Eskalasi insiden memastikan bahwa masalah yang kompleks atau kritis mendapatkan perhatian yang tepat, koordinasi tim yang diperlukan, dan sumber daya yang memadai untuk memulihkan layanan IT dengan segera. Dengan melakukan eskalasi yang tepat, insiden dapat diatasi secara efektif dan dalam waktu yang singkat.
* *Investigation and diagnosis* (investigasi dan diagnosis) dalam proses *incident management* di dalam domain *Service Operation* dari *framework* ITIL v3 2011 adalah tahap di mana tim melakukan penyelidikan dan analisis mendalam terhadap insiden. Ini melibatkan pengumpulan data, pengujian, dan pemantauan untuk mengidentifikasi akar penyebab insiden. Selanjutnya, dilakukan diagnosa untuk memahami dampaknya pada layanan dan pengguna. Dengan melakukan investigasi dan diagnosis yang komprehensif, tim dapat menentukan langkah-langkah pemulihan yang tepat, mencegah kejadian serupa di masa depan, dan meningkatkan kualitas dan ketersediaan layanan IT.
* Resolusi (*resolution and recovery*) Ini melibatkan upaya untuk menyelesaikan insiden dengan mengembalikan layanan ke keadaan normal secepat mungkin. *Resolution* berfokus pada mengidentifikasi dan menerapkan tindakan yang diperlukan untuk mengatasi akar penyebab insiden, sementara *recovery* berkaitan dengan mengembalikan layanan ke tingkat yang dapat diterima. Tujuan utamanya adalah mengurangi dampak pada bisnis dan pelanggan serta memastikan keberlanjutan operasional. Proses *resolution and recovery* membutuhkan koordinasi tim yang efektif dan penggunaan best practice untuk mencapai pemulihan yang sukses.
* *Closing* (*incident closure*) adalah tahap akhir dalam manajemen insiden di mana insiden dianggap selesai dan ditutup secara formal. Ini melibatkan verifikasi bahwa insiden telah diselesaikan, pemantauan untuk memastikan tidak ada dampak berkelanjutan, evaluasi pelaksanaan tindakan, dan penutupan catatan insiden. *Incident closure* juga melibatkan pembelajaran dari insiden yang terjadi untuk meningkatkan proses dan mencegah kejadian serupa di masa mendatang. Tujuan utamanya adalah memulihkan layanan secepat mungkin dan meminimalkan dampak negatif pada operasi TI.



Gambar 3 Arus Proses Incident - Management

**Gambar 2.6 Arus Proses *Incident - Management***

## Standart Operasional Prosedur (SOP)

Pengertian Standar Operasional Prosedur adalah sebuah pedoman pelaksanaan administrasi untuk meningkatkan pelayanan dalam suatu organisasi(Annisa Rachmi et al., 2014). Dalam penerapannya membantu membentuk suatu fungsi kerja serta *flow* kerja yang dinamis, serta setiap kerangka kerja dapat di pertanggung jawabkan dan memberikan gambaran tujuan pekerjaan yang dilaksanakan sesuai dengan kebijakan dan peraturan yang berlaku. Perancangan SOP mengacu pada Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan.

## Gambaran umum obyek penelitian

Gambaran umum obyek penelitian yang digunakan dalam penelitian ini adalah PT Surya Jawara Eco yang menjadi salah satu kelompok bisnis produk layanan dan produk otomotif di Indonesia, yang didirikan pada tahun 2002. PT Surya Jawara Eco melakukan distribusi produk otomotif untuk kebutuhan pasar bisnis. PT Surya Jawara Eco menggunakan aplikasi *sales monitoring* untuk membantu memantau dari alur bisnis yang dilakukan serta membantu dalam rekap data. Dalam penanggung jawaban aplikasi *Sales Monitoring* saat ini sedang dipegang oleh *Chief Technology Officer (CTO)* beserta tim *developer* selaku *Project Manager* dalam perusahaan. *Developer* yang dinaungi oleh CTO hanya berfokus pada layanan problem yang terjadi dan mengarahkan kepada pihak *outsourcing .* Penggunaan Aplikasi *sales monitoring* dibagi menjadi 2, Aplikasi berbentuk *website* untuk melihat statistika penjualan dan rekap data keseluruhan bisnis. Sales monitoring berbentuk *website* hanya bisa diakses oleh *Chief Executive Officer(CEO), Chief Technology Officer(CTO)*, dan *Chief Operating Officer(COO)*. Sementara itu untuk aplikasi berbentuk *Mobile* berisikan transaksi penjualan, stock barang masuk dan keluar, di dalamnya dapat di akses oleh *Sales*.

**Gambar 2.8 Struktur Organisasi**

Gambar 4 Struktur Organisasi