# Incident Management - Manajemen Insiden

***ITIL® 4 Practice Guide***

***Raihanda Naufal Ashava - 6026242013***

---

## ● Informasi Umum

- **Tujuan Manajemen Insiden**

  Tujuan dari melakukan penerapan manajemen insiden adalah meminimalkan dampak negatif dari insiden dengan mengembalikan layanan ke kondisi normal secepat mungkin.

  **Contoh:**

  Di perusahaan e-commerce, server database melambat karena penggunaan tinggi. Walaupun pelanggan belum menyadarinya, tim IT sudah tahu dari monitoring bahwa performa menurun dari standar yang disepakati (misal: waktu respon > 1 detik). Maka, tim segera melakukan tindakan untuk mengembalikan kecepatan ke kondisi normal sebelum pelanggan terkena dampaknya.

- **Kata Kunci**
  - ❖ Insiden - *Incident*

    Insiden adalah gangguan tak terencana pada layanan atau penurunan kualitas layanan.

    **Contoh:**

    Situs e-commerce tidak bisa diakses karena server overload. Ini termasuk insiden yang harus segera ditangani agar pelanggan bisa kembali berbelanja.

  - ❖ Model Insiden - *Incident Model*

    Model Insiden merujuk kepada pendekatan standar yang bisa diulang untuk menangani jenis insiden tertentu. Fungsi dari memiliki model insiden adalah dapat mempercepat dan mempermudah penanganan insiden yang sering terjadi dengan solusi yang sudah terbukti.

    **Contoh:**

    Misalnya setiap kali printer kantor mengalami error karena konflik driver, tim IT langsung ikuti langkah-langkah perbaikan standar yang sudah terdokumentasi dalam model insiden.

❖ Insiden Besar - *Major Incident*

*Major Incident* adalah insiden yang memiliki dampak besar terhadap bisnis dan perlu penanganan cepat dan terkoordinasi. Karakteristik dari insiden yang memiliki dampak besar yaitu seperti, dampak bisnis yang signifikan (misalnya layanan penting berhenti), kompleksitas tinggi atau menyebabkan gangguan di banyak sistem, perlu penanganan darura**t** dengan sumber daya khusus, dan butuh komunikasi intensif ke pengguna, manajemen, bahkan media.

**Struktur Penanganan Insiden Besar:**

1. Kriteria Identifikasi
   Ditentukan sejak awal (misalnya jika memengaruhi > 50% user, downtime > 1 jam, dll).
2. *Major Incident Manager* (MIM)
   Orang yang ditugaskan untuk memimpin, mengoordinasikan, dan memastikan penanganan insiden besar berjalan efektif.
3. Tim Penanganan Khusus (*War Room / Swarming Team*)
   Gabungan dari berbagai tim ahli: jaringan, aplikasi, database, keamanan, dsb.
4. Sumber Daya Tambahan
   Anggaran khusus, konsultan eksternal, komponen hardware/software darurat.
5. Model Komunikasi
   Jalur komunikasi ke user, manajemen, mitra, bahkan regulator sudah disiapkan dan teruji.
6. Dokumentasi & Review
   Setelah insiden selesai → dilakukan post-incident review untuk evaluasi dan pembelajaran.

**Contoh:**

Insiden: Website E-commerce down di tengah flash sale nasional.

Penanganan:

- Dinyatakan sebagai *Major incident* karena menyangkut pendapatan besar & reputasi.
- *Swarming* tim backend, frontend, server, dan devops.
- Komunikasi aktif di social media & email pelanggan.
- Setelah pulih, dilakukan evaluasi sistem *load balancing*.

❖ Solusi Sementara - *Workaround*

*Workaround* atau solusi sementara adalah solusi yang mengurangi dampak insiden atau masalah, meski belum menyelesaikannya secara permanen. Dalam melakukan solusi yang bersifat semetara terdapat catatan bahwa solusi ini dapat dengan cepat membantu operasional tetap jalan, tapi bisa juga menambah beban perbaikan di masa depan (*technical debt*). *Workaround* sendiri dapat digunakan ketika saat solusi permanen belum tersedia, saat butuh pemulihan layanan cepat (misalnya layanan penting harus tetap jalan), dan untuk insiden yang tidak kritis namun berulang.

**Contoh:**

Misalnya terdapat situasi bahwa aplikasi HR tidak bisa diakses untuk mengajukan cuti. Solusi sementara yang bisa dilakukan adalah menggunakan Google Form untuk input cuti sementara agar proses cuti tetap berjalan.

❖ Utang Teknis - *Technical Debt*

*Technical debt* adalah akumulasi pekerjaan yang muncul karena memilih solusi sementara (*workaround*) daripada solusi yang benar secara teknis. Sama seperti "utang" yang harus dibayar nanti: makin lama dibiarkan, makin besar dan sulit dibereskan. Dengan kata lain hubungan antara penerapan solusi sementara dan utang teknis adalah jika *workaround* dibiarkan menumpuk tanpa solusi permanen maka akan menjadi utang teknis.

**Contoh:**

Tim IT membuat skrip sementara untuk mengatasi error pada sistem login karyawan agar layanan tetap berjalan. Solusi ini efektif dalam jangka pendek, tapi karena tidak segera diganti dengan perbaikan permanen, skrip tersebut menimbulkan masalah baru seperti celah keamanan dan integrasi yang gagal. Akhirnya, perbaikan jadi lebih rumit dan memakan biaya.

- **Lingkup Manajemen Insiden**

Cakupan utama dalam melakukan praktik manajemen insiden mencakup aktivitas sebagai berikut:

1. Mendeteksi dan mencatat insiden
2. Mendiagnosis dan menyelidiki insiden
3. Memulihkan layanan ke kondisi normal
4. Mengelola catatan insiden
5. Berkomunikasi dengan pihak terkait sepanjang siklus insiden
6. Meninjau insiden dan melakukan perbaikan setelahnya

Ada beberapa aktivitas atau kegiatan yang tidak termasuk dalam praktik manajemen insiden, meskipun masih berkaitan erat dengan hal tersebut. Aktivitas-aktivitas ini dapat ditangani oleh praktik ITIL lain, bukan manajemen insiden secara langsung, misalnya:

| Aktivitas | Dapat Ditangani Oleh |
|---|---|
| Mencari akar penyebab insiden | Manajemen Masalah (*Problem Management*) |
| Berkomunikasi dengan pengguna | Meja Layanan (*Service Desk*) |
| Menerapkan perubahan pada produk dan layanan | Pemberdayaan Perubahan (*Change Enablement*)<br>Manajemen Deployment (*Deployment Management*)<br>Manajemen Infrastruktur dan Platform (*Infrastructure and Platform Management*)<br>Manajemen Proyek (*Project Management*)<br>Manajemen Rilis (*Release Management*)<br>Manajemen Pengembangan Perangkat Lunak (*Software Development and Management*) |
| Memonitor teknologi, tim, dan performa pihak ketiga (*supplier*) | Manajemen Pemantauan dan Acara (*Monitoring and Event Management*) |
| Mengelola inisiatif perbaikan secara berkelanjutan | Perbaikan Berkelanjutan (*Continual Improvement*) |
| Mengelola dan memenuhi permintaan layanan dari pengguna | Manajemen Permintaan Layanan (*Service Request Management*) |
| Mengembalikan layanan dalam situasi bencana (*disaster recovery)* | Manajemen Keberlangsungan Layanan (*Service Continuity Management)* |

**Contoh Kasus:**

Sebuah perusahaan fintech mendapati aplikasi mobile-nya sering mengalami lambat (lag) saat banyak pengguna mengakses secara bersamaan, terutama setiap Senin pagi. Tim IT sering menerima laporan insiden dari pengguna tentang lambatnya proses login dan transaksi. Setiap kali insiden terjadi, tim manajemen insiden langsung menanganinya dengan *restart server* dan mengosongkan cache, sehingga layanan bisa pulih dalam waktu singkat. Namun, masalah tetap berulang setiap minggu. Maka insiden-insiden ini mulai dianalisis lebih lanjut sebagai masalah (*problem*) oleh tim yang berbeda. Dapat disimpulkan bahwa, manajemen insiden hanya menyembuhkan “gejala”, tapi manajemen masalah menyelesaikan akar permasalahan agar insiden tidak terulang.

- **Faktor Keberhasilan Praktik**

Faktor keberhasilan praktik atau *Practice Success Factor* adalah komponen penting dari suatu praktik yang harus ada agar tujuan praktik tersebut dapat tercapai secara efektif. PSF bukan sekadar aktivitas tunggal, tetapi gabungan dari keempat dimensi dalam manajemen layanan, yaitu orang (tim), proses, teknologi, dan mitra atau supplier. Dalam Manajemen Insiden, terdapat 3 PSF utama, yaitu:

1. Mendeteksi Insiden Sejak Dini

   Sebelumnya, insiden sering baru terdeteksi setelah pengguna melapor. Sekarang, dengan teknologi modern, insiden sebaiknya terdeteksi otomatis oleh sistem monitoring, bahkan sebelum pengguna menyadarinya. Dengan menerapkan ini, organisasi dapat memperoleh waktu layanan terganggu lebih singkat, beberapa insiden bisa ditangani sebelum berdampak, dan meningkatkan kepuasan pelanggan dan efisiensi tim

   **Contoh:**
   Monitoring server mendeteksi lonjakan CPU 90% dan langsung mengirim alert ke tim IT, sehingga mereka segera bertindak sebelum layanan down dan pelanggan terdampak. Dengan memanfaatkan teknologi pendukung seperti penerapan AI/ML untuk deteksi pola insiden serta menerapkan monitoring tools seperti Zabbix, Prometheus, dll.

2. Menyelesaikan Insiden Secara Cepat dan Efisien

   Setelah insiden terdeteksi, resolusi yang cepat dan tepat sangat penting agar layanan segera pulih dan tim tidak terbebani. Insiden harus ditangani secara cepat dan efisien dengan mempertimbangkan kompleksitasnya. Berikut merupakan cara menangani insiden berdasarkan kompleksitasnya.

| Situasi | Penanganan |
|---|---|
| Insiden umum/berulang | Menggunakan model insiden (solusi standar, bahkan otomatis) |
| Insiden kompleks | Ditangani oleh tim spesialis dengan diagnosis mendalam |
| Insiden sangat kompleks | Gunakan teknik *swarming* (kolaborasi banyak ahli dari berbagai bidang) |

*Swarming* sendiri merujuk kepada teknik untuk menyelesaikan tugas-tugas kompleks, di mana beberapa orang dari berbagai bidang keahlian bekerja bersama pada satu masalah sampai terlihat jelas siapa yang paling tepat untuk menangani bagian tertentu. Dengan menerapkan *swarming* organisasi dapat mengatasi

insiden yang kompleks, terutama yang tidak diketahui penyebabnya, memanfaatkan kolaborasi lintas fungsi, dan meningkatkan efisiensi dan kecepatan dalam menemukan solusi. Penting untuk memastikan kualitas data insiden yang tinggi sejak langkah pertama penanganan insiden. Hal ini memiliki pengaruh yang kuat pada:

- Akurasi pengambilan keputusan
- Kecepatan pemulihan layanan
- Efisiensi penggunaan sumber daya
- Kemampuan menemukan akar masalah
- Kualitas *machine learning* (jika digunakan)

**Contoh:**
Saat layanan pembayaran error, sistem langsung menerapkan skrip otomatis untuk restart modul terkait. Jika gagal, tim back-end dan database langsung swarming untuk investigasi bersama.
Teknik Pendukung : *Swarming*, Analisis log, Safe-to-fail experiments (uji coba aman), Machine Learning untuk diagnosis pola insiden

3. Meningkatkan Pendekatan Manajemen Insiden Secara Berkelanjutan

Setelah insiden selesai, tim perlu melakukan review berkala untuk, menganalisis insiden besar/baru, Menemukan pola insiden berulang, memperbaiki model insiden, dan menambah dokumentasi solusi.

Jenis Review:

- Individu (*Post-Incident Review*): untuk insiden besar atau gagal ditangani tepat waktu
- Berkala (*Periodic Review*): review semua insiden dalam jangka waktu tertentu

**Contoh:**
Dalam 1 bulan, tim IT menerima 40 insiden terkait login VPN gagal. Solusinya beragam dan tidak terdokumentasi. Akibatnya, waktu penyelesaian rata-rata 2 jam.
Tindakan Perbaikan:

- Dilakukan review bulanan untuk mengidentifikasi pola.
- Ternyata, 80% kasus terkait kesalahan konfigurasi DNS.
- Dibuat model insiden VPN berisi langkah-langkah perbaikan standar.
- Artikel dipublikasikan di knowledge base internal.

- **Pengukuran Keberhasilan Manajemen Insiden (*Key Metrics*)**

Penggunaan *Key Metrics* dalam manajemen insiden bertujuan untuk menentukan seberapa baik praktik manajemen insiden dijalankan melalui pengukuran yang terukur, objektif, dan relevan, yang biasa disebut dengan *Key Metrics* atau KPI (*Key Performance Indicators*). Dalam melakukan pengukuran keberhasilan praktik manajemen insiden harus selaras dengan 3 *Practice Success Factors* (PSF). Berikut merupakan contoh *Key Metrics* berdasarkan PSF.

1. Mendeteksi Insiden Sejak Dini

| *Key Metrics* | Penjelasan |
|---|---|
| Waktu antara kejadian dan deteksi insiden | Semakin pendek waktunya → semakin baik deteksi sistem |
| Persentase insiden yang terdeteksi oleh monitoring otomatis | Idealnya makin tinggi, karena tidak tergantung laporan manual dari pengguna |

**Contoh:**
80% insiden jaringan terdeteksi oleh sistem monitoring otomatis sebelum pengguna mengeluh → ini menunjukkan deteksi dini berjalan efektif.

2. Menyelesaikan Insiden Secara Cepat dan Efisien

| *Key Metrics* | Penjelasan |
|---|---|
| Waktu dari deteksi hingga diagnosis | Seberapa cepat insiden bisa dipahami oleh tim |
| Jumlah eskalasi antar tim | Jika terlalu sering, bisa jadi tanda proses belum optimal |
| Tingkat penyelesaian di kontak pertama (*first-time resolution rate*) | Semakin tinggi, artinya dokumentasi dan model insiden efektif |
| Persentase waktu tunggu dalam penanganan insiden | Waktu yang terbuang sebelum insiden benar-benar ditangani |
| Persentase insiden yang diselesaikan secara otomatis | Otomatisasi yang efektif menurunkan beban tim |
| Kepuasan pengguna terhadap penanganan insiden | Diukur lewat survey atau feedback setelah insiden selesai |
| Persentase insiden yang diselesaikan sesuai SLA | Apakah insiden ditangani tepat waktu sesuai standar layanan |

**Contoh:**

Semisal pada sistem email internal tiba-tiba tidak bisa mengirim pesan. Monitoring tool seperti Zabbix langsung mendeteksi SMTP service mati pukul 10:00 WIB dan user baru melapor ke helpdesk pukul 10:15 WIB. Jadi, insiden berhasil terdeteksi **15 menit lebih awal** sebelum dilaporkan oleh pengguna.

3. Meningkatkan Pendekatan Manajemen Insiden Secara Berkelanjutan

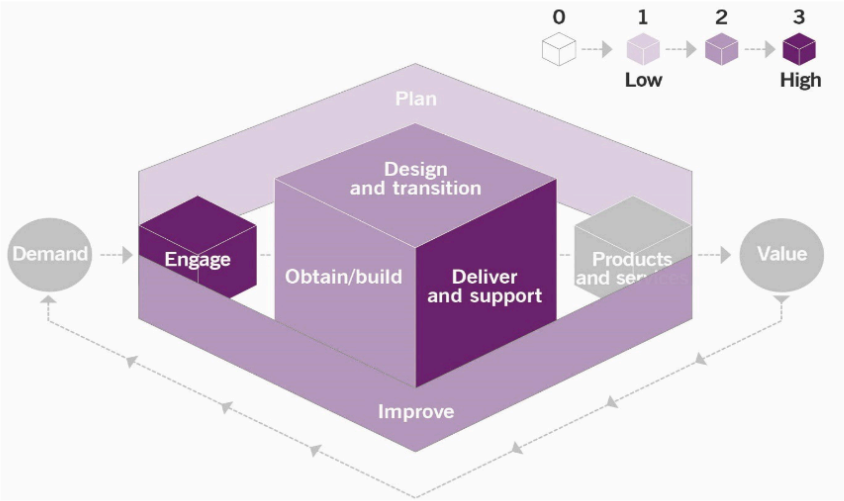
| *Key Metrics* | Penjelasan |
|---|---|
| Persentase insiden yang diselesaikan menggunakan solusi terdokumentasi | Menandakan penggunaan *knowledge base* |
| Persentase insiden yang memakai model insiden | Menunjukkan standar proses sudah digunakan |
| Peningkatan nilai metrik dari waktu ke waktu | Apakah praktik membaik dari bulan ke bulan |
| Keseimbangan antara kecepatan & efektivitas | Jangan hanya cepat, tapi juga benar dan stabil |

**Contoh:**
Untuk metrik tren perbaikan dari waktu ke waktu. Pada sebuah perusahaan pada bulan Januari rata-rata waktu penyelesaian sebuah insiden selama 4 jam, lalu di bulan Februari turun menjadi 3 jam, dan di bulan Maret turun lagi jadi 2,5 jam
→ Terlihat ada tren perbaikan dari waktu ke waktu → hasil dari proses evaluasi dan dokumentasi yang baik.

## ● Aliran Nilai dan Proses

- **Kontribusi Praktik Manajemen Insiden terhadap Aliran Nilai**

*Value stream* atau aliran nilai sendiri merujuk kepada serangkaian aktivitas yang dilakukan untuk menciptakan nilai bagi pelanggan atau organisasi. Seperti praktik ITIL lainnya, insiden manajemen tidak berdiri sendiri, melainkan berkontribusi pada berbagai *value stream* dalam siklus layanan. Contohnya meski tujuan utamanya adalah menyelesaikan insiden, praktik lain seperti Service Desk dan Software Development juga terlibat secara tidak langsung.




Gambar diatas menunjukkan tingkat kontribusi Manajemen Insiden terhadap tiap aktivitas dalam *Service Value Chain* (rantai nilai layanan), dengan skala 0 (tidak ada) sampai 3 (tinggi). Praktik manajemen insiden fokus pada pemulihan layanan normal secepat mungkin di berbagai lingkungan kerja. Oleh karena itu, ia berkontribusi kuat pada aktivitas berikut dalam *Service Value Chain*:

| Aktivitas Rantai Nilai | Tingkat Kontribusi | Peran Incident Management |
|---|---|---|
| Engage | 3 (Tinggi) | Menyambut dan merespons laporan insiden dari pengguna |
| Deliver & Support | 3 (Tinggi) | Aktivitas utama — menangani insiden, memulihkan layanan, dan memberi dukungan langsung |
| Design & Transition | 2 (Sedang) | Memberi masukan dari insiden ke proses desain layanan yang lebih baik |
| Improve | 2 (Sedang) | Memberikan data & insight dari insiden untuk peningkatan proses |
| Obtain/Build | 2 (Sedang) | Kadang memerlukan pengembangan tools, skrip, atau fitur pendukung untuk solusi insiden |

**Contoh:**

Terdapat aplikasi mobile e-banking sering crash setelah update. Lalu kontribusi Incident Management adalah sebagai berikut:

- Engage: Helpdesk menerima laporan user → membuat tiket insiden

- Deliver & Support: Tim IT investigasi dan menemukan error log → menerapkan workaround.
- Obtain/Build: Developer membuat patch darurat untuk mencegah crash ulang.
- Design & Transition: Masukan dari insiden dimasukkan ke proses UAT agar lebih ketat.
- Improve: Dilakukan post-incident review → proses deployment diperbaiki.

- **Proses-proses**

Setiap praktik dapat mencakup satu atau lebih proses dan kegiatan yang mungkin diperlukan untuk memenuhi tujuan praktik tersebut. Proses adalah serangkaian aktivitas yang saling berhubungan atau saling mempengaruhi, yang mengubah input menjadi output. Proses menerima satu atau lebih input yang sudah didefinisikan, lalu menghasilkan output yang juga sudah ditentukan. Proses juga menjelaskan urutan tindakan dan hubungan antar langkah-langkahnya. Terdapat dua proses utama, yaitu

1. Menangani dan Menyelesaikan Insiden

Ini adalah proses inti dari praktik manajemen insiden, tujuannya adalah mengembalikan layanan ke kondisi normal secepat mungkin, serta meminimalkan dampak ke pengguna dan bisnis.

| Input | Aktivitas | Output |
|---|---|---|
| Data pemantauan dan peristiwa (monitoring and event data) | Deteksi insiden | Catatan insiden |
| Pertanyaan/pelaporan dari pengguna | Registrasi insiden | Komunikasi status insiden |
| Informasi konfigurasi (dari CMDB) | Klasifikasi insiden | Permintaan investigasi masalah |
| Informasi aset TI | Diagnosis insiden | Permintaan perubahan (change request) |
| Katalog layanan | Penyelesaian insiden | Laporan insiden |
| SLA dengan konsumen dan mitra | Penutupan insiden | Pembaruan basis pengetahuan |
| Informasi kapasitas dan kinerja | | CI (komponen layanan) dan layanan yang telah dipulihkan |

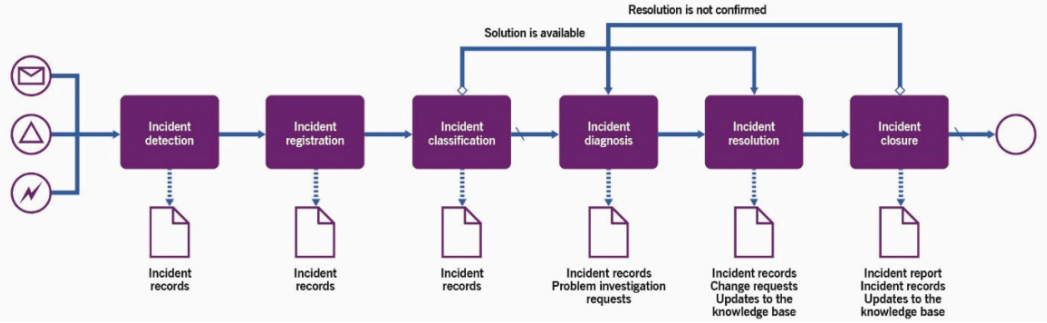
| | | |
|---|---|---|
| Kebijakan dan rencana kesinambungan layanan | | |
| Kebijakan dan rencana keamanan informasi | | |
| Catatan masalah (problem records) | | |
| Basis pengetahuan (knowledge base) | | |

**Contoh:**

Input: Tiket dari helpdesk + alert dari monitoring

Aktivitas: Tiket dicatat → diklasifikasi → diatasi oleh tim L1 → layanan kembali normal

Output: Sistem berjalan kembali, tiket ditutup, catatan tersedia




Gambar diatas menunjukkan *workflow* (alur kerja) dari proses penanganan insiden secara umum, mulai dari deteksi hingga penutupan. Berikut merupakan penjelasan langkah-langkah dalam *workflow* tersebut.

1. *Incident Detection* (Deteksi Insiden)
   Insiden dikenali, baik dari laporan pengguna atau sistem monitoring otomatis.
2. *Incident Registration* (Registrasi Insiden)
   Insiden dicatat ke dalam sistem (ITSM tool) oleh service desk atau sistem otomatis.
3. *Incident Classification* (Klasifikasi Insiden)
   Insiden dikategorikan berdasarkan tipe, dampak, urgensi, dan siapa yang harus menangani.
4. *Incident Diagnosis* (Diagnosis Insiden)
   Dilakukan analisis untuk menemukan akar masalah atau gejala teknis yang terjadi.
5. *Incident Resolution* (Penyelesaian Insiden)

Solusi diterapkan untuk memulihkan layanan.

6. *Incident Closure* (Penutupan Insiden)
   Setelah layanan kembali normal dan disetujui pengguna, insiden ditutup dan didokumentasikan.

2. Meninjau dan Meningkatkan Penanganan Insiden Secara Berkala

Proses ini merupakan proses yang mendukung perbaikan berkelanjutan (*continual improvement*). Tujuannya adalah menganalisis data insiden, mengidentifikasi pola insiden berulang, menemukan peluang perbaikan, dan meningkatkan dokumentasi dan model insiden.

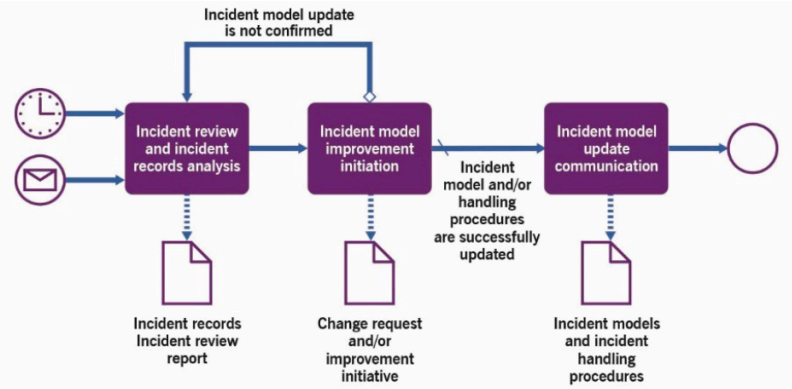
| Input | Aktivitas | Output |
|---|---|---|
| Model dan prosedur insiden saat ini | Tinjauan insiden dan analisis catatan insiden | Model insiden yang diperbarui |
| Catatan insiden | Inisiasi perbaikan model insiden | Prosedur penanganan insiden yang diperbarui |
| Laporan insiden | Komunikasi pembaruan model insiden | Catatan insiden |
| Kebijakan dan peraturan yang berlaku | | Komunikasi tentang pembaruan model dan prosedur insiden |
| Informasi konfigurasi sistem | | Permintaan perubahan |
| Informasi aset TI | | Inisiatif perbaikan |
| SLA (Perjanjian Layanan) dengan pihak lain | | Laporan tinjauan insiden |
| Informasi kapasitas dan performa sistem | | |
| Kebijakan dan rencana keberlanjutan | | |
| Kebijakan dan rencana keamanan | | |

**Contoh:**

Misalnya, suatu perusahaan IT mengalami banyak insiden (gangguan layanan) dalam sebulan. Tim operasional mengumpulkan semua catatan dan laporan

insiden yang terjadi (masukan). Mereka lalu melakukan analisis untuk melihat pola dan kelemahan dalam prosedur yang ada (aktivitas).

Jika ditemukan bahwa banyak insiden terjadi karena kesalahan konfigurasi, maka mereka memperbarui model dan prosedur penanganan insiden (keluaran). Mereka juga mengajukan permintaan perubahan sistem dan membuat inisiatif peningkatan layanan.




Gambar diatas menunjukkan *workflow* (alur kerja) dari proses meninjau dan meningkatkan penanganan insiden secara berkala. Proses tinjauan insiden berkala mengikuti tiga langkah utama, yaitu

1. Tinjauan dan Analisis Catatan Insiden
   Mengevaluasi insiden-insiden sebelumnya dan catatannya dan menghasilkan laporan tinjauan insiden dan catatan insiden
2. Inisiasi Perbaikan Model Insiden
   Jika perlu perbaikan, ajukan perubahan atau inisiatif peningkatan. Jika tidak perlu diperbarui Proses dihentikan (tidak ada pembaruan model/prosedur). Hasil dari tahap ini adalah permintaan perubahan atau inisiatif perbaikan
3. Pembaruan dan Komunikasi
   Jika disetujui dan berhasil diperbarui, prosedur baru dikomunikasikan dan menghasilkan prosedur dan model insiden yang diperbarui

## ● Organisasi dan Manusia

- **Peran, Kompetensi, dan Tanggung Jawab**

  Prinsip Umum:

  ➢ ITIL tidak mewajibkan jabatan formal seperti Practice Owner atau Coach.
  ➢ Fokusnya adalah pada peran-peran fungsional yang bisa dipegang oleh siapa saja

➢ Satu orang bisa menjalankan banyak peran, dan satu peran bisa dipegang oleh banyak orang.

Setiap peran ditandai dengan profil kompetensi berdasarkan model yang ditunjukkan pada tabel dibawah ini.

| Kode | Jenis Kompentensi | Contoh Peran |
|---|---|---|
| L | Leader | Mengambil keputusan, mengatur orang lain, memberi motivasi |
| A | Administrator | Menyusun laporan, mencatat tugas, melakukan perbaikan dasar |
| C | Coordinator/communicator | Koordinasi antar tim, menjaga komunikasi dengan pihak terkait |
| M | Method Expert | Mendesain dan memperbaiki proses kerja, dokumentasi |
| T | Technical Expert | Ahli teknis, menyelesaikan masalah teknis, konsultasi teknis |

❖ Peran *Incident Manager* (Manajer Insiden)

Tanggung Jawab Utama:

- Mengkoordinasikan penyelesaian insiden di suatu area (misal: produk, teknologi, wilayah).
- Memantau pekerjaan tim dan memastikan insiden ditangani dengan benar.
- Menyebarkan informasi status insiden ke seluruh organisasi.
- Melakukan evaluasi berkala atas proses manajemen insiden.

Dalam insiden besar, bisa ada Major Incident Manager (MIM) — fokus hanya pada insiden besar, punya kewenangan lebih.

Kompetensi Dibutuhkan:

LCTA (Leader, Communicator, Technical expert, Administrator)

❖ Peran Lain yang Terlibat dalam Manajemen Insiden

| Aktivitas | Peran Terlibat | Kompetensi | Keterampilan |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Deteksi insiden | Spesialis teknis, pengguna | TC | Memahami desain layanan dan dampak bisnis |
| Registrasi insiden | Manajer insiden, agen helpdesk | AT | Mengoperasikan tools ITSM, dokumentasi |
| Klasifikasi insiden | Agen helpdesk, spesialis teknis | TC | Pahami model insiden, komitmen penyelesaian |
| Diagnosis insiden | Spesialis teknis, pemasok | TC | Analisis teknis, pakai alat diagnosis |
| Resolusi insiden | Spesialis teknis, pengguna | T | Menerapkan solusi atau prosedur teknis |
| Penutupan insiden | Agen helpdesk, manajer insiden | ACT | Dokumentasi lengkap dan validasi penyelesaian |
| Tinjauan insiden | Manajer insiden, pemilik layanan | TCL | Review penyebab, usulkan perbaikan |
| Komunikasi pembaruan | Manajer insiden, agen helpdesk | CA | Menyampaikan pembaruan prosedur baru |

- **Struktur Organisasi dan Tim**

Dalam ITIL, tidak memaksakan untuk suatu model struktur organisasi tertentu. Hal terpenting adalah organisasi punya cara mengelompokkan orang-orang yang memiliki keahlian berbeda secara efisien. Organisasi biasanya membagi spesialis berdasarkan:

1. Bidang teknis (misalnya: jaringan, server, database)
2. Produk/layanan tertentu (misalnya: tim khusus untuk sistem ERP)
3. Wilayah teritorial (misalnya: tim Jakarta, Surabaya)

4. Tipe pelanggan (misalnya: tim VIP support, tim pelanggan retail)

Organisasi perlu fleksibel agar bisa menarik anggota tim dari berbagai departemen internal dan bahkan mitra eksternal saat diperlukan.

- Model Tim Bertingkat (*Tiered*) vs. Rata (*Flat*)
  - ➔ Model Tim Bertingkat

    Model tradisional yang terdiri dari L1 – L2 – L3:

| Tingkat | Tugas |
|---|---|
| L1 | Service desk → menangani insiden ringan dan umum |
| L2 | Tim teknis → tangani insiden lebih rumit yang tidak bisa ditangani L1 |
| L3 | Spesialis/vendor → tangani insiden kompleks atau yang butuh eskalasi |

    Masalah Model Ini:
    - Proses lambat karena terlalu banyak eskalasi
    - Informasi tidak mengalir bebas antar level
    - Tidak fleksibel untuk insiden kritis
  - ➔ Model Tim Rata
    - Lebih fleksibel & kolaboratif
    - Mengandalkan kerja sama langsung lintas tim
    - Cocok untuk organisasi modern (DevOps, Agile)

  Contoh Perubahan Pendekatan:

  Daripada L1 meneruskan ke L2 → buat pasangan kerja langsung (pairing) untuk selesaikan insiden

  Di L3 → kolaborasi antar tim untuk ganti peran ahli yang terlalu tergantung

  **Contoh Kasus:**

  Dalam sistem e-commerce:

  Model Tiered: Helpdesk (L1) → Developer (L2) → Vendor payment gateway (L3)

  Model Flat: Saat checkout error, langsung bentuk tim swarming: developer + QA + network → masalah lebih cepat selesai

- Dinamika Tim (*Team Dynamics*)

  Dinamika tim merupakan elemen yang sangat penting karena interaksi dalam tim menentukan kelancaran dan keberhasilan manajemen insiden.

  Masalah yang Sering Terjadi:

- Insiden dilempar ke tim lain, tanpa kepemilikan
- Tim tidak punya kendali → frustrasi
- Budaya "hero" → hanya satu orang yang tahu cara menyelesaikan
- Komunikasi buruk → solusi lambat, tim tidak termotivasi

Berikut merupakan 3 Elemen Budaya Tim yang Sehat:

1. Tanggung Jawab Kolektif (*Collective Responsibility*)
   Tim harus berbagi tanggung jawab, bukan saling lempar tugas. Walau satu orang memimpin, semua anggota aktif terlibat membantu.
   **Contoh:**
   Ali yang menerima tiket tetap mengajak Budi (network) dan Santi (DevOps) untuk menyelesaikan insiden bersama → hasilnya lebih cepat.
2. Budaya Tanpa Menyalahkan (*No-Blame Culture*)
   Tim didorong untuk mencari solusi tanpa takut disalahkan jika idenya gagal. Kalau tim takut disalahkan, mereka jadi pasif atau tidak mau mencoba solusi baru.
   **Contoh:**
   Ide Santi gagal saat mencoba restart container. Tapi tim tidak menyalahkan, malah membahas bareng dan menemukan solusi yang benar.
3. Pembelajaran Berkelanjutan (*Continual Learning*)
   Pelajaran dari insiden harus dibagikan agar semua tim bisa belajar dan berkembang bersama. Termasuk dari eksperimen yang gagal sekalipun.
   **Contoh:**
   Setelah insiden besar, tim buat review dan menulis artikel pengetahuan. Artikel itu membantu menyelesaikan insiden serupa 3 minggu kemudian.

## ● Teknologi dan Informasi

- **Pertukaran Informasi**

  Keberhasilan praktik manajemen insiden sangat tergantung pada kualitas informasi yang digunakan dan dipertukarkan antar pihak yang terlibat. Semakin lengkap dan akurat informasi yang dikumpulkan → semakin cepat dan tepat insiden bisa diselesaikan. Berikut adalah jenis informasi utama yang harus dikumpulkan selama proses manajemen insiden:

  - Pelanggan dan pengguna layanan
  - Desain dan arsitektur layanan
  - Mitra dan pemasok, termasuk kontrak dan SLA
  - Kebijakan dan peraturan terkait layanan
  - Kepuasan pemangku kepentingan terhadap praktik insiden

  Informasi penting terkait insiden itu sendiri:

| Jenis Informasi | Penjelasan |
|---|---|
| Sumber informasi | Siapa atau sistem apa yang melaporkan insiden |
| Referensi produk/layanan/CI | Komponen mana yang bermasalah |
| Pengguna/layanan yang terdampak | Siapa yang terpengaruh dan bagaimana |
| Gejala penurunan performa | Apa yang tidak normal? (misalnya: lambat, gagal login) |
| Waktu kejadian gejala | Kapan gejala pertama terlihat |
| Waktu terakhir layanan normal | Untuk menentukan sejak kapan layanan gagal |
| Perbaikan otomatis? | Apakah sistem sudah mencoba memperbaiki? Kalau gagal, kenapa? |
| Dampak ke operasional | Seberapa besar gangguan terhadap aktivitas bisnis |
| Sistem terkait lainnya | Apakah ada sistem lain yang terganggu atau tetap normal |
| Kronologi kejadian | Langkah-langkah yang terjadi hingga gejala muncul |

Informasi tambahan yang akan dipertukarkan dan dicatat selama praktik manajemen insiden manajemen insiden harus mencakup rincian tentang:

- Penyelidikan, seperti apakah dilakukan investigasi mendalam? Catat prosesnya
- Tindakan yang diambil, semua tindakan, skrip, perubahan yang dilakukan, dan hasilnya

- **Otomatisasi dan Alat untuk Manajemen Insiden**

Tujuan utama penggunaan alat dan otomatisasi adalah untuk mempercepat proses manajemen insiden, mengurangi pekerjaan manual, dan meningkatkan efisiensi dan akurasi. Otomatisasi sangat berguna, terutama untuk organisasi besar dengan volume insiden tinggi.

Kapan Otomatisasi Cocok Digunakan?

- Untuk aktivitas yang berulang dan bisa diprediksi
- Untuk insiden dengan solusi yang sudah diketahui
- Saat butuh tanggapan cepat tanpa keterlibatan manusia langsung
- Ketika ingin mengurangi waktu tanggap dan penyelesaian

Berikut adalah tabel ringkasan aktivitas proses insiden yang dapat diotomatisasi, alat yang digunakan, dan dampaknya:

- Proses Penanganan dan Penyelesaian Insiden

| Aktivitas | Otomatisasi | Fungsionalitas | Dampak |
|---|---|---|---|
| Incident detection | Monitoring & event correlation tools | Deteksi dini dan pemicu proses manajemen insiden | Tinggi |
| Incident registration | Workflow & user query tools | Pencatatan insiden secara efisien | Tinggi |
| Incident classification | ML tools, knowledge base, config mgmt tools | Klasifikasi cepat & akurat, identifikasi solusi & insiden besar | Sangat tinggi |
| Incident diagnosis | Investigation tools + kolaborasi + knowledge base | Diagnosa cepat dan kolaboratif, pengujian hipotesis, kerjasama tim | Tinggi |
| Incident resolution | Remote access tools, deployment automation | Pemulihan cepat, terutama layanan jarak jauh | Tinggi |
| Incident closure | Workflow & collaboration tools | Dokumentasi akhir otomatis, pelaporan lengkap | Sedang (medium) |

- Proses Review Insiden Berkala

| Aktivitas | Otomatisasi | Fungsionalitas | Dampak |
|---|---|---|---|
| Incident review & root cause analysis | Collaboration & analytics tools | Analisis insiden, pelaporan tren, survei pengguna | Sedang ke tinggi |
| Incident model improvement initiation | Workflow systems, backlog tools | Registrasi formal inisiatif perbaikan | Rendah ke sedang |
| Incident model update | Komunikasi & kolaborasi tools | Menginformasikan update ke tim | Sedang ke tinggi |

| | | | |
|---|---|---|---|
| communications | | terkait | |

**Contoh Implementasi Alat Otomatisasi:**
Kasus: Server aplikasi mati mendadak
Tanpa Otomatisasi:
Monitoring alert → staf melihat manual → buat tiket → tim L2 terima → remote login → restart service → catat penyelesaian
Dengan Otomatisasi:

- Zabbix mendeteksi down
- Tiket otomatis dibuat di Jira
- Skrip restart dijalankan otomatis
- Status insiden diupdate otomatis
- Jika gagal → tim L2 langsung diberi notifikasi

Hasil:
Waktu pemulihan berkurang dari 30 menit jadi 5 menit

## ● Mitra dan Pemasok

Hampir semua layanan TI saat ini tidak dibangun sepenuhnya oleh satu organisasi sendiri, melainkan:

- Mengandalkan pihak ketiga, seperti vendor cloud, penyedia sistem, atau support eksternal
- Maka, pengelolaan hubungan dengan mitra dan pemasok sangat penting, terutama dalam penanganan insiden

Untuk memperlancar komunikasi lintas vendor, bisa disepakati:

- Aturan pertukaran data
- Prosedur koordinasi & eskalasi
- Proses yang seragam agar semua vendor bicara "bahasa operasional" yang sama

Dengan kolaborasi yang aktif, pekerjaan dapat diselesaikan secara cepat dan efektif. Organisasi yang ingin menyelesaikan insiden dengan cepat sebaiknya:

- Menghapus hambatan birokrasi
- Fokus pada komunikasi terbuka & pengambilan keputusan cepat bersama mitra

**Contoh Kolaborasi yang efektif:**

- Layanan pembayaran digital menggunakan API dari vendor A:
- Saat insiden terjadi (gagal transaksi), vendor perlu ikut investigasi
- Organisasi punya prosedur: “jika error code X, hubungi vendor A dalam 10 menit”
- Tim internal + vendor bahas penyebab dan solusi lewat sistem kolaborasi

## ● Catatan Penting

Perlu diingat bahwa praktik (*practice*) merupakan sebuah panduan, bukan aturan baku. Jadi harus dicatat bahwa *practice guide* seperti ini bersifat saran, bukan keharusan. Artinya ketika menggunakan konten panduan praktik, organisasi harus selalu mengikuti 7 panduan prinsip-prinsip ITIL (*Guiding Principles*).