CERT pada Enterprise Menggunakan Framework COBIT 5

Iffah Kholidatun Nisrina (23215121)
Magister Teknik Elektro
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
iffahnisrina@gmail.com

ABSTRAK

COBIT 5 merupakan suatu framework yang menyediakan penjabaran bisnis secara end-to-end dari tata kelola teknologi informasi perusahaan untuk menggambarkan peran utama dari informasi dan teknologi dalam menciptakan nilai perusahaan. Hampir semua perusahaan telah mengimplementasikan teknologi informasi untuk meningkatkan efisiensi dan efektivitas kerja. Apabila perusahaan telah mengimplementasikan teknologi informasi, maka ada beberapa tata kelola yang harus ada pada perusahaan, salah satunya adalah pengelolaan insiden. Insiden sendiri adalah suatu peristiwa gangguan secara tidak terencana/sengaja, yang dapat menurunkan kualitas layanan tersebut kepada pelanggan serta tidak begitu berdampak secara signifikan atau masih dapat ditoleransi dan dapat diperbaiki atas gangguan tersebut. Akar permasalahan dari insiden sudah dapat diketahui sehingga dapat diperbaiki. Makalah ini membahas mengenai bagaimana cara menangani insiden pada sebuah enterprise dengan mengikuti framework COBIT 5. Nantinya akan dijelaskan bagaimana prosedur dalam menangani insiden mengacu pada framework COBIT 5 sehingga akan terlihat jelas aktivitas apa saja yang harus dilakukan oleh perusahaan untuk menangani insiden.

1. Pendahuluan

Keamanan informasi merupakan bagian penting yang tidak dapat diabaikan dalam perkembangan teknologi saat ini. Akibat perkembangan teknologi, pertukaran informasi semakin cepat untuk dilakukan. Saat ini, sangat mudah untuk mendapatkan informasi tidak dilihat dari daerah tempat tinggalnya. Komunikasi bukan menjadi masalah sehingga kemajuan dalam bidang lainnya seperti bisnis, ekonomi, sosial, dan lain sebagainya juga dapat dicapai. Namun seiring dengan perkembangan tersebut, tidak lupa terdapat ancaman-ancaman yang dapat terjadi. Ancaman tersebut berkaitan dengan teknologi informasi, dari

pencurian informasi sampai dengan memanfaatkan media internet untuk kejahatan. Berdasarkan [2] sebanyak 228.420.754 serangan yang terjadi pada kuarter pertama tahun 2016 diseluruh 195 negara di dunia. Selain itu juga terdapat 459.970 serangan yang berhubungan dengan pencurian uang dari akun bank secara online. Kemudahan mengakses informasi tentu saja memicu tantangan yang lebih besar. Hal tersebut memicu perusahaan-perusahaan untuk melindungi data penting yang dimilikinya. Hal tersebut sudah menjadi kewajiban bagi setiap perusahaan agar menjaga data-data penting miliknya untuk tidak jatuh ditangan yang salah. Tidak ada jaminan suatu perusahaan yang memiliki sistem keamanan yang tinggi tidak terkena oleh serangan. Serangan tersebut biasa disebut dengan insiden. Insiden sendiri adalah suatu peristiwa gangguan secara tidak terencana/sengaja, yang dapat menurunkan kualitas layanan tersebut kepada pelanggan serta tidak begitu berdampak secara signifikan atau masih dapat ditoleransi dan dapat diperbaiki atas gangguan tersebut. [7]

Pada paper ini akan difokuskan analisisnya pada enterprise yang terdapat di Indonesia. Di Indonesia sendiri sudah banyak bermunculan CERT yang dipelopori oleh ID-CERT pada tahun 1998. [1] Pada tahun 2016 sudah banyak CERT lain yang muncul, ada yang berdiri secara voluntir dan ada juga CERT pada suatu perusahaan. Perusahaan di Indonesia banyak yang sudah menerapkan sistem tersebut namun masih terdapat banyak masalah dalam keberjalanannya karena masih baru saja dibuat. Banyak perusahaan yang masih belajar bagaimana prosedur untuk menangani insiden yang baik. Namun ada juga yang sudah berjalan dan mengalami kendala-kendala seperti kurangnya SDM, peran yang kurang jelas dari personil, regulasi yang belum jelas, dan lain sebagainya. [8]

2. *Computer Emergency Respond Team* (CERT)

2.1 Pengertian CERT

CERT merupakan kepanjangan dari *Computer Emergency Response Team* memiliki nama lain yaitu diantaranya *Incident response Team* (IRT), *Incident response Team* (IRC), *Incident Handling Team* (IHT), *Incident Managing/Management Team* (IMT), *Computer Security Incident response Team* (CSIRT), *Computer Incident response Team* (CIRT), *Computer Incident response Capability or Center* (CIRC), *Security Incident response Team* (SIRT), dan *Security Emergency Response Team* (SERT). [11] CERT sendiri memiliki pengertian sebuah

tim yang berhubungan dengan spesialisasi keamanan informasi sehingga mempersiapkan dan melakukan respon pada insiden keamanan informasi. Tim tersebut bertanggung jawab untuk menerima, melakukan review, mengkoordinasikan, dan melakukan respon pada aktivitas dan insiden keamanan komputer. [3]

Tujuan utama dari CERT adalah untuk mengentikan aksi dari insiden dan sistem yang terkena serangan dapat kembali beroperasi dengan normal. Serangan bisa saja terjadi walaupun telah memiliki infrastruktur keamanan yang canggih, keamanan tersebut tidak dapat memberikan jaminan apakah sistem bisa ditembus oleh serangan atau tidak. Serangan yang terjadi sering dimotivasi oleh hal finansial. Pihak yang diserang juga akan mengalami kerugian secara finansial yang tentunya tidak sedikit. Untuk mengurangi hal-hal tersebut maka perlu dilakukan pencegahan dan pengurangan dampak saat terjadinya insiden sehingga dapat mengurangi biaya untuk pemulihan. CERT sendiri memiliki konsep *prepare, detect*, dan *response*. *Prepare* sendiri merupakan hal yang penting dalam kegiatan insident response ini, hal yang dilakukan adalah mengumpulkan informasi, merancang prosedur penanganan insiden, perancangan deteksi, dan lain sebagainya. *Detect* merupakan hal penting juga karena perlu dilakukan pengawasan yang baik agar sistem tidak terjadi insiden. *Response* juga bagian yang tidak kalah penting karena konsep inilah yang bertugas untuk mengembalikan layanan seperti semula. [9]

2.2 CERT pada Enterprise di Indonesia

CERT di Indonesia tergolong cukup banyak. Ada dua macam CERT yang ada, yaitu CERT yang berdiri sendiri secara independen dan juga CERT yang berasal dari suatu perusahaan atau lembaga. Di Indonesia, CERT yang ada antara lain ID-CERT, ID-SIRTII, BPPT CSIRT, Telkom CSOC, XL-CSIRT, Jatim CSIRT, Jabar ACAD CSIRT, dan lain sebagainya. [8] CERT tersebut ada yang tergolong baru dan juga ada yang sudah beroperasi dari lama. CERT yang terdapat pada perusahaan relatif baru dibandingkan dengan yang dimiliki oleh lembaga pemerintahan.

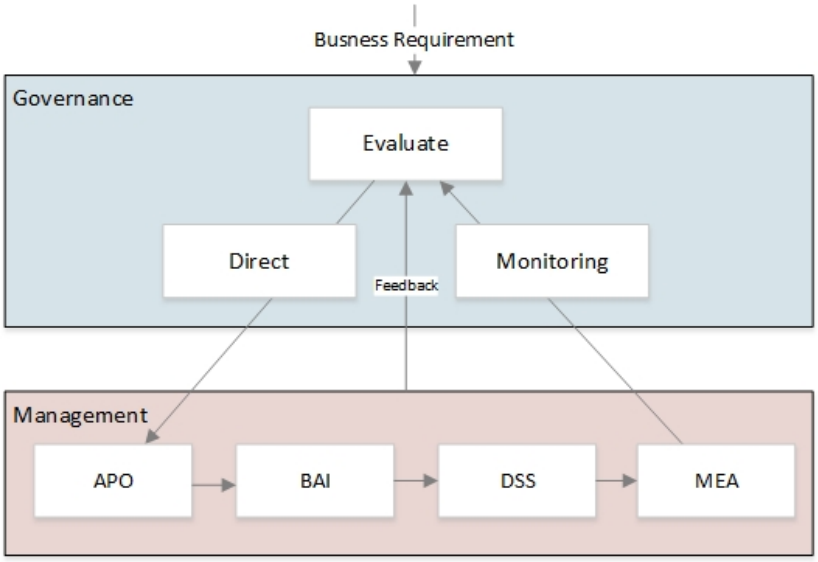
Di indonesia sendiri, penerapan tata kelola perusahaan masih jarang yang memenuhi standar. Manajemen insiden merupakan salah satu bagian dari tata kelola tersebut. Standar yang digunakan disini adalah peraturan BUMN nomor PER-02/MBU/2013 [10] yang menyatakan bahwa target *maturity level* tata kelola perusahaan yang direkomendasikan

kementrian BUMN dan mengacu pada *best practice* standar di industri dunia adalah level 3. Namun dalam perjalanannya karena CERT di perusahaan masih baru didirikan maka belum bisa mencapai level yang diinginkan. Untuk itu pada paper ini akan dibahas mengenai prosedur insident response, pihak-pihak yang terlibat, dan juga bagaimana tahapan untuk mencapai level 3 dari *best practice* yang digunakan, dalam kali ini standar yang digunakan adalah *framework* COBIT 5.

3. COBIT 5 [4]

Framework COBIT 5 adalah *framework* yang digunakan untuk menyusun tata kelola dan manajemen TI perusahaan. COBIT 5 merupakan perluasan dari COBIT 4.1 dan mengintegrasikan beberapa *framework* utama, standar, dan sumber-sumber lain, termasuk Val TI, Risk TI, ITIL, dan ISO. COBIT 5 memberikan *framework* yang mencakup lima domain, yaitu:

1) *Evaluate, Direct, and Monitor* (EDM);
2) *Align, Plan, and Organize*(APO);
3) *Build, Acquire, and Implement* (BAI);
4) *Deliver, Service, and Support* (DSS); dan
5) *Monitor, Evaluate, and Assess* (MEA).



Gambar 1 Area COBIT [5]

Kelima domain tersebut dikelompokkan ke dalam dua area, yaitu Area Tata Kelola (domain EDM) dan Area Manajemen (domain APO, BAI, DSS, dan MEA). Domain EDM merupakan area tata kelola pada COBIT 5, yang memiliki fungsi mengevaluasi, mengarahkan dan memonitor kegiatan manajemen TI secara keseluruhan yang dilakukan oleh perusahaan. Terdapat lima proses pada domain EDM yaitu EDM01 *Ensure Governance Framework Setting and Maintenanc,* EDM02 *Ensure Benefit Delivery,* EDM03 *Ensure Risk Optimisation,* EDM04 *Ensure Resource Optimisation,* dan EDM05 *Ensure Stakeholder Transparency.*

Pada domain kedua yaitu domain APO memiliki fungsi sebagai penyelarasan dan pengelolaan perencanaan TI yang dilakukan untuk diimplementasikan dan dikembangkan oleh perusahaan. Terdapat tiga belas proses dalam domain ini, yaitu APO01 *Manage the TI Management Framework,* APO02 *Manage Strategy,* APO03 *Manage Enterprise Architecture,* APO04 *Manage Inovation,* APO05 *Manage Portfolio,* APO06 *Manage Budget and Cost,* APO07 *Manage Human Resurce,* APO08 *Manage Relationship,* APO09 *Manage Service Agreements,* APO10 *Manage Supplier,* APO11 *Manage Quality,* APO12 *Manage Risk,* dan APO13 *Manage Security.*

Domain ketiga merupakan area manajemen pada COBIT 5 yaitu BAI yang memiliki fungsi sebagai pembangunan dan implementasi TI berdasarkan hasil yang didapatkan dari kebutuhan pengguna dan telah direncanakan oleh perusahaan. Domain BAI memiliki 10 proses, yaitu BAI01 *Manage Programmes and Projects,* BAI02 *Manage Requirements Definition,* BAI03 *Manage Solutions Identification and Build,* BAI04 Ma*nage Availability and Capacity,* BAI05 *Manage Organisational Change Enablement,* BAI06 *Manage Changes,* BAI07 *Manage Change Acceptance and Transitioning,* BAI08 *Manage Knowledge,* BAI09 *Manage Assets,* dan BAI10 *Manage Configuration*.

Domain keempat merupakan DSS yang memiliki fungsi menjalankan dan memelihara hasil implementasi program TI agar dapat digunakan secara terus menerus dan aman, serta memberikan dukungan kepada pengguna yang membutuhkan dan mendapatkan masalah ketika menggunakan fasilitas TI perusahaan. Proses pada domain ini antara lain DSS01 *Manage Operations,* DSS02 *Manage Service Request and Incident,* DSS03 *Manage Problem,* DSS04 *Manage Continuity,* DSS05 *Manage Security Services,* dan DSS06 *Manage Business Process Controls.*

Domain terakhir merupakan salah satu domain di area manajemen yaitu MEA. MEA berfungsi untuk monitor, evaluasi dan *assesment* terhadap performa dan kesesuaian dari sistem TI yang berjalan, kegiatan pengontrolan sistem TI yang dilakukan oleh perusahaan, dan kesesuainnya dengan kebutuhan dan peraturan eksternal perusahaan. Proses pada domain ini ada 3, antara lain MEA01 *Monitor, Evaluate, and Assess Performance and Conformance,* MEA02 *Monitor, Evaluate, and Assess the System of Internal Control,* dan MEA03 *Monitor, Evaluate, and Assess Compliance with External*.

Pada proses-proses diatas, COBIT juga menjelaskan sumber daya manusia yang perlu ikut terlibat dalam masing-masing prosesnya. COBIT menyajikan standar tersebut melalui diagram RACI. Diagram RACI sendiri merupakan kependekan dari *Responsible, Accountable, Consulted, and Informed*. Hal ini menjelaskan peran apa yang dilakukan oleh suatu jabatan tertentu. Berikut adalah penjelasannya :

- *Responsible (R)*

  R merupakan penjelasan bagi suatu proses tertentu dan suatu jabatan tertentu, maka orang tersebut yang bertangungg jawab untuk melakukan kegiatan tersebut.
- *Accountable (A)*

  A menjelaskan bahwa orang tersebut yang memberikan tugas kepada orang yang bertanggung jawab diatas, sekaligus sebagai penyetuju akhir dari kegiatan yang akan dilakukan. Sehingga A disini juga sering disebut dengan *Approver* atau *final approving authority*.
- *Consulted (C)*

  C menjelaskan bahwa orang yang bersangkutan dibutuhkan saran dan umpan baliknya untuk melakukan kegiatan tersebut. Hal ini menjadikan untuk mengimplementasikan kegiatan tersebut dibutuhkan komunikasi dua arah.
- *Informed (I)*

  Orang yang bersangkutan merupakan orang yang perlu mengetahui kemajuan dan hasil dari implementasi kegiatan tersebut, komunikasi yang dilakukan merupakan komunikasi satu arah yaitu pelaporan oleh orang yang melakukan kegiatan tersebut.

Pada COBIT terdapat level untuk menentukan *maurity level* dari proses yang telah diimplementasikan. Pada COBIT sendiri, kita dapat melakukan penilaian sendiri terhadap suatu proses yang telah diimplementasikan dalam suatu perusahaan dengan cara

melakukan *mapping* pada proses-proses COBIT. Ketentuan untuk menentukan maturity level antara lain ada dua yaitu *rating level* dan *capability level*. *Rating level* merupakan pendefinisian seberapa jauh proses tersebut telah dilakukan dan dinyatakan dalam persen. *Capability level* sendiri merupakan penentuan *maturity level* sesuai dengan perhitungan pencapaian yang telah dinilai tiap prosesnya. [6]

Tabel 1 Rating Level COBIT 5 [6]

N	Not achieved	0-15% achievement
P	Partially achieved	>15-50% achievement
L	Largely achieved	>50-85% achievement
F	Fully achieved	>85-100% achievement

Tabel 2 Capability Level COBIT 5 [6]

	Level 1	Level 2	Level 3	Level 4	Level 5
Process Performance	L/F	F	F	F	F
Performance Management	-	L/F	F	F	F
Work Product Management	-	L/F	F	F	F
Process Definition	-	-	L/F	F	F
Process Deployment	-	-	L/F	F	F
Process Measurement	-	-	-	L/F	F
Process Control	-	-	-	L/F	F
Process Innovation	-	-	-	-	L/F
Process Optimization	-	-	-	-	L/F

4. Prosedur *Incident response* pada CERT di Indonesia

Pada paper kali ini, akan dibahas mengenai prosedur *incident response* mengacu pada standar COBIT 5. Seperti sudah dijelaskan sebelumnya COBIT memiliki banyak ketentuan untuk suatu perusahaan yang menjalankan teknologi informasi. Untuk perusahaan yang menjalankan teknologi informasi, tentu saja tidak lepas dari ancaman pada teknologinya. Bisa berupa serangan malware, bugs pada program, penipuan menggunakan teknologi informasi, dan lain sebagainya. Untuk itu perlu dibuat CERT pada suatu perusahaan sehingga dapat mengatasi hal-hal yang tidak diinginkan berkaitan dengan teknologi informasi. CERT sendiri sangat penting bagi suatu perusahaan untuk mencegah dan mengatasi ancaman dan serangan yang terjadi.

Untuk melakukan hal tersebut, maka perusahaan perlu membuat suatu prosedur kerja yang berhubungan dengan hal tersebut. Pada standar COBIT 5 telah dijelaskan standar apa saja yang harus ada untuk mengatasi risiko tersebut. Untuk itu akan dibuat sebuah prosedur yang menangani hal tersebut. Pada COBIT 5 sendiri mengenai standar untuk melakukan *incident response* sendiri ada pada domain DSS (Deliver, Service, and Support) yang ada pada area manajemen. Domain DSS sendiri memberikan penjelasan mengenai prosedur operasional yang harus dilakukan oleh sebuah perusahaan yang menggunakan TI sebagai pendukungnya. *Incident response* sendiri ada pada proses kedua dari DSS (DSS02) yang bernama *Manage Service Requests and Incidents*. Disini insiden disatukan dengan service requets karena apabila ada permintaan layanan dari pelanggan maka hal tersebut dapat merubah keadaan yang ada sekarang sehingga perlu dilakukan perubahan terhadap layanan yang ada sekarang. Karena hal tersebut maka prosedur untuk memenuhi permintaan pelanggan dan mengatasi insiden sama.

Pada DSS02 ini menjelaskan bahwa proses tersebut untuk memberikan respon pada permintaan pengguna dan resolusi dari semua tipe insiden. Yang akan dilakukan adalah mengembalikan layanan kembali seperti semula, mencatat dan memenuhi request dari pengguna, dan merekam, menginvestigasi, mendiagosa, mengekskalasi, dan mencari jalan keluar dari suatu insiden yang terjadi. Hal tersebut dilakukan dengan waktu yang cepat dan juga efektif. Sangat penting untuk menyelesaikan insiden tepat pada waktunya karena akan berpengaruh pada operasional perusahaan yang bisa berimbas pada kerugian secara finansial. Tujuan dari proses ini adalah untuk meningkatkan produktivitas perusahaan dengan cara mengurangi dampak risiko dari insiden dan juga mengurangi gangguan yang dapat terjadi melalui pengambilan keputusan yang cepat dari pertanyaan pelanggan dan juga insiden.

Proses ini juga mendukung tujuan perusahaan yang berkaitan dengan TI yang telah diinvestasikan. Tujuan tersebut adalah mengelola risiko bisnis yang berhubungan dengan TI dan juga menyelaraskan layanan TI yang diberikan sesuai dengan kebutuhan bisnis perusahan. Hal yang berhubungan dengan risiko bisnis antara lain adalah persentase proses bisnis kritis, layanan TI, dan program bisnis yang menggunakan TI yang telah didefinisikan pada *risk assessment*, jumlah insiden yang berhubungan dengan TI yang tidak didefinisikan di *risk assessment*, persentase *risk assessment* perusahaan yang berhubungan dengan TI,

dan frekuensi untuk memperbarui *risk profile*. Kemudian hal-hal yang berhubungan dengan penyelarasan layanan TI dengan tujuan perusahaan antara lain adalah jumlah gangguan bisnis yang terjadi akibat insiden TI, persentase kepuasan stakeholder terhadap layanan IT yang telah memenuhi standar level layanan yang telah disepakati, dan persentasi pelanggan yang puas dengan kualitas dari layanan TI.

Tujuan dari proses ini antara lain untuk layanan yang berhubungan dengan TI dapat digunakan, insiden dapat diselesaikan berdasarkan level layanan yang telah disepakati, dan request layanan disesuaikan dengan kemampuan level layanan perusahaan dan dapat memuaskan pelanggan. Hal yang berhubungan dengan layanan TI yang bisa digunakan adalah jumlah dan persentase insiden yang menyebabkan gangguan pada proses bisnis kritis dan waktu rata-rata antar insiden sesuai dengan layanan yang menggunakan TI. Hal-hal yang perlu diperhatikan untuk mencapai penyelesaian kasus insiden antara lain persentasi insiden yang telah diselesaikan pada suatu rentang waktu yang telah disepakati. Kemudian untuk pemenuhan permintaan layanan, hal-hal yang perlu dijadikan parameter adalah level kepuasan pelanggan terhadap pemenuhan permintaan layanan dan waktu rata-rata yang diperlukan untuk menangani masing-masing request layanan.

4.1 Prosedur *Incident response* menurut COBIT

Pada proses DSS02 terdapat 7 standar proses praktis yang masing-masing memiliki contoh aktivitas yang bisa dilakukan. Proses praktis yang dijelaskan antara lain :

1. *Define incident and service request classification schemes*
2. *Record, classify and prioritise request and incidents*
3. *Verify, approve and fulfill service request*
4. *Investigate, diagnose and allocate incidents*
5. *Resolve and recover from incidents*
6. *Close service request and incidents*
7. *Track status dan produce reports*

Pada proses pertama yaitu *define incident and service request classification schemes* yang berarti mendefinisikan skema klasifikasi insiden dan request layanan. Hal ini menjelaskan bahwa insiden dan request yang masuk sebaiknya diklasifikasikan dan skema dan model klasifikasi harus didefinisikan terlebih dahulu sehingga apabila terjadi hal

tersebut bisa langsung diklasifikasikan. Untuk pembuatan skema dan model klasifikasi diperlukan beberapa input data. Input daya yang diperlukan antara lain *service level agreement* (SLA), repositori konfigurasi, repositori terbaru dengan *configuration items*, laporan status konfigurasi, peraturan pemantauan aset dan kondisi even, skema klasifikasi masalah, dan aksi dan komunikasi *incident response*.

Dari proses ini maka akan dilakukan aktivitas-aktivitas untuk mencapai tujuannya, antara lain mendefinisikan skema dan kriteria klasifikasi dan prioritas insiden dan request layanan untuk registrasi masalah. Hal tersebut dilakukan untuk memastikan bahwa insiden yang masuk dapat ditangani secara konsisten sesuai dengan klasifikasinya dan juga dapat menginformasikan pengguna mengenai analisis yang akan dilakukan. Kemudian kegiatan yang kedua adalah mendefinisikan model insiden untuk standar yang digunakan untuk pemecahan masalah yang efektif dan efisien. Kemudian kegiatan ketiga adalah mendefinisikan model permintaan layanan sesuai dengan tipe permintaan layanan untuk membangun kemandirian pada user dan layanan yang efisien untuk standar permintaan. Kegiatan ketiga adalah mendefinisikan peraturan dan prosedur ekskalasi insiden terutama untuk insiden major dan insiden keamanan. Kegiatan yang terakhir yang bisa dilakukan untuk mencapai proses tersebut adalah mendefinisikan sumber pengetahuan insiden dan layanan dan juga contoh penggunaannya sehingga saat insiden tersebut terjadi dapat dipelajari lebih lanjut.

Dari aktivias-aktivitas yang bisa dilakukan pada proses pertama ini, output yang dihasilkan ada tida, yaitu model dan skema klasifikasi insiden dan request layanan, peraturan untuk ekskalasi insiden, dan juga kriteria untuk registrasi masalah. Output tersebut yang nantinya menjadi dasar apabila terjadi insiden dan juga request layanan dari pelanggan. Untuk model dan skema klasifikasi insiden dan request layanan dan peraturan ekskalasi insiden akan digunakan dalam proses ini, namun untuk kriteria untuk registrasi masalah akan berhubungan dengan proses lain yaitu manajemen masalah.

Setelah itu terdapat proses kedua yaitu *record, classify and prioritise request and incidents* yang berarti merekam, mengklasifikasikan, dan memprioritaskan request dan insiden. Proses ini bermaksud untuk melakukan indentifikasi, rekam, dan klasifikasi pada request layanan dari pelanggan dan insiden. Setelah melakukan klasifikasi, maka insiden dan request layanan akan diprioritaskan sesuai dengan bisnis yang kritis dan perjanjian layanan. Untuk melakukan proses ini, diperlukan beberapa input yaitu SLA, prosedur ekskalasi

darurat, ketetapan insiden dan peraturan pengawasan aset dan kondisi even, dan ketetapan insiden keamanan.

Aktivitas yang bisa dilakukan pada proses ini antara lain mencatat semua request layanan dan insiden beserta informasi yang relevan sehingga dapat diselesaikan dengan efektif dan dapat menjaga rekaman *history* secara efisien. Kemudian untuk menentukan tren untuk menganalisis insiden, maka insiden dan request layanan perlu diklasifikasikan berdasarkan tipe dan kategorinya sehingga terlihat insiden dan request layanan apa yang sedang banyak terjadi dan bisa dilakukan penanganan yang lebih efektif bahkan pencegahannya. Selain itu, aktivitas yang bisa dilakukan adalah memprioritaskan insiden dan request layanan sesuai dengan definisi layanan pada *service level agreement* (SLA) yang dapat berpengaruh pada dampak dan urgensi bisnisnya. Dari aktivitas yang dilakukan tersebut maka output yang dihasilkan antara lain adalah log request layanan dan insiden dan insiden dan request layanan yang telah terklasifikasi dan terprioritisasi.

Proses selanjutnya pada DSS02 ini adalah *verify, approve and fulfill service request* yang berarti memastikan, menyetujui dan memenuhi request layanan. Pada proses ini akan dilakukan pemilihan prosedur yang tepat untuk memeuhi request layanan dan memastikan bahwa request layanan tersebut terpenuh sesuai dengan definisi pada kriteria request. Apabila sudah dipilih maka apabila diperlukan meminta persetujuan dan menyelesaikan pemenuhan request layanan. Input yang dibutuhkan untuk menjalankan prosedur ini adalah penyebab awal masalah yang berkaitan dengan risiko.

Aktivitas yang bisa dilakukan pada proses ini adalah memastikan penggunaan hak request layanan jika diperlukan maka dibuat perubahan alur proses dan standar. Kemudian aktivitas yang kedua adalah mendapatkan persetujuan secara finansial dan fungsional untuk menyetujui perubahan standar yang akan dilakukan untuk pemenuhan request layanan. Kemudian aktivitas yang terakhir adalah memenuhi request layanan dengan cara melakukan prosedur request yang telah dipilih. Dari aktivitas tersebut maka output yang diharapkan adalah request layanan yang telah disetujui dan request layanan yang telah terpenuhi.

Proses selanjutnya adalah *investigate, diagnose and allocate incidents* yang artinya memeriksa, mendiagnosa, dan mengalokasikan insiden. Proses ini adalah melakukan indentifikasi pada gejala insiden kemudian melakukan pencatatan terhadap gejala tersebut. Setelah melakukan identifikasi dan pencatatan maka menentukan penyebab yang mungkin dari terjadi insiden tersebut dan kemudian menentukan solusi yang mungkin untuk

dilakukan. Input yang dibutuhkan untuk melakukan proses ini adalah rencana dukungan suplemen.

Aktivitas yang bisa dilakukan untuk mencapai proses ini yang pertama adalah mengidentifikasi dan mendeskripsikan gejala insiden yang relevan untuk menentukan penyebab yang mungkin dari insiden tersebut. Untuk melakukan hal ini perlu melihat pada *knowledge* yang ada seperti masalah yang telah terjadi dan error yang telah diketahui. Hal tersebut digunakan untuk mengidentifikasi solusi insiden yang mungkin. Apabila masalah yang terjadi tidak ada di database *known error* maka disarankan meregistrasi masalah baru yang prosedurnya mengacu pada manajemen problem. Kemudian aktivitas yang terakhir adalah membuat prosedur khusus untuk menyelesaikan insiden tersebut disertai dengan kebutuhan-kebutuhan khusus lainnya seperti kebutuhan tenaga ahli tertentu atau personel level management tertentu. Pada proses ini, output yang dihasilkan antara lain adalah gejala-gejala insiden dan log masalah.

Proses selanjutnya adalah *resolve and recover from incidents* yang artinya menyelesaikan dan memulihkan kembali insiden. Maksud dari proses ini adalah mendokumentasikan, menjalankan, dan melakukan pengujian pada solusi yang telah teridentifikasi. Melakukan aksi pemulihan kembali untuk mengembalika layanan TI yang terganggu seperti semula. Input yang dibutuhkan untuk melakukan proses ini adalah rancangan respon insiden yang berhubungan dengan risiko, data *known error*, dan juga ilmu yang telah dipelajari berkaitan dengan insiden yang sedang berlangsung.

Aktivitas yang bisa dilakukan pada proses ini antara lain memilih dan mengimplementasikan solusi insiden yang paling sesuai. Kemudian mencatat apakah diperlukan observasi atau coba-coba untuk menyelesaikan insiden tersebut. Kemudian melakukan aksi pemulihan layanan bila diperlukan. Dan yang terakhir mendokumentasikan solusi insiden dan melakukan penilaian apakah solusi yang baru saja dilakukan bisa digunakan sebagai acuan apabila insiden serupa terjadi di masa depan. Output yang dihasilkan dari proses ini adalah solusi insiden yang telah terdokumentasi.

Proses selanjutnya merupakan proses ke enam dari DSS02 ini yaitu *close service request and incidents* yang artinya melakukan penutupan pada request layanan dan insiden. Yang dimaksud pada proses ini adalah memastikan bahwa penyelesaian insiden dan pemenuhan request layanan telah selesai dan sudah mencapai level kepuasan yang

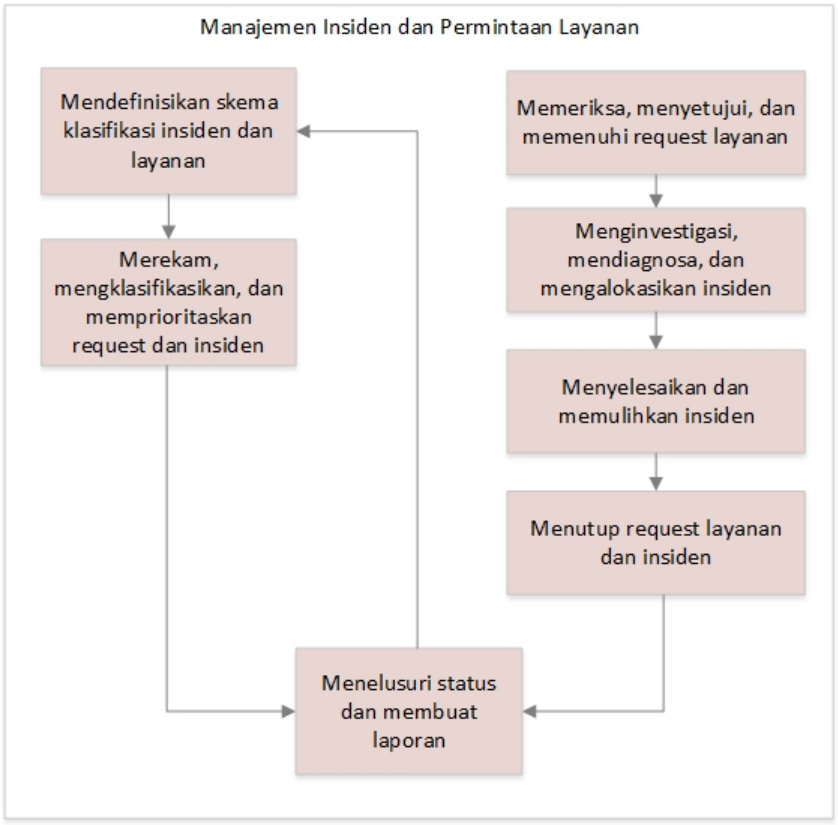
diinginkan. Kemudian melakukan penutupan pada prosedur yang baru saja dilakukan. Input yang dibutuhkan untuk melakukan ini adalah rekaman masalah yang telah ditutup.

Aktivitas yang dilakukan yaitu memastikan pelanggan yang bersangkutan telah puas dengan pemenuhan request layanan yang diminta dan juga insiden yang terjadi telah diselesaikan dengan baik. Hal ini perlu dilakukan yaitu meminta umpan balik dari pelanggan untuk mengetahui apakah request yang diminta telah selesai. Selain itu juga perlu memastikan apakah insiden yang terjadi sudah terselesaikan dengan baik dan layanan sudah kembali seperti semula sehingga setelah itu baru bisa melakukan penutupan. Penutupan request layanan dan insiden perlu dilakukan untuk menyatakan bahwa requets layanan dan insiden yang terjadi sudah terselesaikan. Output dari proses ini adalah request layanan dan insiden yang telah tertutup dan konfirmasi dari user mengenai kepuasan dari solusi yang dilakukan.

Yang terakhir dari DSS02 ini adalah *track status and produce report* yang artinya mengikuti status dan membuat laporan. Yang dimaksud dari proses ini adalah secara berkala tetap mengikuti perkembangan dari insiden dan request layanan yang kemudian akan di analisis dan dibuatkan laporan mengenai tren yang sedang terjadi. Hal ini bisa digunakan perusahaan untuk perkembangan secara kontinyu mengenai request layanan dan juga insiden. Input yang dibutuhkan pada proses ini antara lain *Operational Level Agreement* (OLA), laporan status masalah, laporan solusi masalah, dan laporan pengawasan solusi masalah.

Aktivitas yang bisa dilakukan antara lain adalah mengawasi dan mengikuti ekskalasi dan resolusi prosedur penanganan insiden yang sedang dilakukan. Kemudian mengidentifikasi informasi yang dibutuhkan untuk pelaporan kepada stakeholder berupa frekuensi kejadian dan mediumnya. Aktivitas selanjutnya adalah menganalisa insiden dan reqeust layanan berdasarkan kategori dan tipenya untuk menentukan tren. Informasi tersebut yang kedepannya akan digunakan untuk rencana pengembangan secara kontinyu. Aktivitas yang terakhir adalah membuat dan mempublikasikan laporan secara berkala. Output dari proses ini adalah laporan tren dan status insiden dan laporan tren dan status request layanan.

Dari penjelasan prosedur diatas maka berikut adalah ringkasannya.



Gambar 2 Prosedur *Incident response* COBIT 5

4.2 Peran Sumber Daya Manusia pada *Incident response* Mengacu pada COBIT 5

Untuk menjalankan prosedur yang telah dibuat diatas, maka perlu mendefinisikan sumber daya manusia yang menjalankannya. Sumber daya manusia yang akan didefinisikan disini adalah secara umum tidak spesifik pada suatu perusahaan tertentu. Berikut adalah definisi jabatan pada suatu perusahaan dan perannya pada prosedur *incident response* yang dituliskan pada Tabel 3.

1. Jajaran direksi merupakan jajaran yang paling bertanggung jawab terhadap keseluruhan perusahaan dan memiliki kontrol pada bidangnya masing-masing
2. Eksekutif bisnis merupakan pejabat struktural yang bertanggung jawab di unit kerja yang berkaitan langsung dengan bisnis perusahaan
3. Pemilik proses bisnis merupakan seluruh unit kerja perusahaan yang dalam pelaksanaan proses bisnisnya didukung oleh fasilitas TI perusahaan.
4. Satuan Pengawas Internal (SPI) merupakan divisi yang bertanggung jawab untuk melakukan audit internal pengelolaan dan pelaksanaan TI oleh bagian sistem informasi terhadap ketetapan yang telah disepakati.

Tabel 3 Pihak yang Terlibat pada Prosedur *Incident response*

Pihak Terkait	**Pengelolaan Permintaan Layanan dan Insiden**						
	Mendefinisikan skema klasifikasi insiden dan permintaan layanan	Melakukan record, klasifikasi dan prioritisasi permintaan dan insiden	Melakukan verifikasi, penyetujuan dan pemenuhan permintaan layanan	Melakukan investigasi, diagnosis dan alokasi insiden yang terjadi	Mengatasi dan pulih dari insiden	Menutup permintaan layanan dan insiden	Melakukan *track* terhadap status beserta pelaporannya
Direktur Utama							
Direktur Keuangan dan Administrasi							
Direktur Pemasaran							
Direktur Teknologi dan Produksi							
Eksekutif Bisnis							
Pemilik Proses Bisnis	C	I	R	R	I	I	I
Divisi SPI	I	I		C/I	I	I	I
Divisi MSO							
Divisi Logistik							
Divisi Keuangan dan Akuntansi							
Divisi HCGA							
Sekper							
CIO	A	I	I	I	I	I	I
Manajer Sisfo	C	A	A	A	A	A	A
Bidang Value Manajemen dan Compliance Sistem TI			C	C/I	C/I	C/I	C/I
Bidang Pengembangan, Perencanaan, dan Implementasi Sistem TI	R	R	C	R	R	C	C
Bidang Operasi dan Layanan Sistem TI	R	R	R	R	R	R	R

5. Manajemen, Strategi, dan Operasi (MSO) merupakan divisi yang bertanggung jawab dalam membuat rencana, strategi, dan pengelolaan standar pada taraf korporat.
6. Logistik merupakan divisi yang bertanggung jawab dalam hal logistik yang berkaitan dengan pengadaan barang dan jasa.
7. Keuangan dan akuntansi merupakan divisi yang bertanggung jawab mengenai finansial perusahaan.
8. Human Capital and General Affair (HCGA) merupakan divisi yang bertanggung jawab dalam kegiatan yang berkaitan dengan sumber daya manusia.
9. Sekretaris perusahaan merupakan divisi yang bertanggung jawab terhadap penerapan tata kelola pada perusahaan.
10. CIO merupakan orang yang bertanggung jawab untuk menyelaraskan TI perusahaan dengan strategi bisnis perusahaan.
11. Manajer sistem informasi (Sisfo) merupakan orang yang mengepalai bagian sistem informasi.
12. Value manajemen dan Compliance Sistem TI merupakan bidang pada sistem informasi yang bertanggung jawab untuk memastikan sistem TI berjalan sesuai dengan pihak internal, eksternal, dan ekspektasi yang diinginkan.
13. Pengembangan, perencanaan, dan implementasi sistem TI merupakan bidang dalam sistem informasi yang bertanggung jawab terhadap pengembangan, perencanaan, dan implementasi teknologi informasi yang dijalankan oleh perusahaan.
14. Operasi dan layanan sistem TI merupakan bidang di dalam bagian sistem informasi yang bertanggung jawab terhadap berjalannya sistem teknologi informasi pada perusahaan.

4.3 Tahapan Pencapaian *Maturity Level*

Untuk mencapai *maturity level* 3 mengacu pada *best practice* dunia yaitu COBIT 5, maka diperlukan langkah-langkah praktis untuk mencapai target tersebut. Tahapan yang dilakukan akan dibagi menjadi dua, yaitu tahap 1 dan tahap 2. Berikut adalah penjelasannya :

- Tahap 1

Pada tahap 1 ini target akhir yang akan dicapai adalah mencapai level 2 *maturity* pada COBIT 5. Untuk mencapai level 2 maka diharuskan mencapai level 1 terlebih dahulu dengan cara melakukan semua prosedur yang telah dibuat. Tidak harus satu proses satu kegiatan namun bisa saja kegiatan yang dilakukan bersamaan namun tujuan dari proses yang telah

didefinisikan oleh COBIT 5 telah tercapai. Kemudian setelah mengimplementasikan proses yang telah dibuat maka akan dicapai level 2. Untuk mencapai level 2 *performance management* harus dilakukan setidaknya mencapai 50%. Untuk mencapai level *performance* 50% maka yang harus dilakukan adalah pengelolaan tujuan dari masing-masing proses, proses direncanakan dan diawasi, kemudian proses tersebut dikembangkan untuk mencapai rencana, tanggung jawab dan otoritas proses, sumber daya dan informasi yang dibutuhkan diidentifikasikan, dan kerja sama dengan pihak lain dikelola dengan baik. Hal-hal tersebut sebaiknya dilakukan sehingga mencapai 50% dari yang ingin dicapai.

Selain *performance management*, pada level 2 juga diharapkan mencapai 50% pada *work product management*. Setiap proses yang telah dibuat menghasilkan keluaran berupa dokumen atau jenis output lainnya. Keluaran tersebut dinamakan *work product*. Hal-hal yang harus dilakukan untuk mencapai hal tersebut adalah kebutuhan untuk *work product* setiap proses didefinisikan, kebutuhan akan dokumentasi dan kontrol untuk *work product* didefinisikan, *work product* yang dihasilkan diidentifikasi, didokumentasikan, dan dikontrol, dan melakukan review terhadap work product dan dikembangkan untuk mencapai tujuan. Hal-hal tersebut diimplementasikan setidaknya 50% untuk mencapai level 2. Sehingga pada akhir tahap ini setidaknya *process performance* mencapai 85%, *performance management* mencapai 50%, dan *work product management* mencapai 50%.

- Tahap 2

Pada tahap 2 ini diharapkan mencapai level 3. Untuk mencapai level 3 karena sebelumnya telah mencapai level 2. Sehingga dari pencapaian di level 2 harus ditingkatkan. Untuk *performance management* dan *work product management* harus ditingkatkan implementasinya sampai dengan 85%. Selain peningkatan dari tahap 1, untuk mencapai level 3 maka perlu melakukan *process definition* dan *process deployment*. Keduanya perlu diimplementasikan paling tidak sampai dengan 50%.

Process definition bermaksud untuk menentukan standar atau ukuran pada proses yang diimplementasikan. Untuk mencapai hal tersebut maka perlu membuat standar proses yang mendefinisikan elemen-elemen yang harus ada pada proses, menentukan interaksi antara satu proses dengan proses lain, menentukan kompetensi personil yang menjalankan proses tersebut, menentukan infrastruktur apa saja yang mendukung implementasi, dan menentukan metode yang sesuai untuk pengawasan efektivitas proses. Hal tersebut sebaiknya dijalankan paling tidak mencapai 50% dari keseluruhan.

Selanjutnya adalah *process deployment* dimana yang telah didefinisikan atau telah ditentukan pada *process definition* bisa diimplementasikan secara efektif untuk mencapai keluaran yang diharapkan. Hal-hal yang perlu dilakukan adalah mengeimplementasikan proses yang telah didefinisikan sebelumnya, peran, tanggung jawab, dan otoritas untuk menjalankan proses tersebut ditentukan dan dikomunikasikan, mempekerjakan personel dengan kompetensi tertentu untuk menjalankan proses tersebut, mengalokasikan dan menggunakan sumber daya dan informasi yang dibutuhkan, mengadakan, mengelola, dan menjaga infrastruktur dan lingkungan kerja yang dibutuhkan, dan melakukan evaluasi keberjalanan proses dengan cara mengumpulkan dan menganalisis data-data yang sesuai untuk pengembangan proses lebih lanjut. Apabila tahapan ini dilakukan, diakhir tahap 2 akan mencapai level 3 COBIT.

5. Kesimpulan

Kesimpulan dari paper ini adalah telah dibuat prosedur *incident response* yang mengacu pada standar best practice dunia COBIT 5 yang bisa diadopsi oleh CERT pada perusahaan di Indonesia. Prosedur yang dihasilkan terdapat pada Gambar 2. Selain itu telah didefinisikan pihak-pihak yang terlibat dalam proses *incident response* serta tugasnya yang telah diungkapkan melalui diagram RACI dan terdapat pada Tabel 3. Yang terakhir untuk mencapai level 3 COBIT 5 maka terdapat dua tahapan yang harus dilakukan perusahaan. Tahap 1 diharapkan mencapai level 2 dan pada tahap 2 diharapkan mencapai level 3. Dalam melakukan tahap 1, maka yang perlu dicapai oleh perusahaan adalah *process performance* mencapai 85%, *performance management* mencapai 50%, dan *work product management* mencapai 50%. Selanjutnya untuk tahap 2, perlu melakukan pengembangan dari tahap 1 yaitu diharapkan *performance management* dan *work product management* dapat 85% diimplementasikan. Selain itu, *process definition* dan *process deployment* juga diimplementasikan untuk mencapai level 3. *Process definition* dan *process deployment* ditargetkan untuk dicapai sebesar 50% dari implementasi secara keseluruhan. Maka diakhir tahap 2 perusahaan dapat mencapai *maturity level* 3 dari standar COBIT.

DAFTAR PUSTAKA

[1] Alkasimy, Ahmad. *Incident Handling ID-CERT.* Indonesia Computer Emergency Response Team, 2016.

[2] Gostev, Alexander, Roman Unuchek, Maria Garnaeva, Denis Makrushin, dan Anton Ivanov. *IT Threat Evolution in Q1 2016.* Kaspersky Lab HQ, 2016.

[3] Grobler, Marthie, dan Harri Bryk. *Common Challenges Faced During the Establishment of a CSIRT.* Information Security for South Africa, 2010.

[4] ISACA. *COBIT 5 : Enabling Process.* 2012.

[5] —. *COBIT 5: A Bussiness Framework for Governance and Management Enterprise.* 2012.

[6] —. *Self-assessment Guide: Using COBIT 5.* 2013.

[7] ISO. *ISO 27001 Information Security Management.* 2013.

[8] Julismail. *Diskusi CERT CSIRT Indonesia.* 2016. http://julismail.staff.telkomuniversity.ac.id/diskusi-cert-csirt-indonesia/.

[9] Keisuke, Kamata. *Organizational Internal Computer Security Incident Responding Structure : CSIRT.* JPCERT Coordination Center, 2008.

[10] *Peraturan Menteri Badan Usaha Milik Negara Nomor : PER-02/MBU/2013 tentang Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara.* 2013.

[11] West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, dkk. *Handbook for Computer Security Incident response Teams (CSIRTs).* Carnegie Mellon University, 2003.