Penerapan Framework ITIL v3 untuk Perbaikan Tata Kelola Manajemen Insiden Teknologi Informasi (Studi Kasus Bank XYZ)

Saleh Firdausi
18917223

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Sistem Informasi Enterprise
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2022

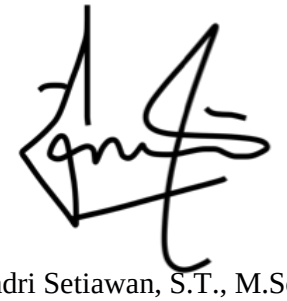
Lembar Pengesahan Pembimbing

Penerapan Framework ITIL v3 untuk Perbaikan Tata Kelola Manajemen Insiden Teknologi Informasi
(Studi Kasus Bank XYZ)

Saleh Firdausi
18917223

Yogyakarta, April 2022

Pembimbing



M. Andri Setiawan, S.T., M.Sc., Ph.D.

Lembar Pengesahan Penguji

Penerapan Framework ITIL v3 untuk Perbaikan Tata Kelola Manajemen Insiden Teknologi Informasi
(Studi Kasus Bank XYZ)

Saleh Firdausi
18917223

Yogyakarta, April 2022

Tim Penguji,

M. Andri Setiawan, S.T., M.Sc., Ph.D.
Ketua Penguji

Dr. R Teduh Dirgahayu
Penguji I

Dr. Ir. Elisa Kusrini, MT.
Penguji II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Penerapan Framework ITIL v3 untuk Perbaikan Tata Kelola Manajemen Insiden Teknologi Informasi (Studi Kasus : Bank XYZ)

Teknologi informasi (TI) merupakan salah satu investasi strategis bagi perbankan. Penggunaan TI oleh suatu bank dapat meningkatkan efisiensi dan efektivitas kegiatan operasional serta meningkatkan daya saing bank. Mengingat bahwa teknologi informasi merupakan suatu investasi yang mahal, sementara dalam penyelenggaraannya mengandung berbagai risiko, maka Bank perlu menerapkan tata kelola teknologi informasi (IT *Governance*). Bank dituntut untuk menerapkan berbagai standar untuk tata kelola teknologi informasi di berbagai aspek, salah satunya adalah aspek manajemen insiden TI. Layanan TI di Bank merupakan hal yang krusial karena diharuskan bekerja secara maksimal tanpa henti. Bank harus menjamin pengelolaan dan pencegahan setiap masalah yang muncul guna mendukung keberlangsungan proses bisnis perusahaan. Salah satu *framework* yang dapat digunakan untuk manajemen insiden layanan TI yang baik adalah *Information Technology Infrasturcture Library* version 3 (ITIL v3). Manajemen insiden ITIL bertujuan untuk memulihkan layanan TI yang terganggu kembali ke keadaan normalnya dan mengurangi dampak bisnis yang ditimbulkan. Untuk mengukur sejauh mana Bank sudah menyelenggarakan Tata Kelola Manajemen Insiden TI, dilakukan pengukuran tingkat kematangan dengan cara membandingkan keadaan saat ini (*as is*) dan keadaan yang diinginkan (*to be*) untuk memperoleh kesenjangannya (*gap*). Proses pengukuran tingkat kematangan dilakukan dengan metode wawancara dan kuesioner yang ditujukan kepada seluruh *stakeholder* yang terlibat dalam keseluruhan proses manajemen insiden TI. Hasil penelitian yang telah dilakukan menunjukkan 15 dari 42 atribut proses manajemen insiden TI yang belum mencapai keadaan yang diinginkan. Berdasarkan temuan kesenjangan tersebut, dirumuskan rekomendasi tata kelola manajemen insiden TI yang berdasarkan *framework* ITIL v3 yang diharapkan ketika sudah diterapkan dalam operasional Bank sehari-hari akan meningkatkan ketersediaan layanan, khususnya pada layanan TI Bank.

Kata kunci

IT *governance*, Manajemen Insiden, Pengukuran Tingkat Kematangan, ITIL, Bank.

Abstract

ITIL v3 Framework Application to Design Information Technology Incident Management Governance (Case Study: Bank XYZ)

Information technology (IT) is one of the strategic investments for Banks. IT can increase the efficiency and effectiveness of operational activities and strengthen their competitive position. Given that IT is an expensive investment, while its implementation contains various risks, Banks need to implement Information Technology Governance. Banks are required to implement some standards for IT governance in multiple aspects, one of which is the IT incident management aspect. IT services at the Bank are crucial because they must work optimally with zero downtime. They must ensure the management and prevention of any problems that may arise to support the sustainability of the company's business processes. One of the frameworks that can be used for good IT service incident management is Information Technology Infrastructure Library version 3 (ITIL v3). ITIL's incident management aims to restore disrupted IT services to their normal state and reduce the business impact. To measure the extent to which the Bank has implemented IT Incident Management Governance, the maturity level is calculated by comparing the current state (as is) and the desired shape (to be) to obtain the gap. The process of maturity level assessment is carried out using interviews and questionnaires addressed to all stakeholders involved in the entire IT incident management process. The research results show that 15 of the 42 IT incident management processes have not reached the desired state. Based on these gaps, an IT incident management governance document was designed based on the ITIL v3 framework, which is expected when implemented in the Bank's daily operations. It will increase the availability of IT services.

Keywords

IT *governance,* Incident Management, Maturity Level Assessment, ITIL, Bank.

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, April 2022

Saleh Firdausi

Daftar Publikasi

“**Tidak ada publikasi yang menjadi bagian dari tesis**”

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**".

Halaman Persembahan

Assalamualaikum Warahmatullahi Wabarakatuh.

Segala puji dan syukur milik Allah SWT. Yang telah memberikan Rahmat, Taufiq dan Inayah-nya, sehingga tesis dengan judul Penerapan Framework ITIL v3 untuk Perbaikan Tata Kelola Manajemen Insiden Teknologi Informasi (studi kasus : Bank XYZ) ini dapat diselesaikan dengan baik meskipun masih banyak hal yang perlu mendapatkan tambahan dan sumbangan ide serta pikiran demi lebih baiknya karya ilmiah ini. Selawat dan salam semoga tetap terlimpahkan kepada Nabi Muhammad SAW, yang telah memberikan bimbingan dan petunjuk sehingga kita tetap teguh dalam rengkuhan iman dan Islam. Demikian juga rahmat dan kasih sayang semoga tetap tercurahkan kepada keluarga, para sahabat, pencari ilmu serta seluruh umat muslim. Selama proses penyelesaian karya ilmiah ini, penulis menyadari betapa banyak bantuan, dorongan, sumbangan yang diberikan oleh beberapa pihak, baik yang bersifat moril maupun material. Maka dari itu penulis mengucapkan terima kasih sebanyak-banyaknya kepada semua pihak yang sudah memberikan doa, dukungan, semangat, dan bimbingannya selama masa penulisan karya ilmiah ini.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Kata Pengantar

Puji syukur kepada Allah SWT atas karunia dan ijinnya. Atas ijinnya penulis bisa menyelesaikan karya ilmiah ini, tak lupa juga penulis ucapkan banyak terima kasih kepada:

1. Ibu, Bapak dan Adik yang telah memberikan doa dan dukungannya untuk menyelesaikan karya ilmiah ini.
2. Anindya Marisa Putri, S.T.P. yang telah menemani, menyemangati, dan selalu memberikan doa dan dukungannya untuk penulis.
3. Bapak M. Andri Setiawan, S.T., M.Sc., Ph.D. selaku dosen pembimbing yang selalu memberikan bimbingan dan masukan kepada penulis dalam penulisan karya ilmiah ini.
4. Ibu Direktur Program Pascasarjana, Izzati Muhimmah, S.T., M.Sc., Ph.D. dan para Asisten Direktur atas segala fasilitas yang telah di berikan selama penulis menempuh studi.
5. Program Pasca Sarjana Fakultas Teknologi Industri Universitas Islam Indonesia, yang telah memberikan kesempatan kepada untuk mengikuti program pendidikan Magister Informatika.
6. Bapak, Ibu dosen Pasca Sarjana Fakultas Teknologi Industri Universitas Islam Indonesia, yang telah membina dan menularkan ilmunya dengan tulus ikhlas.
7. Para Staf dan Karyawan Pasca Sarjana Fakultas Teknologi Industri Universitas Islam Indonesia, yang telah melayani dengan baik.
8. Para pimpinan, karyawan, dan seluruh orang-orang dari Bank NTB Syariah yang bersedia meluangkan waktunya demi kepentingan penelitian ini.
9. Kepada semua pihak yang telah turut serta di dalam membantu penulis untuk meraih gelar magister.
10. Tidak lupa terima kasih kepada rekan seperjuangan yang telah memberikan dukungan dalam menyelesaikan karya ilmiah ini.

Daftar Isi

Daftar Tabel xii

Daftar Gambar xiii

BAB 1 Pendahuluan 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 6

1.3 Kontribusi Ilmiah 6

BAB 2 Tinjauan Pustaka 7

2.1 Kajian Penelitian Terdahulu 7

2.2 Profil Bank XYZ 9

2.3 Tata Kelola Teknologi Informasi 11

2.4 *Framework* ITIL 12

2.4.1 Tujuan dan Objektif Manajemen Insiden ITIL 13

2.4.2 Ruang Lingkup Manajemen Insiden ITIL 13

2.4.3 Nilai Terhadap Bisnis 14

2.4.4 Kebijakan Manajemen Insiden 14

2.4.5 Prinsip dan Konsep Dasar ITIL 15

2.4.6 *Input* dan *Output* Manajemen Insiden 17

2.4.7 Pencatatan Insiden 18

2.4.8 Proses kegiatan, metode dan teknik ITIL 19

2.4.9 Model Kematangan ITIL (ITIL *Maturity Model*) 21

2.4.10 *Critical Success Factor* (CSFs) dan *Key Performance Indicators* (KPIs) 23

BAB 3 Metodologi 24

3.1 Langkah-langkah Penelitian 24

3.1.1 Pengumpulan Informasi dan Analisa Awal 25

3.1.2 Penilaian Tingkat Kematangan 26

3.1.3 Perancangan Saran Perbaikan Tata Kelola 29
3.1.4 Validasi Saran Perbaikan Tata Kelola 30
3.1.5 Kesimpulan 30
BAB 4 Hasil dan Pembahasan 31
4.1 Pengumpulan Informasi dan Analisa 31
4.2 Proses Manajemen Insiden di Bank XYZ Saat Ini 31
4.3 Penilaian Tingkat Kematangan 35
4.3.1 Tinjauan Dokumen Pendukung Manajemen Insiden 35
4.2.3 Analisis Tingkat Kematangan Saat Ini 38
4.2.3 Analisis Tingkat Kematangan yang Diharapkan 41
4.2.4 Analisis Kesenjangan 44
4.2.5 Kriteria Model Kematangan 52
4.2.6 Usulan Perbaikan Tata Kelola Manajemen Insiden TI 61
BAB 5 Kesimpulan dan Saran 63
5.1 Kesimpulan 63
5.2 Saran 63
Daftar Pustaka 64
LAMPIRAN A 68
LAMPIRAN B 70
LAMPIRAN C lxxiv

Daftar Tabel

Tabel 2.1 Perbandingan Penelitian Terdahulu 7
Tabel 2.2 CSF dan KPI ITIL v3 23
Tabel 3.1 Skala Tingkat Kematangan (Pratomo, 2016) 27
Tabel 3.2 Karakteristik Tingkat Kematangan Manajemen Insiden 27
Tabel 4.1 Dokumen Pendukung Proses Manajemen Insiden 35
Tabel 4.2 Proses Manajemen Insiden Saat ini 39
Tabel 4.3 Aktivitas Manajemen Insiden Saat ini 40
Tabel 4.4 Matriks Manajemen Insiden Saat ini 40
Tabel 4.5 Interaksi Proses Manajemen Insiden Saat ini 41
Tabel 4.6 Proses Manajemen Insiden Yang Diharapkan 42
Tabel 4.7 Aktivitas Manajemen Insiden Yang Diharapkan 43
Tabel 4.8 Matriks Manajemen Insiden Yang Diharapkan 43
Tabel 4.9 Interaksi Proses Manajemen Insiden Yang Diharapkan 43
Tabel 4.10 Rekap Kuesioner Kematangan Manajemen Insiden 46
Tabel 4.11 Kriteria Kematangan Proses Manajemen Insiden 53
Tabel 4.12 Kriteria Kematangan Aktivitas Manajemen Insiden 55
Tabel 4.13 Kriteria Kematangan Pengukuran Manajemen Insiden 58
Tabel 4.14 Kriteria Kematangan Interaksi Proses Manajemen Insiden 59

Daftar Gambar

Gambar 1.1 Rekap Laporan Insiden TI di Bank XYZ 3
Gambar 1.2 Rekap Klasifikasi Insiden TI di Bank XYZ 4
Gambar 1.3 Distribusi Penerapan *Framework* Manajemen Insiden TI..... 5
Gambar 2.1 Struktur Organisasi Bank XYZ 11
Gambar 2.2 *Service Lifecycle* pada *framework* ITIL v3 (The Stationery Office, 2011) 12
Gambar 2.3 Proses Manajemen Insiden (The Stationery Office, 2011)..... 19
Gambar 2.4 Representasi Maturity Model (UCISA, 2015)..... 22
Gambar 3.1 Tahapan Metode Penelitian 24
Gambar 4.1 Prosedur Manajemen Insiden Bank XYZ saat ini 33
Gambar 4.2 Kesenjangan Tingkat Kematangan Manajemen Insiden pada Bank XYZ 45

BAB 1
Pendahuluan

1.1 Latar Belakang

Teknologi Informasi (TI) menjadi salah satu kunci untuk menghadapi dan memenangkan persaingan. Badan pemerintah, organisasi, dan perusahaan di seluruh dunia menjadikan TI sebagai "tulang punggung" bagi setiap proses bisnis untuk mencapai tujuan bisnisnya masing-masing (Chi et al., 2017). TI adalah senjata penting bagi organisasi untuk mempercepat komunikasi dan koordinasi lintas organisasi, merampingkan proses bisnis, menyederhanakan komunikasi antara pelanggan dan perusahaan, dan mempercepat distribusi informasi ke seluruh organisasi (Samopa et al., 2017). Kenyataan yang terjadi adalah investasi yang dikeluarkan untuk TI tergolong mahal, namun tidak diikuti dengan nilai balik yang menguntungkan perusahaan (Chandra, 2018). Dalam lingkungan suatu organisasi yang kegiatan operasional sehari-harinya sangat bergantung pada TI, bahkan masalah kecil dapat mengurangi produktivitas. Berkaitan dengan hal tersebut, maka diperlukan suatu kerangka kerja untuk memastikan bahwa investasi TI dapat memaksimalkan keuntungan dan risiko TI dikelola dengan benar serta digunakan secara bertanggung jawab (Naim et al., 2021). Mengingat bahwa TI merupakan aset penting dalam operasional dan dapat meningkatkan nilai tambah dan daya saing bank, sementara dalam penyelenggaraannya mengandung berbagai risiko, maka bank perlu menerapkan tata kelola TI (*Information Technology Governance*). Tata kelola TI membantu perusahaan merencanakan dan mengendalikan investasi TI untuk mencapai tujuan bisnis mereka (Gërvalla et al., 2018). Bank adalah salah satu jenis perusahaan yang menggunakan TI sebagai inti operasionalnya (*core banking*).

Penerapan TI membawa perubahan positif dalam kegiatan operasional bank khususnya pada pengelolaan data bank sehingga dapat dilakukan dengan lebih efisien dan efektif serta menghasilkan informasi yang lebih cepat dan akurat. Bank dituntut untuk mengembangkan suatu strategi bisnis yang optimal dalam pemanfaatan TI guna meningkatkan efisiensi kegiatan operasional dan mutu pelayanan kepada nasabahnya. Salah satu bank daerah yang menggunakan TI sebagai inti kegiatan operasionalnya adalah Bank XYZ. Konversi yang dilakukan bank ini dari yang sebelumnya merupakan bank konvensional menjadi bank syariah memberikan semangat bagi Bank XYZ untuk dapat

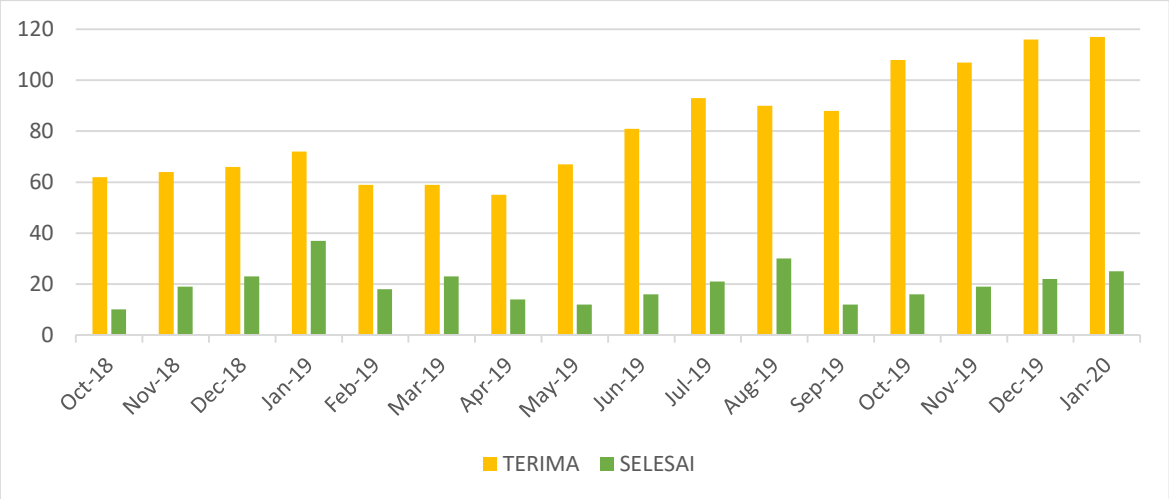
terus menyediakan layanan perbankan syariah bagi masyarakat serta meningkatkan perekonomian. Sejalan dengan hal tersebut, Bank XYZ melakukan revalidasi atas visi, misi, dan nilai-nilai budaya perusahaan, salah satunya yang berkaitan dengan TI yaitu "memperluas cakupan layanan untuk akses dan bertransaksi melalui penerapan TI yang andal". Konversi yang dilakukan akan juga berdampak pada proses bisnis yang ada di perusahaan dan secara langsung akan mempengaruhi layanan TI. Berdasarkan hal tersebut, TI menjadi inti dari operasional perbankan sehingga memerlukan perhatian khusus dalam pengelolaannya.

Penerapan tata kelola TI dalam sektor perbankan dilakukan dengan penyelarasan strategi TI dengan strategi bisnis bank, optimalisasi penggunaan sumber daya, pemanfaatan TI, pengukuran kinerja, dan penerapan manajemen risiko yang efektif. Penelitian sebelumnya telah menunjukkan bahwa perusahaan dengan tata kelola TI yang baik memberikan pengembalian nilai investasi TI yang lebih unggul daripada pesaing mereka, terutama karena mereka membuat keputusan TI yang lebih baik (Arisenta et al., 2020). Menurut Peraturan Otoritas Jasa Keuangan tahun 2016 tentang "Penerapan Manajemen Risiko Dalam Penggunaan TI oleh bank umum", bank diharuskan menerapkan beberapa standar acuan penilaian terkait TI. Standardisasi ini bertujuan untuk menyelaraskan strategi bisnis organisasi, strategi TI, infrastruktur TI, dan proses (Rizun et al., 2021). Penerapan *best practice* atau kerangka kerja untuk layanan TI seperti *Information Technology Infrastructure Library* (ITIL) adalah salah satu faktor kunci untuk menjamin kesesuaian proses, tidak hanya untuk implementasi tetapi juga untuk tindak lanjut dan pemeliharaan (Lucio-Nieto et al., 2012). Standardisasi untuk pelayanan TI sangat perlu dilakukan suatu organisasi untuk menjamin layanan yang ditawarkan dapat memuaskan dan memenuhi kebutuhan nasabah.

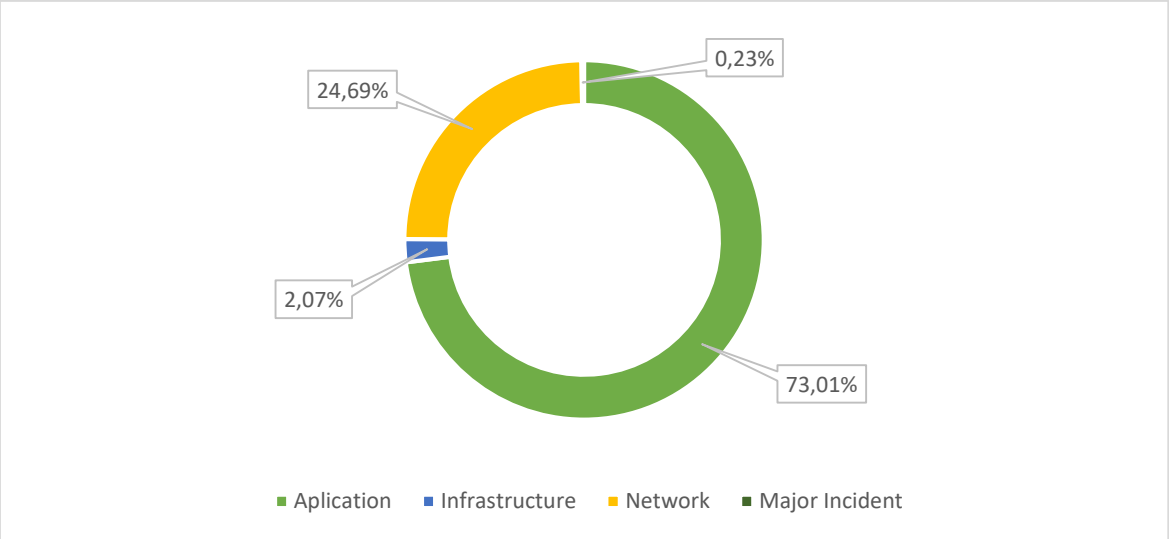
Persaingan antar bank dalam hal pemberian layanan yang berkualitas kepada nasabah sangat bergantung pada ketersediaan layanan TI (Alansari & Musleh Al-Sartawi, 2021). Ketersediaan layanan memiliki pengaruh yang sangat penting pada bisnis bank, pemenuhan kebutuhan nasabah, peningkatan referensi dan kepercayaan nasabah, produktivitas, dan citra perusahaan (Tadesse & Bakala, 2021). Layanan TI pada perbankan merupakan suatu hal yang sangat krusial karena layanan TI dituntut untuk selalu beroperasi dengan baik setiap saat. Layanan TI diakui sebagai aset organisasi yang penting, strategis, yang harus dikelola untuk kesuksesan bisnis (Amorim et al., 2021). Layanan TI dapat meningkatkan kenyamanan pelanggan dengan memungkinkan transaksi 24 jam, sehingga

meningkatkan kepuasan pelanggan dan memberikan keunggulan kompetitif (Gangopadhyay & Nilakantan, 2021). Pelayanan perbankan membutuhkan manajemen layanan yang berkualitas dan akurat sehingga meminimalkan terjadinya gangguan layanan (Palilingan & Batmetan, 2018). Bank harus menjamin bahwa kinerja layanan TI dapat berjalan dengan maksimal dan juga mampu melakukan pengelolaan dan pencegahan setiap insiden yang muncul guna mendukung keberlangsungan proses bisnis perusahaan (Pratomo, 2016).

Insiden adalah sebuah interupsi atau pengurangan kualitas layanan TI (UCISA, 2015). Kegagalan dalam mengelola insiden dapat mengakibatkan interupsi yang berkelanjutan, prioritas resolusi yang tidak ditentukan dengan baik dan informasi manajemen yang buruk. Salah satu ukuran utama suatu organisasi berhasil mengelola insiden dengan baik adalah lamanya waktu yang dibutuhkan untuk menyelesaikan suatu insiden (J. Aguiar et al., 2018). Insiden TI dapat mempengaruhi operasional bisnis dan bisa menyebabkan dampak bisnis yang lebih parah (Yandri et al., 2019). Berdasarkan data yang didapat dari observasi awal pada Bank XYZ yaitu pada Gambar 0.1, terlihat bahwa penanganan insiden di Bank XYZ masih terdapat insiden yang belum diselesaikan dari periode sebelumnya. Hal ini membutuhkan perhatian lebih karena adanya layanan yang menjadi terganggu yang diakibatkan insiden yang tak kunjung terselesaikan. Kemudian pada Gambar 0.2 terlihat bahwa jenis insiden yang paling banyak dilaporkan adalah insiden aplikasi, diikuti oleh insiden jaringan. Maka dari itu dibutuhkan suatu proses Manajemen Insiden yang dirancang dengan baik agar layanan TI dapat berjalan sebagaimana mestinya, meningkatkan penyelesaian insiden, meminimalkan dampak yang ditimbulkan, dan terlebih lagi untuk meningkatkan kepuasan nasabah.



Gambar 0.1 Rekap Laporan Insiden TI di Bank XYZ

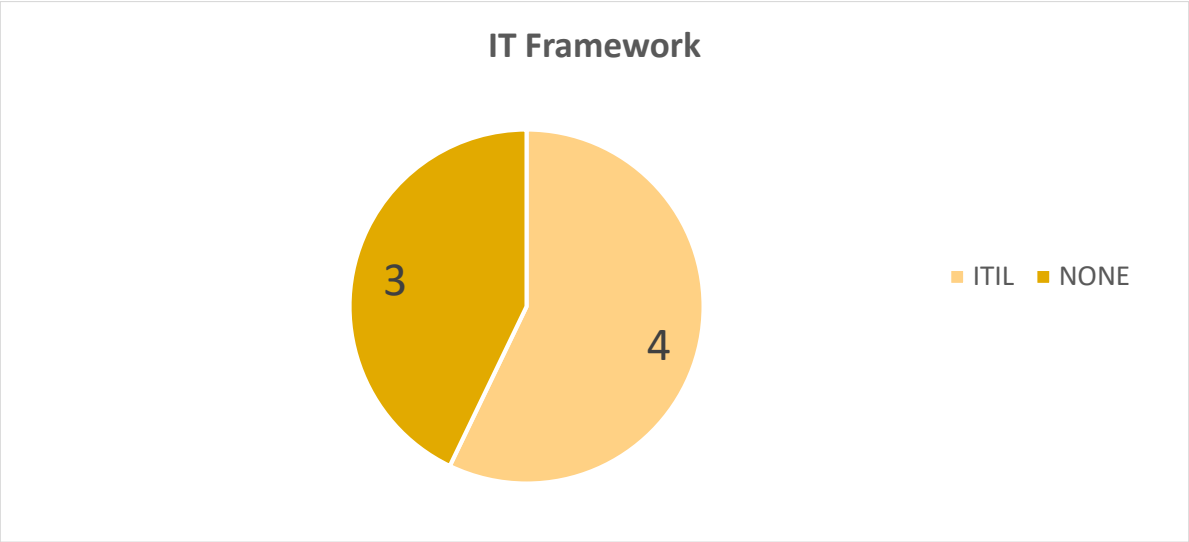


Gambar 0.2 Rekap Klasifikasi Insiden TI di Bank XYZ

Manajemen Insiden merupakan elemen kunci bagi tersedianya layanan TI (Haryanti & Pribadi, 2019). Manajemen insiden memerlukan perhatian lebih dari perusahaan karena berkaitan langsung dengan operasional dan layanan yang diberikan ke nasabah. Hal ini berarti bahwa Manajemen Insiden dapat membentuk cara pandang nasabah terhadap keseluruhan organisasi. Tujuan utama dari proses manajemen insiden adalah untuk memulihkan layanan operasional secepat mungkin dan meminimalkan dampak yang ditimbulkan. Manajemen insiden dapat meminimalkan penundaan (*delay*) antara resolusi insiden, mengurangi ketidaktersediaan layanan, dan biaya karena hilangnya layanan (Gërvalla et al., 2018). Manajemen insiden memerlukan suatu kerangka kerja yang baik dan benar sehingga diharapkan manajemen insiden TI lebih sigap terhadap segala macam permasalahan yang akan muncul. Salah satu *framework* yang dapat digunakan sebagai standar manajemen insiden layanan TI suatu organisasi adalah ITIL v3. Meskipun begitu, banyak organisasi hanya berfokus pada masalah teknis dan tidak fokus pada nilai (*value*) yang didapat dari penerapan standar/kerangka kerja dalam upaya peningkatan ketersediaan layanan (Palilingan & Batmetan, 2018).

ITIL adalah seperangkat *best practice* yang digunakan untuk membantu implementasi dari sebuah kerangka kerja untuk pengelolaan layanan TI (IT *Service Management*) yaitu termasuk pendefinisian pengelolaan layanan yang terintegrasi, berbasis proses, dan praktik-praktik terbaik yang diterapkan dalam sebuah organisasi (Ruiz et al., 2018). ITIL bertujuan untuk meningkatkan standar kualitas layanan TI serta meningkatkan efektivitas dan efisiensi pemberian layanan TI. Semakin pentingnya peningkatan

manajemen layanan telah menyebabkan munculnya standar dan kerangka kerja internasional seperti: COBIT 5 (*Control Objectives for Information and Related Technology*), ITIL v3 2011 *Edition* (*Information Technology Infrastructure Library*), ISO/IEC 38500:2008, ISO 17799 / ISO 27000 *Series,* ISO/IEC 20000, CMMI/SPICE (ISO/IEC 15504), *Balanced Scorecard*, dan AS 8015-2005 (Orta et al., 2014).



Gambar 0.3 Distribusi Penerapan *Framework* Manajemen Insiden TI

Beberapa perusahaan yang menjadikan TI sebagai inti operasionalnya telah menerapkan *framework* ITIL v3 sebagai acuan dalam pelaksanaan manajemen insiden di perusahaan mereka. Gambar 0.3 menunjukkan bahwa 4 dari 7 perusahaan menggunakan *framework* ITIL dalam hal manajemen insiden TI (J. F. F. Aguiar, 2017). Penelitian sebelumnya (Marrone & Kolbe, 2011a, 2011b) menunjukkan ada manfaat operasional dan strategis yang diperoleh organisasi dengan implementasi ITIL di perusahaan mereka. ITIL adalah *framework* yang paling banyak digunakan untuk manajemen insiden TI (Ruiz et al., 2018; Widianto & Subriadi, 2021; Yamamoto, 2017). Studi menunjukkan bahwa penerapan kerangka kerja manajemen insiden yang baik mengarah pada (1) meningkatkan efisiensi operasional dan mengurangi pengeluaran TI, (2) meningkatkan orientasi layanan dan fokus pada pemberian layanan, (3) meningkatkan keselarasan, baik secara eksternal dengan pelanggan maupun secara internal, dan (4) untuk meningkatkan kualitas layanan dan meningkatkan kepuasan pelanggan (Yamamoto, 2017). Pemilihan *framework* ITIL v3 dikarenakan memiliki kelebihan rekomendasi secara praktis (*best practice*) jika dibandingkan dengan *framework* lain seperti COBIT yang membahas strategis (J. Aguiar et al., 2018). Manajemen insiden memerlukan tindakan yang cepat untuk mengembalikan

layanan TI seperti keadaan normalnya, karena itu ITIL cocok digunakan untuk hal yang bersifat teknis seperti ini (Yandri et al., 2019). ITIL memberikan kualitas layanan yang lebih baik, ketersediaan dan stabilitas layanan TI yang lebih baik, pandangan yang jelas tentang kapasitas area layanan TI, dan peningkatan kepuasan pelanggan (De Barros et al., 2015). Penelitian ini akan melakukan perancangan tata kelola manajemen insiden TI yang berdasarkan *framework* ITIL v3 pada Bank XYZ.

1.2 Rumusan Masalah

Penerapan TI yang dikelola dengan baik dan bertanggung jawab akan memaksimalkan manfaat dan meminimalkan risiko yang akan timbul. Penerapan TI yang baik dilakukan dengan menyelaraskan TI dengan tujuan bisnis yang ingin dicapai organisasi. Berdasarkan hal tersebut, dibuat rumusan masalah dalam penelitian sebagai berikut :

1. Bagaimanakah kesenjangan tata kelola manajemen insiden TI saat ini (*as is*) dan yang diharapkan (*to be*) guna mendukung layanan TI di Bank XYZ?
2. Bagaimana merancang perbaikan tata kelola manajemen insiden TI untuk mendukung operasional Bank XYZ yang berdasarkan *framework* ITIL v3?

Lingkup penelitian ini yaitu penelitian dilakukan di Bank XYZ menggunakan *framework* ITIL v3 untuk mengukur tingkat kematangan manajemen insiden. Domain ITIL yang diteliti yaitu *Service Operation* yang berfokus pada manajemen insiden. Sedangkan tujuan yang ingin dicapai dari penelitian ini adalah :

1. Mengetahui kondisi kesenjangan tata kelola manajemen insiden TI saat ini (*as is*) dan yang diharapkan (*to be*) guna mendukung layanan TI di Bank XYZ.
2. Membuat rancangan perbaikan tata kelola manajemen insiden TI untuk mendukung kegiatan operasional Bank XYZ yang berdasarkan *framework* ITIL v3.

1.3 Kontribusi Ilmiah

Manfaat yang dapat diperolah dari penelitian ini adalah sebagai berikut :

1. Pelajaran yang didapat (*lesson learned*) terkait penerapan dan perbaikan tata kelola manajemen insiden yang menggunakan *framework* ITIL v3 di sektor perbankan sehingga dapat menjadi bahan acuan untuk penelitian selanjutnya.
2. Penelitian ini dapat menjadi pertimbangan bagi Bank XYZ untuk meningkatkan proses manajemen insiden yang berjalan di perusahaan mereka untuk meningkatkan layanan TI yang diberikan serta meningkatkan kepuasan nasabah.

BAB 2
Tinjauan Pustaka

2.1 Kajian Penelitian Terdahulu

Guna mendukung studi kasus yang akan dilakukan, perlu dilakukan pembuatan tabel perbandingan dari penelitian-penelitian sebelumnya yang berupa makalah. Adapun hasil studi pustaka dapat dilihat pada Tabel 0.1 berikut :

Tabel 0.1 Perbandingan Penelitian Terdahulu

Nama Peneliti	**Kerangka Kerja**	**Pengukuran *Maturity Level***	***Self-Assessment Tool***	**Hasil Penelitian**
(Pratomo, 2016)	ITIL v3	tidak ada	UCISA	Dokumen proses manajemen insiden TI berdasarkan *framework* ITIL v3.
(Silitonga & Ali, 2010)	ITIL v3	tidak ada	tidak ada	Perbaikan Dokumen Tata Laksana *Help Desk*, metrik dan CSF, dan SLA.
(Chandra, 2018)	COBIT v4	ITGI *Maturity Model*	tidak ada	Saran perbaikan tata kelola teknologi informasi berdasarkan *maturity level* berbasis *framework* COBIT
(Wardani *et al*., 2016)	ITIL v3	ISO 15504	tidak ada	Pembuatan dokumen rekomendasi kebijakan TI, SOP, dan dokumen pendukung berdasarkan *maturity level* dan analisis prioritas.
(Aguiar, 2017)	ITIL v3, COBIT 5, dan CMMI-SVC	COBIT PAM, ISO/IEC 15504, CMMI-SVC, TIPA, Axelos	tidak ada	perbandingan *framework* manajemen insiden TI dan perbandingan pengukuran tingkat kematangan.

Tabel 0.1 di atas menunjukkan adanya persamaan yaitu pembuatan dokumen rekomendasi tata kelola teknologi informasi baik berupa perbaikan atas dokumen/kebijakan yang lama, maupun pembuatan dokumen/kebijakan yang baru didasarkan atas hasil analisis *maturity level*. Tabel tersebut juga menunjukkan beberapa *gap* dari penelitian yang pernah dilakukan sebelumnya. Beberapa penelitian belum menggunakan model pengukuran untuk tingkat kematangan (*maturity level*). Pengukuran tingkat kematangan sangat diperlukan untuk melakukan kontrol terhadap manajemen insiden TI. (J. F. F. Aguiar, 2017) menyatakan bahwa perusahaan tidak menggunakan model *maturity* yang spesifik dalam pengukuran kinerja terkait tata kelola teknologi informasi di perusahaan mereka, namun mereka menyadari akan pentingnya hal tersebut. Penelitian ini akan menggunakan ITIL *mautity model*. Alasan pemilihan ITIL *maturity model* ini karena merupakan model pengukuran bawaan dari *framework* ITIL v3 yang karakteristik tiap level kematangannya sudah terdefinisi secara jelas. ITIL *maturity model* terdiri dari 6 level yaitu *Absence*, *Initial*, *Repeatable*, *Defined*, *Managed*, dan *Optimized*. Penelitian ini akan menggunakan ITIL v3 untuk manajemen insiden dibandingkan dengan ITIL v4, karena ITIL v3 lebih detail membahas hal-hal teknis tentang manajemen insiden, sedangkan ITIL v4 lebih menekankan pada bagaimana kontribusi manajemen insiden dalam *service value chain*.

Gap lainnya adalah beberapa penelitian belum menggunakan *tools* pengukuran kemampuan diri (*Self-Assessment*) dalam pengukuran tingkat kematangan perusahaannya. Berdasarkan *University and Colleges Information System Association* (UCISA), proses penilaian manajemen insiden dilakukan menggunakan 4 *Service Operation Area* yang membagi *best practice* manajemen insiden yang ada pada ITIL ke dalam 4 komponen penilaian utama yang dipetakan secara kualitatif ke dalam skala ITIL *maturity level* yang terdiri dari (Alshathry, 2016):

- *The Incident Management Process* : kategori yang membahas pembentukan siklus (*life-cycle*) hidup manajemen insiden dalam sebuah organisasi yang termasuk kebijakan proses dan lain-lain.
- *Activities in Place Needed for the Success of Incident Management* : kategori ini membahas tentang kebutuhan-kebutuhan lanjutan (*advanced*) yang berkaitan dengan manajemen insiden yang menjamin kinerja yang efisien seperti adanya mekanisme eskalasi aktif, bas is pengetahuan, dan lain-lain.

- *Incident Management Metrics* : kategori yang membahas tentang *Key Performance Indicator* (KPI), laporan, dan metrik kinerja.
- *Incident Management Process Interactions* : kategori yang membahas integrasi manajemen insiden dengan area fungsional pendukung lainnya dalam organisasi seperti manajemen masalah, akar penyebab, dan lain-lain.

Keempat dimensi kematangan tersebut akan dinilai praktiknya dalam organisasi sehingga gambaran proses manajemen insiden yang berjalan saat ini dapat diketahui. Pembagian *best practice* ITIL ke dalam kategori seperti itu dapat memudahkan dalam pembuatan dan pengisian kuesioner *maturity level*. Penelitian ini akan menghasilkan rekomendasi tata kelola manajemen insiden teknologi informasi yang berdasarkan pada *framework* ITIL v3.

2.2 Profil Bank XYZ

Bank XYZ adalah Bank milik Pemerintah Provinsi Nusa Tenggara Barat bersama–sama dengan Pemerintah Kota/Kabupaten se-Nusa Tenggara Barat. Bank XYZ didirikan dan mulai beroperasi pada tanggal 5 Juli 1964 berdasarkan:

1. Peraturan Daerah Provinsi Nusa Tenggara Barat No.06 Tahun 1963 tentang Pendirian Bank Pembangunan Daerah Nusa Tenggara Barat, beserta beberapa perubahannya;
2. Disempurnakan dengan Peraturan Daerah Provinsi Nusa Tenggara Barat No.08 Tahun 1984 tentang Bank Pembangunan Daerah Provinsi Nusa Tenggara Barat;
3. Kemudian diubah kembali dengan Peraturan Daerah Provinsi Nusa Tenggara Barat No. 01 Tahun 1993 tentang Bank Pembangunan Daerah Nusa Tenggara Barat.
4. Perubahan Bentuk Hukum Bank Pembangunan Daerah Nusa Tenggara Barat dari Perusahaan Daerah menjadi Perseroan Terbatas (PT) Bank Pembangunan Daerah Nusa Tenggara Barat tanggal 19 Maret 1999.

Persiapan pendirian Bank XYZ dilakukan oleh Bapak H. Muhammad Syareh, SH yang kemudian menjadi Direktur Utama pertama. Dan seiring dengan berjalannya waktu sesuai dengan periode masa jabatan hingga saat ini tahun 2021 Bapak H. Kukuh Rahardjo sebagai Direktur Utama untuk periode tahun 2018-2022. Perubahan Bentuk Hukum dari Perusahaan Daerah menjadi Perseroan Terbatas (PT) pada tanggal 19 Maret 1999.

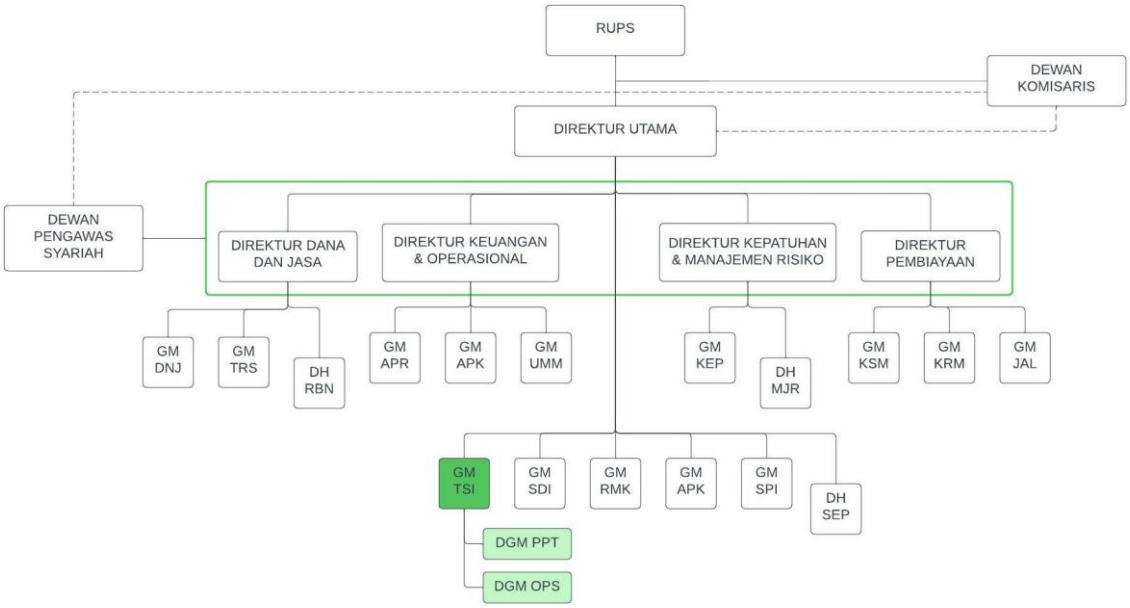
Sesuai hasil keputusan Rapat Umum Pemegang Saham tanggal 13 Juni 2016 yang menyetujui PT Bank XYZ melaksanakan konversi menjadi Bank XYZ memberikan harapan baru bagi penguatan ekonomi kerakyatan yang berkeadilan di Nusa Tenggara

Barat. Sesuai keputusan tersebut proses konversi Bank agar dilaksanakan melalui kajian komprehensif dan sesuai dengan ketentuan yang berlaku. Alhamdulillah, proses konversi yang membutuhkan waktu selama hampir 2 (tahun) melahirkan Bank XYZ resmi melakukan kegiatan operasional sesuai prinsip-prinsip syariah pada tanggal 24 September 2018, sesuai Keputusan Anggota Dewan Komisioner Otoritas Jasa Keuangan Nomor : Kep-145/D.03/2018 tentang Pemberian Izin Perubahan Kegiatan Usaha Bank Umum Konvensional menjadi Bank Umum Syariah PT Bank XYZ menetapkan bahwa memberikan izin kepada PT Bank XYZ yang berkedudukan di Mataram untuk melakukan perubahan kegiatan usaha Bank Umum Konvensional menjadi Bank Umum Syariah dengan nama PT Bank XYZ.

Didirikan dengan tujuan untuk dapat menjadi Bank Syariah yang amanah, terkemuka dan pilihan masyarakat, memberikan semangat lebih bagi Bank XYZ untuk dapat terus menyediakan layanan perbankan syariah untuk membantu masyarakat dalam transaksi perbankan syariah serta meningkatkan perekonomian daerah di Nusa Tenggara Barat.

Model bisnis yang telah disusun, merumuskan segmen bisnis utama Bank dan bagaimana Bank bisa mewujudkan visi, misi, dan sasaran bisnisnya. Sebagaimana tercermin dalam visi Bank untuk menjadi Bank Syariah yang amanah, terkemuka dan pilihan masyarakat. Visi ini akan diwujudkan oleh Bank dengan memberikan solusi keuangan yang menyeluruh kepada nasabah sehingga Bank dapat menjadi partner keuangan nasabah sepanjang masa, serta mencapai nilai tambah yang bermanfaat bagi seluruh *stakeholder* yaitu nasabah, investor, karyawan, komunitas, dan industri keuangan.

Seiring dengan berjalannya waktu, Bank XYZ terus berkembang hingga saat ini memiliki Kantor yang berjumlah 50 kantor yang terdiri dari 1 kantor pusat, 12 kantor cabang, 24 kantor cabang pembantu, 6 kantor kas dan 7 kantor pelayanan. Guna mendukung kualitas pelayanan Bank XYZ 255 ATM yang tersebar di seluruh kota/Kabupaten se-NTB. Bank XYZ didukung oleh karyawan dan karyawati sampai dengan 31 Desember 2021 berjumlah 1.433 orang. Struktur organisasi Bank XYZ dapat dilihat pada Gambar 0.1 berikut :



Gambar 0.1 Struktur Organisasi Bank XYZ

Penelitian ini akan berfokus pada Divisi Teknologi Sistem informasi (TSI) yang dikepalai oleh seorang *General Manager* (GM) dan dibantu oleh 2 *Deputy General Manager* yaitu DGM Pengembangan dan DGM Operasional. Divisi TSI bertanggung jawab mengelola seluruh sistem informasi yang ada dalam seluruh area operasional Bank XYZ mulai dari Kantor Cabang Pembantu, Kantor Cabang, sampai dengan sistem di Kantor Pusat. Divisi TSI beranggotakan 20 orang yaitu 4 analis pengembangan, 8 admin pengembangan (*programer*), dan 8 admin operasional.

2.3 Tata Kelola Teknologi Informasi

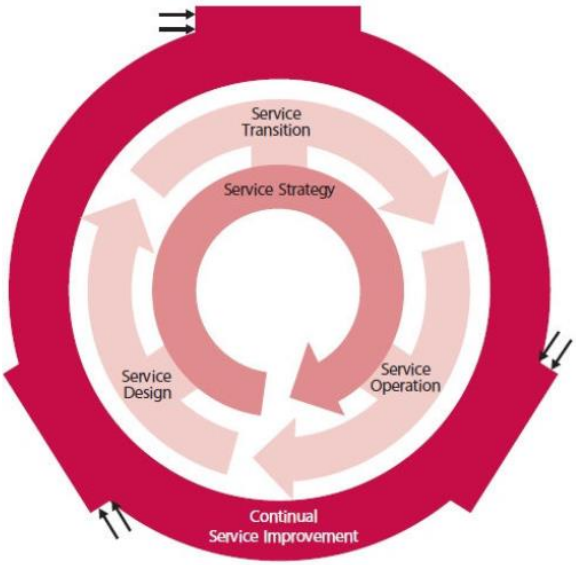
Dalam perspektif umum, tata kelola (*governance*) adalah kemampuan pemerintah (*goverment*) untuk membuat aturan dan menegakkannya, serta untuk pemberian layanan kepada masyarakatnya, terlepas pemerintah tersebut apakah demokratis ataupun tidak (Fukuyama, 2013).

Tata kelola TI adalah sekumpulan aturan yang mencangkup mulai dari manajemen, perencanaan, kebijakan penilaian kinerja, proses dan penerapan; hal-hal yang terkait dengan hak keputusan, kewenangan, kendali, dan ukuran kinerja terhadap investasi, perencanaan, anggaran belanja, komitmen, layanan, perubahan besar, keamanan, privasi, keberlangsungan bisnis agar sesuai dengan hukum dan kebijakan organisasi (Selig, 2008)

Struktur tata kelola TI menjelaskan tentang berbagai hak dan tanggung jawab serta aturan dan prosedur dalam pengambilan keputusan yang terkait TI. Tata kelola TI yang ada pada suatu organisasi disesuaikan dengan kebutuhan organisasi tersebut. Pengembangan tata kelola TI di berbagai organisasi, terdapat berbagai kerangka kerja (*framework*) yang dapat digunakan sebagai acuan dalam pembuatannya. Beberapa contoh diantaranya adalah : COBIT 5, ITIL v3 2011 *Edition*, ISO/IEC 38500:2008, ISO 17799 / ISO 27000 *Series,* ISO/IEC 20000, CMMI/SPICE (ISO/IEC 15504), *Balanced Scorecard*, dan AS 8015-2005. Penelitian ini akan menggunakan *framework* ITIL v3 sebagai alat pengukuran tingkat kematangan perusahaan dalam hal manajemen insiden TI. *Framework* ITIL v3 juga digunakan sebagai dasar untuk pembuatan saran perbaikan penerapan tata kelola manajemen insiden TI di Bank XYZ.

2.4 *Framework* ITIL

Framework ITIL (*Information Technology Infrastructure Library*) adalah sebuah kerangka kerja untuk tata kelola TI yang berisi praktik-praktik terbaik (*best practice*) khususnya dalam hal manajemen layanan TI (Silitonga & Ali, 2010). Gambar 0.2 *Service Lifecycle* pada *framework* ITIL v3 yang menjelaskan tahapan-tahapan pengelolaan manajemen layanan TI pada *framework* ITIL, yaitu sebagai suatu *service lifecycle*. Proses Manajemen Insiden dalam *framework* ITIL terdapat pada domain *Service Operation* yang akan dijelaskan pada sub-bab 2.3.1.



Gambar 0.2 *Service Lifecycle* pada *framework* ITIL v3 (The Stationery Office, 2011)

Menurut *framework* ITIL, pengertian insiden adalah sebuah interupsi atau pengurangan kualitas yang terjadi pada layanan TI. Suatu kesalahan konfigurasi pada sistem juga dapat dianggap sebagai insiden walaupun belum menimbulkan masalah yang berarti pada sistem tersebut. Manajemen insiden (*incident management*) adalah serangkaian proses yang dilakukan untuk menyelesaikan suatu insiden, mulai dari pelaporan hinggap penutupan insiden. Proses manajemen insiden dilakukan berdasarkan laporan dari *user* melalui *Help Desk*, laporan teknisi, dan juga laporan otomatis yang dibuat oleh *tool event management*. Pembahasan berikut akan menjelaskan mengenai praktik terbaik (*best practice*) yang dapat diterapkan dalam manajemen insiden TI menurut *framework* ITIL, mulai dari tujuan dan objektif manajemen insiden hingga prosedur yang dilakukan dalam manajemen insiden TI.

2.4.1 Tujuan dan Objektif Manajemen Insiden ITIL

Tujuan utama (*Purpose*) dari manajemen insiden (*incident management*) adalah untuk mengembalikan kondisi layanan TI ke keadaan normal secepat mungkin, dan meminimalkan dampak negatif yang ditimbulkan terhadap kegiatan bisnis utama organisasi (The Stationery Office, 2011). Keadaan normal layanan TI adalah keadaan yang telah didefinisikan sebelumnya dalam sebuah *Service Level Agreement* (SLA) yaitu keadaan dimana layanan TI bekerja sesuai tingkat layanan dan operasional yang telah disetujui. Objektif dari proses manajemen insiden antara lain sebagai berikut :

1. Memastikan terdapat prosedur standar dalam penanganan insiden yang efisien dan cepat.
2. Meningkatkan visibilitas dan komunikasi insiden kepada staf pendukung bisnis dan TI
3. Meningkatkan kecepatan komunikasi dan pelaporan saat insiden terjadi
4. Menyelaraskan aktivitas dan prioritas manajemen insiden dengan tujuan bisnis.
5. Meningkatkan kepuasan nasabah terhadap kualitas layanan TI.

2.4.2 Ruang Lingkup Manajemen Insiden ITIL

Manajemen insiden mencangkup setiap peristiwa yang dapat mengganggu suatu layanan. Termasuk laporan dari pengguna baik melalui *Help Desk* maupun laporan dari perangkat deteksi otomatis. Insiden juga dapat dilaporkan dan/atau dicatat oleh staf teknis. Misalnya, staf teknis mendeteksi suatu hal yang tidak diinginkan dari perangkat keras atau komponen jaringan, mereka dapat melaporkan atau mencatat insiden dan merujuknya ke *Help Desk*.

Meskipun insiden dan permintaan layanan (*service request*) dilaporkan ke *Help Desk*, bukan berarti keduanya adalah hal yang sama. Permintaan layanan tidak menunjukkan gangguan terhadap layanan, tetapi merupakan mekanisme untuk memenuhi kebutuhan pengguna. Permintaan layanan ditangani oleh proses pemenuhan permintaan (*request fulfilment process*).

2.4.3 Nilai Terhadap Bisnis

Manajemen insiden dapat memberikan nilai tambah (*value*) bagi perusahaan dengan cara :

1. Mengurangi pekerjaan yang tidak direncanakan (*unplanned labour*) dan biaya yang disebabkan oleh insiden.
2. Meningkatkan ketersediaan layanan dengan cara mengurangi waktu henti (*downtime*) yang dibutuhkan untuk mendeteksi dan menyelesaikan suatu insiden.
3. Penyelarasan aktivitas TI dengan prioritas bisnis secara *real-time* dengan cara mengidentifikasi prioritas bisnis dan secara dinamis mengalokasikan sumber daya yang diperlukan.
4. Mengidentifikasi potensi peningkatan layanan.

2.4.4 Kebijakan Manajemen Insiden

Berikut beberapa contoh kebijakan manajemen insiden yang dapat diterapkan dalam perusahaan :

1. Insiden dan statusnya harus dikomunikasikan dengan efektif dan tepat waktu. Fungsi meja layanan (*Help Desk*) yang baik adalah untuk mengoordinasikan komunikasi terkait insiden kepada mereka yang terkena dampak serta mereka yang bekerja untuk menyelesaikannya.
2. Insiden harus diselesaikan dalam jangka waktu (*timeframes*) yang dapat diterima oleh bisnis. Artinya terdapat dukungan teknologi yang tepat untuk merekam, mengklasifikasikan, memprioritaskan, dan mendiagnosis insiden secara efisien.
3. Kepuasan nasabah harus selalu dijaga. Staf pendukung yang berorientasi pelanggan dan terlatih secara teknis dengan tingkat keterampilan yang benar digunakan secara efektif di semua tahap proses.
4. Pemrosesan dan penanganan insiden harus diselaraskan dengan tingkat dan tujuan layanan secara keseluruhan. Aktivitas manajemen insiden mendukung tingkat dan tujuan layanan dengan memprioritaskan aktivitas tersebut berdasarkan kebutuhan bisnis yang sebenarnya.

5. Semua insiden harus disimpan dan dikelola dalam satu sistem manajemen. Status dan informasi rinci tentang insiden harus dicatat dan diperbarui secara tepat waktu dalam catatan insiden (*incident records*).
6. Semua insiden harus mengikuti skema klasifikasi standar yang konsisten. Hal ini bertujuan untuk memberikan akses lebih cepat ke informasi insiden dan pemecahan masalah, memberikan dukungan yang lebih baik untuk diagnosis insiden.
7. Catatan insiden harus diaudit secara teratur untuk memastikan telah di-*input* dan dikategorikan dengan benar. Hal ini bertujuan untuk memastikan bahwa informasi insiden akurat, dikategorikan dengan benar, dan dapat dipercaya.
8. Semua catatan insiden harus menggunakan format umum. Hal ini dilakukan untuk memastikan bahwa semua informasi yang diperlukan tentang insiden tersedia dalam format umum untuk mendukung aktivitas manajemen insiden dan mudah dibagikan ke area dukungan lain yang bergantung pada informasi insiden.
9. Adanya seperangkat kriteria umum dan disepakati untuk prioritasi dan eskalasi insiden. Memastikan bahwa cara prioritasi dan eskalasi insiden berdasarkan kebijakan yang disepakati dan tidak hanya ditentukan oleh individu dalam organisasi.

2.4.5 Prinsip dan Konsep Dasar ITIL

Ada beberapa hal dasar yang perlu dipertimbangkan dan diputuskan ketika mempertimbangkan manajemen insiden.

1. Skala Waktu (*Timescales*)

Skala waktu harus disetujui dalam setiap tahapan penanganan insiden (tergantung pada tingkat prioritas insiden), berdasarkan respons insiden secara keseluruhan dan target resolusi yang tertuang dalam SLA. Semua staf pendukung operasional harus memahami sepenuhnya tentang rentang waktu ini. *Tools* manajemen layanan digunakan untuk automasi rentang waktu dan eskalasi insiden berdasarkan aturan yang telah ditentukan sebelumnya.

2. Model Insiden

Kebanyakan insiden berurusan dengan sesuatu yang telah terjadi sebelumnya dan mungkin akan terjadi lagi. Maka dari itu perlunya dilakukan penetapan standar model insiden dan menerapkannya pada saat insiden terjadi.

Model insiden adalah cara untuk menentukan langkah-langkah yang harus diambil untuk menangani suatu proses (dalam hal ini proses untuk menangani jenis insiden tertentu) dengan cara yang telah disepakati. Tujuan dari model insiden adalah untuk

memastikan bahwa insiden ditangani dengan prosedur standar yang telah ditentukan dan dalam rentang waktu (*timescales*) yang telah ditentukan. Model insiden harus terdiri dari beberapa hal berikut

- Tahapan-tahapan yang harus dilakukan.
- Urutan kronologis bagaimana tahapan-tahapan tersebut dilakukan
- Uraian Tanggung jawab setiap orang yang terlibat
- Tindakan pencegahan yang dilakukan sebelum penyelesaian insiden (contoh : *backup data*)
- Skala waktu (*timescales*) untuk penyelesaian tindakan
- Prosedur eskalasi
- Kegiatan pemeliharaan bukti (*evidence-preservation*) terkait insiden

3. Insiden Besar (*Major Incident*)

Insiden Besar memerlukan suatu prosedur terpisah, dengan rentang waktu yang lebih pendek dan urgensi yang lebih besar. Definisi tentang apa yang merupakan insiden besar harus disepakati dan idealnya dipetakan ke dalam skema prioritas insiden secara keseluruhan sedemikian rupa sehingga akan ditangani melalui prosedur terpisah.

Jika diperlukan, prosedur insiden besar harus mencakup pembentukan tim yang terpisah di bawah kepemimpinan langsung manajer insiden, yang berfokus pada insiden ini saja untuk memastikan bahwa sumber daya yang memadai digunakan untuk menemukan penyelesaian yang cepat. Jika manajer *Help Desk* juga merangkap peran manajer insiden (misalnya dalam organisasi kecil), maka orang yang terpisah perlu ditunjuk untuk memimpin tim investigasi insiden besar untuk menghindari konflik waktu atau prioritas tetapi harus akhirnya melaporkan kembali ke manajer insiden.

4. Pelacakan status insiden

Insiden harus dilacak sepanjang siklus hidupnya (*lifecycle*) untuk mendukung penanganan dan pelaporan yang tepat mengenai status insiden. Dalam sistem manajemen insiden, kode status dapat digunakan untuk menunjukkan di mana posisi insiden berada dalam kaitannya dengan siklus hidup. beberapa kode status manajemen insiden adalah sebagai berikut :

- Open: Suatu insiden telah diidentifikasi tetapi belum dialokasikan ke sumber daya untuk penyelesaiannya.
- In-Progress : Insiden ini sedang dalam proses penyelidikan dan penyelesaian
- Resolved : Resolusi telah dilakukan untuk insiden tersebut tetapi keadaan normal layanan belum divalidasi oleh bisnis atau pengguna akhir

- Closed : Pengguna atau bisnis telah menyetujui bahwa insiden tersebut telah diselesaikan dan bahwa keadaan normal layanan telah dipulihkan.

2.4.6 *Input* dan *Output* Manajemen Insiden

Insiden dapat dipicu pengguna melakukan pelaporan kepada *Help Desk* melalui telepon ataupun aplikasi pesan lainnya. Staf teknis mungkin melihat adanya potensi terjadinya kegagalan sistem dan melaporkannya sebagai insiden. Proses manajemen insiden memiliki masukan (*input*) dan keluaran (*output*). Contoh *input* dari proses manajemen insiden ITIL antara lain :

1. Informasi tentang sistem IT dan statusnya
2. Informasi tentang permasalahan yang diketahui beserta solusinya.
3. Komunikasi dan umpan balik tentang insiden dan gejalanya.
4. Tujuan dan sasaran operasional beserta tingkat layanannya.
5. Umpan balik dari nasabah tentang keberhasilan aktivitas resolusi insiden dan kualitas keseluruhan aktivitas manajemen insiden.
6. Kriteria yang disepakati untuk prioritas dan eskalasi insiden.

Kemudian *output* dari proses manajemen insiden TI menurut ITIL adalah sebagai berikut :

1. Penyelesaian insiden dan tindakan yang diambil untuk mencapainya.
2. Catatan manajemen insiden yang telah diperbarui dengan detail dan riwayat insiden yang akurat.
3. Klasifikasi insiden yang telah diperbarui untuk digunakan untuk mendukung aktivitas manajemen insiden secara proaktif.
4. Catatan khusus untuk insiden yang di mana penyebab yang mendasarinya belum diidentifikasi.
5. Validasi bahwa insiden tidak terulang untuk masalah yang telah terselesaikan.
6. Umpan balik tentang insiden yang terkait dengan perubahan.
7. Identifikasi sistem yang terkait dengan atau dipengaruhi oleh insiden.
8. Umpan balik kepuasan dari nasabah yang pernah mengalami insiden.
9. Komunikasi tentang detail riwayat insiden dan resolusi untuk membantu mengidentifikasi kualitas layanan secara keseluruhan.

2.4.7 Pencatatan Insiden

Menurut *framework* ITIL, informasi yang digunakan dalam proses manajemen insiden berasal dari :

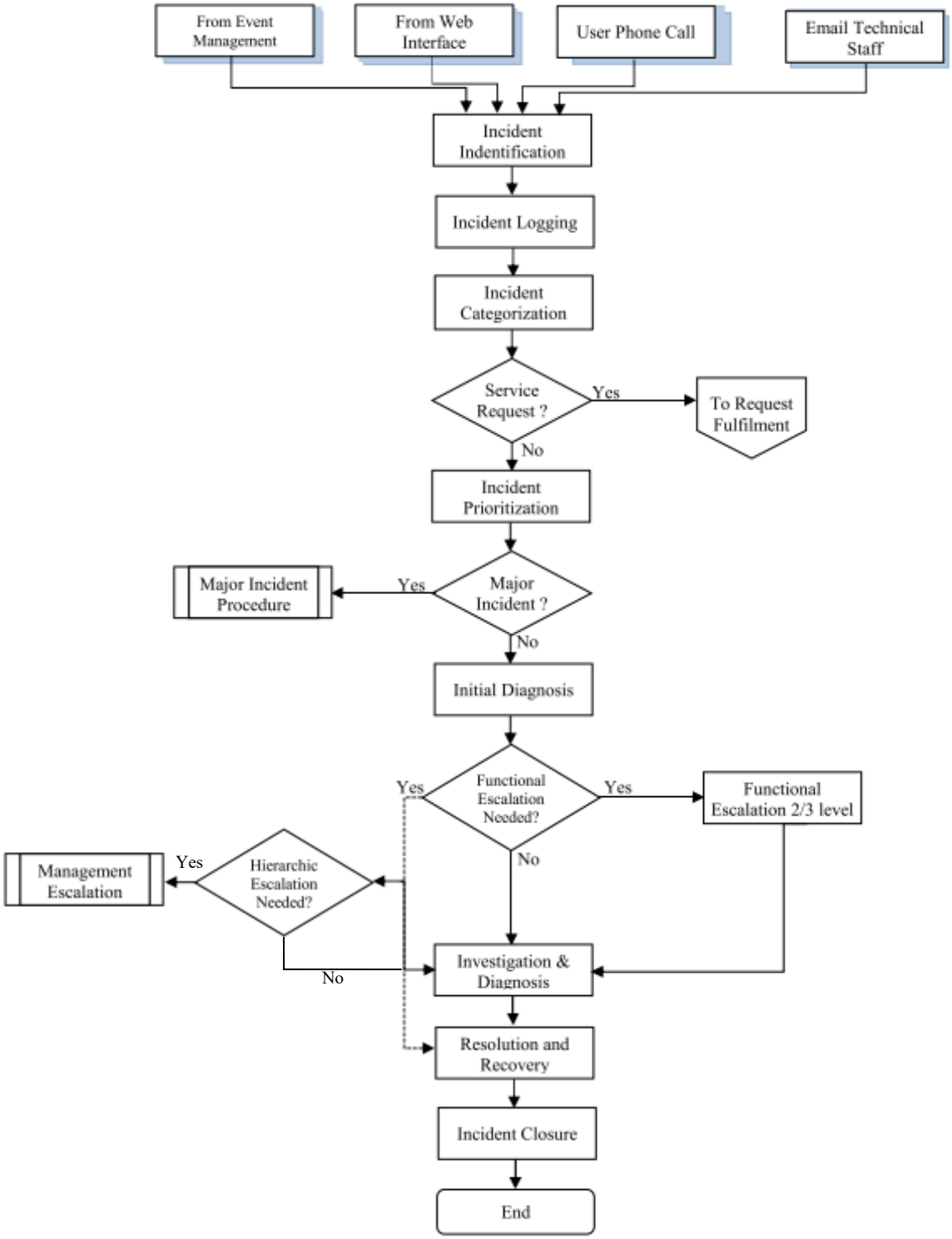
- Riwayat insiden
- Kategori insiden
- Tindakan penyelesaiannya
- Basis pengetahuan.

Catatan insiden yang digunakan dalam pelaporannya biasanya berisi :

- Nomor referensi unik
- Klasifikasi insiden
- Tanggal dan waktu pencatatan dan tindakan selanjutnya
- Nama dan identitas orang yang mencatat dan memperbarui catatan insiden.
- Nama dan detail kontak pengguna yang terdampak.
- Deskripsi gejala/tanda-tanda insiden.
- Detail tindakan apa saja yang diambil untuk mencoba mendiagnosis, menyelesaikan, atau membuat ulang insiden.
- Kategori insiden, dampak, urgensi dan prioritas.
- Hubungan dengan insiden lain, masalah, perubahan atau kesalahan (*error*) yang diketahui.
- Detail penutupan laporan, termasuk waktu, kategori, tindakan yang diambil, dan identitas orang yang menutup laporan tersebut.

2.4.8 Proses kegiatan, metode dan teknik ITIL

Berikut adalah proses-proses yang dilakukan dalam manajemen insiden menurut *framework* ITIL v3 dapat dilihat pada Gambar 0.3 berikut :



Gambar 0.3 Proses Manajemen Insiden (The Stationery Office, 2011)

1. Identifikasi Insiden (*Incident Identification*)

   Proses manajemen insiden (*incident management*) dimulai dengan identifikasi. Identifikasi yang paling umum dilakukan adalah melalui layanan *service desk* dan laporan dari staf teknisi. Selain itu identifikasi insiden dapat dilakukan secara otomatis oleh *tool event management*. *Tool* ini akan mengidentifikasi masalah sesaat ketika insiden terjadi. Kondisi ideal dari langkah identifikasi adalah insiden dapat teridentifikasi sebelum terjadi implikasi terhadap *user*.

2. Pencatatan Insiden (*Incident Logging*)

   Langkah ini wajib dilakukan untuk setiap jenis insiden baik yang berskala besar maupun kecil. Beberapa informasi yang harus dicatat terkait suatu insiden adalah ID, kategori insiden, waktu terjadi, deskripsi insiden, nama orang/grup yang bertanggung jawab atas penanganan, implikasi insiden, dan waktu penutupan tiket insiden.

3. Pengelompokan Insiden (*Incident Categorization*)

   Pembuatan kelompok/kategori insiden membutuhkan sebuah proses khusus antara pengelola TI dan pihak manajemen organisasi. Hal ini bertujuan untuk menghasilkan kategori insiden dan prioritas penanganannya yang sejalan dengan proses bisnis organisasi. Kategori insiden dapat dibuat berdasarkan perkiraan lamanya penanganan, implikasi terhadap proses bisnis organisasi, dan jumlah staf teknis terkait.

4. Prioritas Insiden (*Incident Prioritization*)

   Langkah prioritas insiden dilakukan berdasarkan kategorisasi yang telah dibuat sebelumnya. Prioritas penanganan insiden dapat dilakukan berdasarkan besarnya implikasi insiden terhadap kegiatan bisnis utama organisasi, ataupun berdasarkan lamanya penanganan insiden. Insiden yang memiliki prioritas paling tinggi ditangani terlebih dahulu.

5. Diagnosa Awal (*Initial Diagnosis*)

   Diagnosa awal terhadap insiden wajib dilakukan oleh setiap pihak yang pertama kali berhubungan dengan insiden baik itu *service desk*, staf teknis, maupun perangkat otomatis seperti *tool event management*. Jika insiden ditemukan oleh *service desk* melalui telepon dari *user*, maka diusahakan *service desk* tersebut yang menyelesaikan insiden selama *user* masih berhubungan melalui telepon.

6. Eskalasi Insiden (*Incident Escalation*)

   Eskalasi insiden adalah tindakan menaikkan level penanganan insiden. Hal ini berkaitan erat dengan hasil diagnosa awal terhadap insiden. Jika dari diagnosa

ditemukan insiden yang tidak dapat ditangani, maka wajib dilakukan eskalasi insiden. Eskalasi insiden ada 2 macam, yaitu eskalasi fungsi dan eskalasi hierarki. Eskalasi fungsi adalah tindakan menaikkan level penanganan kepada satu level di atasnya. Sedangkan eskalasi hierarki adalah tindakan menaikkan level penanganan melintasi hierarki organisasi misalnya kepada manajer IT atau manajer bisnis yang terkait.

7. Investigasi (*Investigation and Diagnosis*)

   Tindakan investigasi dilakukan untuk menemukan sumber penyebab insiden. Dalam melakukan investigasi, setiap tindakan wajib dilaporkan juga ke dalam formulir insiden. Hal ini berguna sebagai data historis tindakan penanganan suatu insiden.

8. Resolusi (*Resolution and Recovery*)

   Langkah ini merupakan tindakan penyelesaian suatu insiden. Resolusi dapat dilakukan oleh *service desk* sebagai pihak yang pertama menemukan insiden dari *user*, staf teknisi yang sedang mengerjakan kegiatan konfigurasi, maupun oleh *supplier* terhadap perangkat yang masih dalam garansi.

9. Penutupan (*Incident Closure*)

   Langkah penutupan adalah langkah yang dilakukan oleh *service desk* maupun staf teknisi terkait untuk memastikan apakah insiden telah benar selesai ditangani. Yang harus diperhatikan dalam langkah penutupan ini adalah dokumentasi proses penanganan insiden, perkiraan terhadap perulangan insiden, dan survei kepuasan *user* atas penanganan insiden.

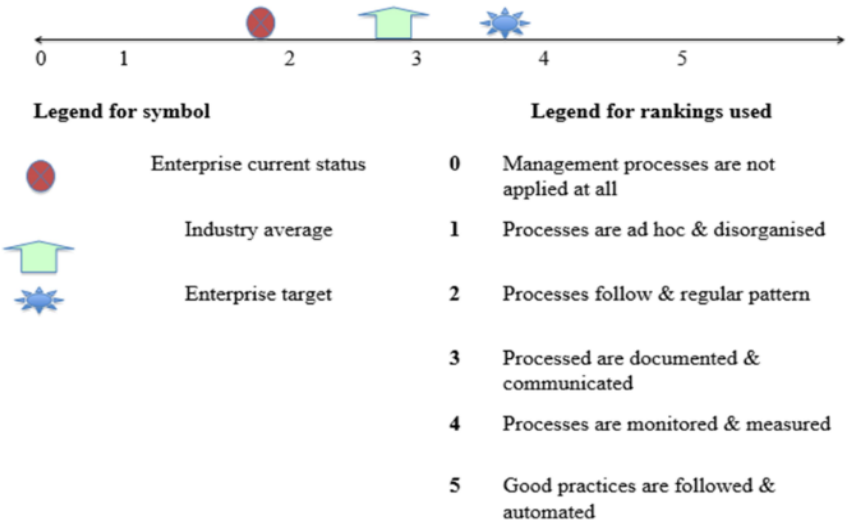
Dari kesembilan proses manajemen insiden tersebut dapat dilakukan pengukuran sejauh mana tingkat kematangan (*maturity level*) perusahaan dalam penerapannya. Pengukuran tingkat kematangan perusahaan dapat dilakukan menggunakan Model Kematangan (*Maturity Model*). Model Kematangan IT digunakan untuk membantu perusahaan memprioritaskan implementasi proses IT yang dianggap paling penting (J. Aguiar et al., 2018). Salah satu model kematangan yang paling banyak digunakan untuk pengukuran adalah Model Kematangan ITIL (ITIL *Maturity Model*).

2.4.9 Model Kematangan ITIL (ITIL *Maturity Model*)

Model kematangan (*maturity model*) adalah suatu metode untuk mengukur sejauh mana kapabilitas manajemen dalam suatu organisasi. Model kematangan berfokus pada evaluasi dan analisis semua elemen penting dalam upaya peningkatan dari proses yang belum matang ke proses yang disiplin, matang, dan efektif (Verdegay & Rodríguez, 2020). Model

kematangan ITIL bertujuan untuk membantu dan membimbing pengguna dalam penerapan *framework* ITIL. Perusahaan dapat menggunakan model kematangan untuk melakukan evaluasi terhadap metode dan proses yang berjalan pada perusahaan mereka sesuai dengan praktik manajemen yang baik (*good management practice*). Kematangan perusahaan ditunjukkan dengan penetapan tingkat maturitas tertentu (J. Aguiar et al., 2018). Peningkatan maturitas akan mengurangi risiko dan meningkatkan efisiensi, berkurangnya *error* dan meningkatkan kualitas proses, dan mendorong efisiensi biaya terkait dengan penggunaan sumber daya teknologi informasi (Chandra, 2018).

Model ini merupakan metode *scoring* yang memungkinkan organisasi untuk memberi peringkat (*ranking*) pada dirinya sendiri. Terdapat 6 peringkat pada model ini mulai dari 0 (*non-existent*) sampai dengan kematangan yang optimis atau 5 (*optimized*). Alat bantu pengukuran ini memungkinkan organisasi untuk menentukan posisi mereka saat ini (*as is*) dan posisi yang mereka inginkan (*to be*) serta memungkinkan organisasi untuk melakukan perbandingan dengan *best practice* dan panduan standar yang sudah ada.



Gambar 0.4 Representasi Maturity Model (UCISA, 2015)

Penilaian kematangan suatu perusahaan juga dapat dilihat dari faktor penentu kesuksesan (*Critical Success Factor*) yang telah ditetapkan pada perusahaan tersebut. Tingkat kematangan akan mencerminkan sejauh mana perusahaan tersebut telah menentukan kebijakan-kebijakan yang dapat menyukseskan target tersebut. Sejauh mana pencapaian target ini dapat diukur menggunakan indikator kinerja (*Key Performance Indicator*). *Framework* ITIL memberikan contoh beberapa CSF serta indikator untuk pengukuran kinerjanya.

2.4.10 *Critical Success Factor* (CSFs) dan *Key Performance Indicators* (KPIs)

Berikut adalah beberapa contoh *Critical Success Factors* beserta dengan *Key Performance Indicator*-nya dalam Manajemen insiden yang berdasarkan pada *framework* ITIL v3 pada Tabel 0.2 berikut :

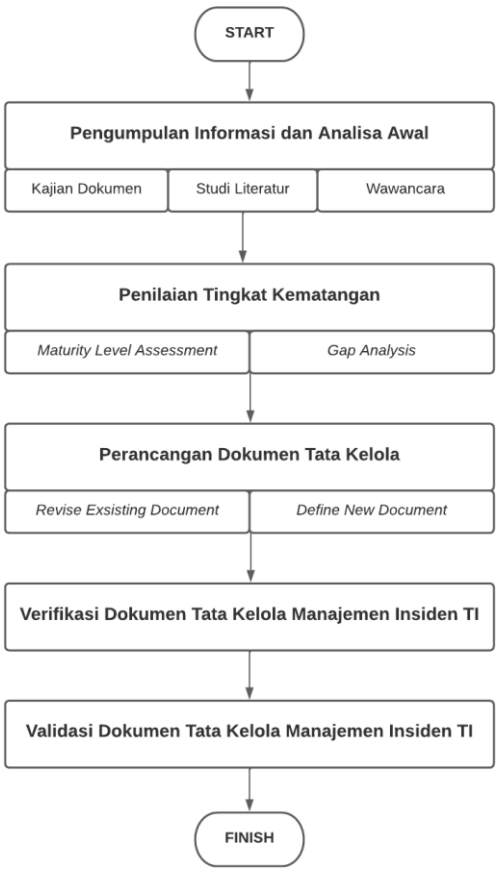
Tabel 0.2 CSF dan KPI ITIL v3

No	*Critical Success Factors*	*Key Performance Indicator*
1	Menyelesaikan insiden secepat mungkin dengan meminimalkan dampaknya terhadap bisnis	Waktu rata-rata yang dibutuhkan untuk mencapai resolusi insiden
		Perincian (*breakdown*) insiden pada setiap tahapan
		Persentase insiden yang dapat diselesaikan oleh *Help Desk* tanpa melakukan eskalasi ke tingkat yang lebih tinggi (*first point of contact*)
		Jumlah dan persentase insiden yang dapat diselesaikan secara *remote* atau tanpa melakukan kunjungan
		Jumlah insiden yang diselesaikan tanpa memberi dampak pada bisnis (mis. insiden dideteksi oleh *event management tools dan* diselesaikan sebelum dapat berdampak pada bisnis)
2	Memelihara kualitas layanan TI	Jumlah total Insiden
		Backlog insiden untuk setiap layanan TI
		Jumlah dan persentase insiden besar untuk setiap layanan TI
3	Menjaga kepuasan nasabah dengan layanan TI	Hasil skor rata-rata survei pengguna/nasabah (total dan berdasarkan kategori pertanyaan)
		Persentase survei kepuasan yang dijawab berbanding jumlah total survei kepuasan yang dikirim
4	Meningkatkan visibilitas dan komunikasi insiden kepada staf pendukung bisnis dan TI	Jumlah rata-rata pelaporan insiden melalui *Help Desk* atau kontak lain dari pengguna bisnis.
		Jumlah keluhan atau masalah pengguna bisnis tentang konten dan kualitas komunikasi insiden
5	Menyelaraskan aktivitas manajemen insiden dengan tujuan bisnis	Persentase insiden yang ditangani sesuai dengan waktu respons yang disepakati (target waktu respons insiden dapat ditentukan dalam SLA, misalnya, berdasarkan kode dampak dan urgensi)
		Biaya rata-rata per insiden
6	Memastikan bahwa metode dan prosedur standar digunakan untuk respons, analisis, dokumentasi, manajemen berkelanjutan dan pelaporan insiden yang efisien dan cepat untuk menjaga kepercayaan bisnis pada kapabilitas TI	Jumlah dan persentase insiden yang salah penugasan
		Jumlah dan persentase insiden yang salah dikategorikan
		Jumlah dan persentase insiden yang diproses per petugas *Help Desk*
		Jumlah dan persentase insiden yang terkait dengan perubahan dan rilis.

BAB 3
Metodologi

3.1 Langkah-langkah Penelitian

Metodologi penelitian adalah suatu metode yang digunakan yang menggambarkan langkah-langkah yang dijalani dalam sebuah penelitian ilmiah. Metodologi penelitian ini bertujuan untuk membuktikan hipotesis awal yaitu "Kondisi kekinian (*as is*) tata kelola manajemen insiden TI di Bank XYZ memerlukan perbaikan berdasarkan *framework* ITIL". Indikator yang menentukan tingkat kematangan Bank XYZ dalam penanganan insiden layanan TI adalah kapabilitas infrastruktur serta sumber daya manusia yang ada di perusahaan tersebut. Variabel yang berkaitan dengan indikator tersebut seperti kecepatan penyelesaian suatu insiden dan apakah dampak yang ditimbulkan dari insiden tersebut dapat diminimalkan. Gambar 0.1 menggambarkan tahapan-tahapan yang akan dilakukan pada penelitian ini :



Gambar 0.1 Tahapan Metode Penelitian

3.1.1 Pengumpulan Informasi dan Analisa Awal

Dilakukan pengumpulan informasi awal yang berkaitan dengan proses manajemen insiden TI yang sekarang sedang berjalan di bank XYZ. Proses analisis dilakukan terhadap seluruh pedoman formal manajemen insiden TI yang dimiliki saat ini. Melalui informasi yang didapat dari proses analisis, diharapkan dapat membantu dalam proses penelitian ke tahap selanjutnya. Adapun proses yang dilakukan adalah sebagai berikut :

A. Kajian Dokumen

Proses ini dilakukan untuk mengetahui lebih lanjut mengenai keadaan terkini (*as is*) pengelolaan insiden TI yang berjalan di Bank XYZ. Dokumen yang menjadi kajian dapat berupa dokumen kebijakan, Buku Pedoman Perusahaan (BPP), prosedur, berita acara, *Standard Operating Prochedure* (SOP), laporan tahunan dan lain-lain. Hal ini dilakukan untuk mendapatkan informasi mengenai pelaksanaan kebijakan dan prosedur tersebut, khususnya mengenai manajemen insiden TI.

B. Studi Literatur

Proses studi literatur dilakukan untuk mengumpulkan informasi mengenai kerangka kerja ITIL v3, khususnya pada proses *Incident Management* yang digunakan untuk mendukung penelitian ini. Studi literatur terkait penelitian sebelumnya yang relevan dengan penelitian ini dibahas pada sub-bab 2.1.

C. Wawancara

Proses wawancara dilakukan dengan tujuan untuk mendapatkan informasi yang lebih detail dari orang-orang yang terlibat secara langsung terhadap manajemen insiden di Bank XYZ. Hal ini bertujuan untuk mengetahui kondisi terkini di lapangan, sehingga didapatkan pemahaman mengenai keadaan *real* manajemen insiden TI yang berjalan sehari-hari. Beberapa pertanyaan yang diajukan untuk mendapatkan informasi awal proses manajemen insiden yang berjalan saat ini adalah :

Beberapa pertanyaan yang diajukan seperti :

- Apa saja dokumen prosedur yang berkaitan dengan proses manajemen insiden yang ada saat ini?
- Bagaimana komitmen manajemen terhadap layanan teknologi informasi secara keseluruhan?
- Berapa total insiden yang diterima *help desk* setiap bulannya?
- Berapa total insiden yang dapat diselesaikan *help desk* setiap bulannya?
- Berapa total *Backlog* insiden untuk setiap layanan TI?

- Berapa lama waktu rata-rata yang dibutuhkan untuk mencapai resolusi insiden?
- Berapa persentase insiden yang dapat diselesaikan oleh *help desk* tanpa melakukan eskalasi ke tingkat yang lebih tinggi (*first point of contact*)?
- Bagaimana hasil skor rata-rata survei kepuasan pengguna/nasabah?
- Berapa persentase survei kepuasan yang dijawab berbanding jumlah total survei kepuasan yang dikirim?
- Bagaimana kualitas komunikasi insiden dari kantor cabang ke kantor pusat?

3.1.2 Penilaian Tingkat Kematangan

Proses penilaian tingkat kematangan (*Maturity Level Assesment*) dilakukan terhadap tata kelola manajemen insiden menggunakan 2 buah kuesioner. Kuesioner pertama untuk mengukur tingkat kematangan penerapan tata kelola manajemen insiden TI yang berjalan saat ini (*as is*) dan kuesioner kedua menilai kondisi tata kelola manajemen insiden TI yang diharapkan di masa depan (*to be*). Responden yang terpilih adalah 20 karyawan-karyawati Bank XYZ yang bertanggung jawab terhadap keseluruhan layanan TI di seluruh area operasional Bank XYZ yaitu pegawai pada Divisi Teknologi Informasi (TSI).

Kuesioner yang digunakan berdasarkan pada UCISA *Self-Assesment Tools for Incident Management* (UCISA, 2015). Kuesioner terdiri dari 42 atribut kematangan yang mencangkup keseluruhan proses manajemen insiden sesuai dengan *best practice* ITIL v3 yang digunakan untuk menilai tingkat kematangan terkait penerapan manajemen insiden pada suatu organisasi. Kuesioner penilaian tingkat kematangan manajemen insiden pada penelitian ini dapat dilihat pada LAMPIRAN B.

Berdasarkan ITIL *Maturity Model* yang ada pada ITIL *Service Lifecycle* sesuai **Error! Reference source not found.**, penilaian tingkat kematangan dilakukan terhadap m odel *Service Operation,* khususnya pada domain *Incident Management.* Proses *Incident Management* tersebut mengandung 9 sub-proses yang dijabarkan dalam 42 atribut yang terbagi dalam 4 *Service Operation Area* yaitu "*The Incident Management Process", "Activities in Place Needed for the Success of Incident Management", "Incident Management Metrics",* dan *"Incident Management Process Interactions"*. Setiap atribut yang ada, terdapat indikator dan parameter dalam memberikan nilai kematangan dalam skala 0 sampai 5 yang dapat terlihat pada Tabel 0.1 berikut :

Tabel 0.1 Skala Tingkat Kematangan (Pratomo, 2016)

Maturity Level	**Keterangan**
0 - ***Absence***	Pada level ini, proses/fungsi tidak ada sama sekali pada operasional Bank.
1 - ***Initial***	Pada level ini, proses/fungsi yang ada bersifat *ad-hoc* atau tidak terorganisir atau tidak terdefinisikan pada Bank.
2 - ***Repeatable***	Pada level ini, proses/ungsi telah tersedia pada Bank, namun proses/fungsi hanya mengikuti pola-pola yang ada.
3 - ***Defined***	Pada level ini, proses/fungsi yang ada telah terkendali. Prosedur yang ada telah sesuai standar, terdokumentasi, dan diberikan melalui pelatihan oleh Bank.
4 - ***Managed***	Pada level ini, proses/fungsi telah sepenuhnya dikenali dan disetujui dalam proses TI yang ada.
5 - ***Optimized***	Pada level ini, proses/fungsi telah menjadi aktivitas rutin oleh Bank. Proses/fungsi telah terintegrasi secara otomatis dengan alur kerja Bank. Proses berkelanjutan dari pengembangan telah dilakukan oleh Bank.

Selain definisi yang dijabarkan di atas, ITIL *Maturity Model* juga memiliki beberapa karakteristik yang sudah terdefinisikan dengan rinci (AXELOS, 2013). Karakteristik ini diturunkan dari berbagai macam sumber termasuk juga dari atribut-atribut umum yang terkandung dalam ITIL *Maturity Model*. Tabel 0.2 berikut adalah karakteristik umum untuk memperjelas skala kematangan manajemen insiden:

Tabel 0.2 Karakteristik Tingkat Kematangan Manajemen Insiden

Maturity level		**Karakteristik**
0	***Absense (chaos)***	Proses/fungsi hanya terdapat sebagian atau bahkan tidak ada sama sekali
		Jika proses/fungsi hanya terdapat sebagian, hal ini dipastikan tidak memiliki struktur, tanggung jawab serta tidak konsisten dalam operasionalnya.
1	***Initial (reactive)***	Adanya sedikit komitmen dari manajemen
		Tidak terdapat tata kelola dari proses/fungsi
		Tidak adanya pro-aktivitas, bersifat reaktif.
		Aktivitas tidak terkoordinasi, sedikit atau bahkan tidak konsisten
		Hanya terdapat sedikit (jika ada) prosedur yang terdokumentasi
		Jalannya aktivitas bergantung pada siapa yang

		mengambilnya
		Sedikit atau bahkan tidak ada automasi dari aktivitas yang ada
		Sedikit (jika ada) catatan performa yang disimpan
		Tidak terdapat prosedur formal untuk proses pengembangan
		Orang yang menjalankan peran dari proses/fungsi, hanya mendapatkan sedikit pelatihan di luar dari yang telah dipelajarinya sendiri.
		Kinerja aktivitas tidak terukur
		Aktivitas bersifat teknis dibandingkan fokus pada pelanggan atau layanan
		Tidak adanya umpan balik (*feedback*) yang didapat dari pemangku kepentingan.
2	***Repeatable (active)***	Terdapat beberapa komitmen dari manajemen
		Aktivitas yang ada terdata
		Target dan tujuan terdefinisikan
		Ruang lingkup dari proses/fungsi telah didefinisikan dan disetujui
		Terdapat prosedur, namun tidak sepenuhnya terdokumentasi
		Prosedur biasanya diikuti, namun berbeda dari orang ke orang dan juga tim ke tim
		Orang yang melakukan aktivitas mempunyai kemampuan, pengalaman, kompetensi dan pengetahuan mengenai perannya
		Peran dapat dikenali, meskipun tidak didefinisikan secara formal
		Kinerja diukur dan dilaporkan, setidaknya ke lingkungan kecil internal
		Kinerja mulai lebih konsisten, tetapi terkadang masih sedikit tidak
		Beberapa proses automasi mulai digunakan untuk meningkatkan efisiensi
3	***Defined (proactive)***	Komitmen manajemen jelas
		Aktivitas tepat terdata, meskipun terkadang dan dalam kondisi yang tidak biasa, mungkin juga tidak memadai
		Mulai untuk fokus pada operasional secara proaktif, meskipun sebagian besar pekerjaan masih bersifat reaktif
		Dokumen penting dicatat dengan versi dan dalam pengendalian perubahan
		Ruang lingkup dari proses/fungsi didokumentasikan
		Prosedur dan instruksi kerja terdokumentasi dan diperbaharui
		Kinerja terukur dengan berbagai perhitungan
4	***Managed (pre-emptive)***	Proses/fungsi dan aktivitas terkait kuat dan jarang

		gagal dari yang telah direncanakan
		Kebanyakan aktivitas yang dapat diautomasi telah dilakukan automasi
		Dokumentasi dilindungi dari perubahan yang tidak diizinkan, dan disimpan secara terpusat
		Aktivitas dilakukan dengan tingkat konsistensi yang tinggi dengan sedikit pengecualian
		Definisi level otoritas dari masing-masing peran yang jelas dan terdokumentasi
		Proses-proses saling terintegrasi
		Fokus pada pelayanan dan pelanggan daripada hal-hal teknis
5	***Optimized***	Aktivitas dilakukan secara konsisten kepada seluruh area (lintas area) dari perusahaan
		Perencanaan menjadi dasar, baik dalam bisnis dan pelayanan
		Perencanaan dan aktivitas TI terintegrasi dengan perencanaan dan aktivitas bisnis perusahaan
		Proses, prosedur, dan fungsi secara berkelanjutan di audit untuk efisiensi dan efektivitas
		Redudansi prosedur dapat teridentifikasi dan dapat dihilangkan
		Kinerja data dan umpan balik dari lingkungan disimpan dan dianalisis untuk mendapatkan tren dan potensi pengembangan

3.1.3 Perancangan Saran Perbaikan Tata Kelola

Pada tahap ini, dilakukan perancangan *draft* tata kelola manajemen insiden TI. *Draft* ini dibuat berdasarkan hasil analisa pengukuran tingkat kematangan (*maturity level assesment*) tata kelola manajemen insiden TI di Bank XYZ. *Draft* ini memuat beberapa hal terkait proses manajemen Insiden TI, mulai dari Tujuan dan Objektif, Ruang Lingkup, Konsep, Prosedur, sampai dengan Matriks Pengukuran Kinerja.

Berdasarkan hasil analisa tingkat kematangan, jika ditemukan penilaian dengan angka yang rendah (kesenjangan kematangan yang tinggi), apabila diperlukan akan dirumuskan prosedur-prosedur baru terkait proses/fungsi tersebut. Namun jika tidak, maka akan dilakukan perbaikan terhadap tata kelola manajemen insiden TI yang sudah ada sesuai dengan *best practice* dari ITIL v3 dan akan disesuaikan dengan kebijakan-kebijakan TI yang berlaku pada Bank XYZ saat ini.

3.1.4 Validasi Saran Perbaikan Tata Kelola

Pada tahap ini, dilakukan proses validasi terhadap saran perbaikan yang telah dirancang. Saran perbaikan ini mencakup prosedur baru maupun perbaikan tata kelola manajemen insiden TI yang sudah ada sebelumnya. Proses validasi dilakukan untuk menentukan apakah *draft* rekomendasi perbaikan yang telah dirancang telah sesuai dengan keinginan dan sesuai dengan kebijakan yang ada di Bank XYZ.

Karakteristik perusahaan Bank XYZ adalah Bank Pembangunan Daerah (BPD), dimana pemegang sahamnya adalah gubernur dan kepala daerah di provinsi Nusa Tenggara Barat. Maka dari itu dapat dikatakan Bank XYZ adalah semi-kedinasan yang pengambilan keputusan untuk tiap-tiap unitnya berada di kepala unit tersebut (Febriananingsih, 2012). Divisi TSI pada Bank XYZ memiliki tugas dan tanggung jawab atas segala sesuatu yang berkaitan dengan penggunaan teknologi informasi, termasuk analisis usulan perubahan. Usulan tersebut akan disampaikan kepada pihak manajemen yaitu Direksi sebagai pemutus dan akhirnya akan ditetapkan peraturannya. Maka dari itu proses validasi kuesioner maupun rekomendasi tata kelola manajemen insiden ini dilakukan oleh *General Manager* Divisi TSI Bank XYZ.

3.1.5 Kesimpulan

Pada tahap ini, hasil penelitian mengenai Penerapan Framework ITIL v3 untuk Perbaikan Tata Kelola Manajemen Insiden TI di Bank XYZ disimpulkan dan dituangkan ke dalam laporan tertulis. Seluruh laporan akan memuat bagaimana kondisi tata kelola manajemen insiden TI di Bank XYZ saat ini, bagaimana keadaan ideal yang diinginkan di masa mendatang, serta bagaimana langkah-langkah yang diambil untuk mencapai tujuan tersebut. Selain itu laporan akan memberikan beberapa saran mengenai perancangan tata kelola manajemen insiden TI di bidang perbankan, khususnya dalam perbankan syariah.

BAB 4
Hasil dan Pembahasan

4.1 Pengumpulan Informasi dan Analisa

Proses pengumpulan informasi dan analisa awal telah dilakukan untuk mendukung perancangan tata kelola manajemen insiden TI di Bank XYZ. Beberapa proses yang sudah dilakukan adalah :

b. Kajian Dokumen

   Beberapa dokumen telah dikaji untuk mengetahui lebih lanjut mengenai keadaan terkini pengelolaan insiden TI yang terdapat pada Bank XYZ. Dokumen yang dikaji antara lain *Standard Operational Prochedure*, Buku Pedoman Perusahaan, peraturan Otoritas Jasa Keuangan, Peraturan Bank Indonesia, dan lain-lain. Hasil kesesuaian dokumen pendukung operasional dengan proses manajemen insiden TI di Bank XYZ dapat dilihat pada Tabel 0.1

c. Studi Literatur

   Proses studi literatur dilakukan untuk mendapatkan pemahaman yang lebih lanjut mengenai tata kelola manajemen insiden dan *framework* ITIL v3 guna mendukung penelitian yang akan dilakukan. Literatur yang dikaji antara lain berasal dari buku dan jurnal ilmiah. Gap antara penelitian sebelumnya dapat dilihat pada Tabel 0.1

d. Wawancara

   Proses wawancara telah dilakukan terhadap *stakeholder* insiden yang terlibat dalam proses manajemen insiden TI di Bank XYZ untuk memperoleh detail pelaksanaan dan masalah-masalah yang dapat muncul sehari-hari. Hasil proses wawancara dibahas pada sub-bab 4.2.

4.2 Proses Manajemen Insiden di Bank XYZ Saat Ini

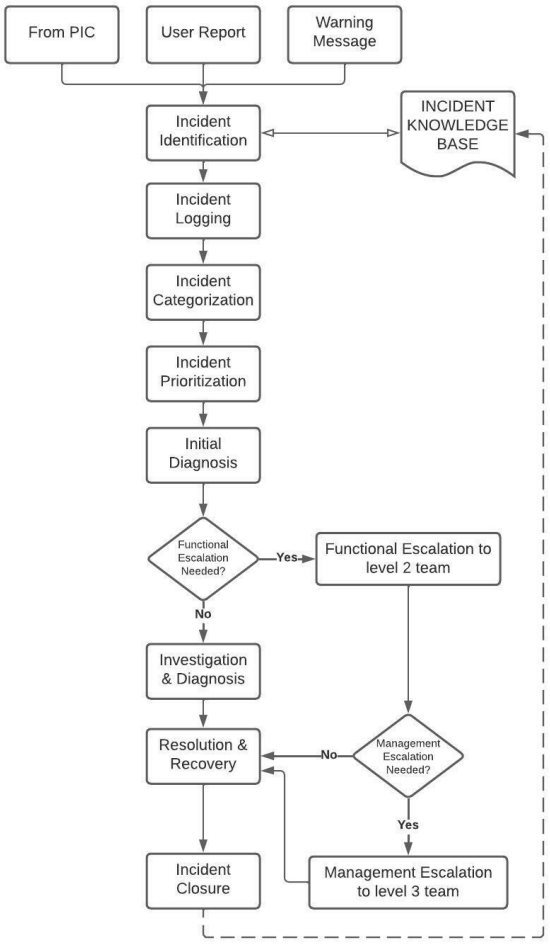
Demi mendapatkan gambaran jelas tentang proses manajemen insiden TI di Bank XYZ saat ini, dilakukan suatu proses wawancara kepada beberapa *stakeholder* insiden yang terlibat dalam keseluruhan proses manajemen insiden di Bank XYZ. Responden yang dipilih adalah beberapa pegawai di Kantor Cabang, salah satu *Branch Manager* kantor cabang, pegawai divisi TSI di Kantor Pusat, *Deputy General Manager* divisi TSI bagian operasional, sampai *General Manager* divisi TSI di Bank XYZ.

Berdasarkan hasil wawancara kami dapat lebih memahami bagaimana keadaan proses manajemen insiden yang berjalan saat ini, kemudian bagaimana keadaan ideal yang diinginkan di masa depan. Manajemen Insiden adalah sebuah instruksi formal yang sudah disiapkan bagi *staff help desk* untuk memproses penerimaan dan penanganan insiden TI, penyelesaian masalah, sampai pada akhirnya menutup laporan insiden tersebut (Beisse, 2015). Proses manajemen insiden yang dimiliki oleh Bank XYZ, khususnya divisi Teknologi Sistem Informasi (TSI), telah digunakan dalam operasional bank hingga saat ini. Sesuai dengan ketentuan penanganan insiden TI pada Standar Operasional dan Prosedur terkait Manajemen Teknologi Informasi Data Center Bank XYZ, Manajemen Insiden mengatur penerimaan terjadinya permasalahan IT termasuk penyelesaiannya atau eskalasi masalah tersebut ke pihak lain. Personil atau PIC (*Person in Charge*) yang bertugas dalam Manajemen Insiden adalah personil *Data Center* yang sedang bertugas ketika terjadinya permasalahan. PIC yang sedang bertugas dapat mengetahui jika salah satu komponen yang berada di dalam *Data Center* mengalami gangguan melalui :

a. Pemantauan secara langsung
b. *Warning message* pada perangkat atau *console* monitor
c. Informasi dari *user* atau nasabah melalui *call center* Bank XYZ

Jika ditemukan permasalahan, PIC harus mencoba menyelesaikan masalah tersebut, jika tidak dapat diselesaikan maka harus di eskalasikan kepada petugas terkait di PT Bank XYZ. Untuk menyampaikan permasalahan kepada petugas terkait, kepala operasional, dan pemimpin divisi TSI, maka PIC dapat menggunakan sarana SMS atau aplikasi WhatsApp dengan format yang sudah disepakati (ex. INFO PROBLEM *: System / Application / Network,* deskripsi, PIC, *Impact*, Waktu).

Untuk setiap masalah yang timbul dan yang membutuhkan penanganan oleh petugas terkait di Bank XYZ, maka segala aktivitas petugas yang berhubungan dengan penanganan masalah harus dicatat oleh personil *Data Center* dan dilaporkan pada berita acara serah terima *shift*. data/informasi yang dicatat meliputi : jenis masalah, petugas yang terlibat, jam petugas datang, jam masalah diatasi/dieskalasi/di-*pending*, dan keterangan yang dipandang perlu. Prosedur Manajemen Insiden yang berlaku di Bank XYZ saat ini dapat digambarkan pada Gambar 0.1 berikut :



Gambar 0.1 Prosedur Manajemen Insiden Bank XYZ saat ini

Setiap keluhan ataupun permasalahan terkait dengan TI, pengguna dapat menyampaikannya kepada petugas *Help Desk* melalui berbagai media komunikasi, seperti telepon, *fax*, email, SMS, serta lisan, maupun media lainnya. Sesuai dengan fungsinya, bahwa *Help Desk* adalah petugas utama yang menerima keluhan/permasalahan yang dialami pengguna, maka petugas *Help Desk* harus dibekali dengan pengetahuan tertentu sehingga dapat memberikan solusi untuk permasalahan sederhana.

Dalam hal permasalahan yang tidak dapat diselesaikan oleh petugas *help desk*, maka diteruskan (eskalasi) kepada petugas yang sesuai dengan bidang permasalahan. Dalam upaya peningkatan kinerja *help desk*, maka diperlukan adanya basis pengetahuan (*knowledge base*) yang berisi daftar permasalahan dan cara penyelesaiannya. *Database* ini harus senantiasa diperbaharui untuk permasalahan-permasalahan yang baru serta solusinya. Bentuk *database* ini bisa berupa *softcopy* maupun *hardcopy*. Prosedur pelaporan dan penanganan permasalahan adalah sebagai berikut :

1. Pelapor menyampaikan permasalahan kepada *Help Desk* melalui berbagai media komunikasi (telepon, *fax*, email, SMS, aplikasi *whatsapp*).
2. *Help Desk* mencatat keluhan pengguna dan identitas pelapor (nama, unit kerja, nomor telepon yang dapat dihubungi) di formulir OPS/017: Catatan Permasalahan.
3. *Help Desk* menindaklanjuti keluhan dengan memberikan solusi berdasarkan pengetahuan yang dimiliki dan *database* pengetahuan yang ada di *Help Desk*
4. Apabila permasalahan dapat teratasi, maka tiket ditutup. *Help Desk* mencatat cara penyelesaian permasalahan di formulir OPS/017: Catatan Permasalahan.
5. Apabila tidak dapat diselesaikan oleh *Help Desk*, maka dilakukan eskalasi permasalahan kepada unit yang terkait melalui media komunikasi maupun lisan. *Help Desk* membubuhkan catatan pada formulir OPS/017: Catatan Permasalahan bahwa permasalahan tersebut sedang dieskalasikan.
6. Berdasarkan laporan eskalasi permasalahan yang disampaikan oleh *Help Desk*, unit terkait melakukan analisis dan mencari solusi permasalahan. Dalam melakukan analisis, unit terkait dapat berkomunikasi langsung dengan pelapor untuk mendapatkan kejelasan terkait permasalahannya.
7. Jika permasalahan dapat terselesaikan, maka unit terkait menyampaikan kepada *Help Desk* tentang cara penyelesaiannya dan menutup tiket permasalahan.
8. Jika permasalahan tidak dapat terselesaikan, maka unit terkait menyampaikan kepada *Help Desk* agar permasalahan dapat dieskalasikan ke jenjang yang lebih tinggi.
9. *Help Desk* melaporkan permasalahan yang tidak dapat teratasi kepada kepala Operasional Data Center agar diteruskan ke pihak manajemen.
10. *Help Desk* memonitor penyelesaian permasalahan dan mencatat solusi atau statusnya pada formulir OPS/017: Catatan Permasalahan
11. *Help Desk* membuat laporan sekurang-kurangnya sebulan sekali tentang :
    - Jumlah laporan permasalahan yang diterima
    - Jumlah laporan permasalahan yang dapat diselesaikan berdasarkan *database* pengetahuan
    - Jumlah laporan permasalahan yang dieskalasi
    - Jumlah laporan permasalahan yang masih berstatus “Open”
    - Jumlah laporan permasalahan sesuai klasifikasi jenis permasalahan, yang terdiri dari APLIKASI, PERANGKAT KERAS, JARINGAN, DATA, dan SISTEM OPERASI.

- Permasalahan signifikan yang memerlukan perhatian pihak manajemen.

12. Kepala Operasional Data Center melakukan *review* sekurang-kurangnya seminggu sekali terhadap formulir OPS/017: Catatan Permasalahan untuk memantau status permasalahan dan untuk mengetahui adanya permasalahan yang membutuhkan penanganan lebih lanjut.

Proses identifikasi insiden hingga penutupan tiket tersebut termasuk dalam serangkaian proses Tata Kelola Teknologi Informasi yang berjalan di Bank XYZ.

4.3 Penilaian Tingkat Kematangan

4.3.1 Tinjauan Dokumen Pendukung Manajemen Insiden

Error! Reference source not found. merupakan rekap kesesuaian dokumen pendukung terkait proses manajemen insiden TI di Bank XYZ yang ada saat ini dengan proses-proses manajemen insiden pada ITIL v3 :

Tabel 0.1 Dokumen Pendukung Proses Manajemen Insiden

Assessment	**Dokumen Pendukung**	**Status**
Incident Management Process		
Tujuan, sasaran dan target dalam proses manajemen insiden	-	Tidak
Ruang lingkup dari proses manajemen insiden	-	Tidak
Nilai dari proses manajemen insiden terhadap bisnis	-	Tidak
Kebijakan, prinsip dan konsep-konsep dasar proses manajemen insiden	-	Tidak
Skala waktu telah ada dan disetujui untuk seluruh tahapan penanganan insiden	SOP Manajemen Teknologi Informasi Data Center - sub bab *Incident Management* DC	Ada
Adanya seorang manajer insiden / pemilik proses	SOP Manajemen Teknologi Informasi Data Center - sub bab *Incident Management* DC	Ada
Model dari insiden telah didefinisikan	BPP Manajemen Risiko Teknologi Informasi - sub bab BCP & DRP	Ada
Insiden besar telah	BPP Manajemen Risiko Teknologi Informasi - sub	Ada

didefinisikan	bab BCP & DRP	
Pengembangan prosedur penanganan insiden besar	SOP BCP & DRP Teknologi Informasi	Ada
Proses “Identifikasi Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Pencatatan Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Pengelompokan Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Prioritas Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Diagnosa Awal”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Eskalasi Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Identifikasi Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Investigasi dan Diagnosa”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Penyelesaian dan Pemulihan Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Proses “Penutupan Insiden”	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Pemicu, *input, output,* dan tampilan dari manajemen insiden	-	Tidak
Pelaporan informasi manajemen insiden	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Tantangan, faktor penentu kesuksesan dan risiko dari manajemen insiden	-	Tidak
Pencatatan insiden yang dilakukan sendiri (otomatis)	-	Tidak
Penelusuran insiden	-	Tidak
Kepemilikan insiden dapat dimengerti	-	Tidak
Data yang diinputkan telah dicek kelengkapannya	-	Tidak
Prosedur peninjauan manajemen insiden	-	Tidak

Activities in Place Needed for the Success of Incident Management		
Fungsi *service desk* telah didefinisikan	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Service desk mengetahui peranannya pada manajemen insiden di level 1	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Tim pada level 2 telah mengetahui peranannya dalam proses manajemen insiden	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Tim pada level 3 telah mengetahui peranannya dalam proses manajemen insiden	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Pihak *supplier* eksternal telah mengetahui peranannya pada manajemen insiden	SOP Manajemen Teknologi Informasi Data Center - hal. 9	Ada
Pengetahuan-pengetahuan dasar telah ada guna mendukung penyelesaian insiden pada *servicedesk*	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Solusi (sementara) penyelesaian insiden telah terdokumentasi dan menjadi bagian dari pengetahuan dasar	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Incident Management Metrics		
Terdapat KPI (*Key Performance Indicator*) dari proses manajemen insiden	-	Tidak
Laporan manajemen insiden telah didefinisikan	SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Ada
Metrik bagi insiden besar telah didefinisikan	SOP BCP & DRP Teknologi Informasi	Ada
Incident Management Process Interactions		
Panduan konfigurasi dan layanan aset yang ada mampu mendukung	-	Tidak

penyelesaian insiden		
Hubungan antara manajemen insiden dan manajemen masalah dapat dimengerti	-	Tidak
Terdapat prosedur pencarian akar permasalahan	-	Tidak
Manajer insiden / pemilik proses diperiksa sebagai bagian dari *Change Management* (tinjauan setelah implementasi)	BPP Manajemen Risiko Teknologi Informasi - hal. 15	Ada
Insiden yang berkaitan dengan peluncuran sebuah produk dilaporkan pada pihak *change/releasemanager*	-	Tidak

Berdasarkan tabel di atas, ditemukan beberapa prosedur manajemen insiden belum memiliki standar dan aturan yang terdokumentasi dalam SOP maupun peraturan tertulis lainnya. Prosedur/proses yang terdokumentasi dengan baik akan menghasilkan pemahaman yang seragam, artinya prosedur tersebut tidak *multi*-tafsir. Prosedur tersebut dijalankan oleh seluruh kantor cabang tanpa adanya perbedaan dari cabang yang satu dengan cabang lainnya. Hal ini juga akan memudahkan dalam proses transfer *knowledge*. Artinya ketika orang yang bertanggung jawab atas insiden manajemen berganti, orang berikutnya akan cepat memahami tanggung jawabnya sebagai PIC manajemen insiden dengan merujuk pada SOP. Maka dari itu prosedur insiden manajemen seharusnya mencangkup proses-prosesnya secara menyeluruh. Pembuatan rekomendasi prosedur-prosedur yang belum tercangkup dalam SOP Bank XYZ dapat merujuk pada *best practice* ITIL v3.

4.2.3 Analisis Tingkat Kematangan Saat Ini

Penentuan tingkat kematangan atau *maturity level* bukan hanya dapat menunjukkan sejauh mana Bank XYZ telah memenuhi standar dalam manajemen insiden TI yang baik. Lebih jauh lagi tingkat kedewasaan tersebut seharusnya dapat digunakan untuk peningkatan kesadaran proses manajemen insiden TI sekaligus mengidentifikasi proses mana yang menjadi prioritas dalam upaya perbaikan/peningkatan yang akan dilakukan. Tingkat kematangan yang dimaksud merupakan representasi kematangan atau kedewasaan proses

manajemen insiden yang berlangsung di Bank XYZ dalam bentuk nilai/angka. Penentuan tingkat kematangan dilakukan pada setiap proses manajemen insiden TI dan dilakukan melalui kuesioner dan wawancara terkait pelaksanaan manajemen insiden TI di Bank XYZ.

Berdasarkan hasil kuesioner yang dilakukan terkait manajemen insiden TI di Bank XYZ, analisis dilakukan untuk menilai tingkat kematangan tata kelola manajemen insiden TI untuk setiap domain UCISA *self-aseessment tool.* Proses penilaian manajemen insiden dilakukan dengan menggunakan 4 *Service Operation Area* yaitu (1) "*The Incident Management Process*", (2) "*Activities in Place Needed for the Success of Incident Management*", (3) "*Incident Management Metrics*", dan (4) "*Incident Management Process Interactions*". Keseluruhan proses manajemen insiden TI diwakilkan pada atribut-atribut yang terdapat pada masing-masing *service area*. Hasil kuesioner diperoleh dari penilaian beberapa *stakeholder* yang terlibat dalam manajemen insiden TI di Bank XYZ. Berikut adalah hasil kuesioner penilaian tingkat kematangan manajemen insiden TI saat ini:

a. *The Incident Management Process*

Tabel 0.2 Proses Manajemen Insiden Saat ini

1	We have defined Incident Management's Purpose, Goal, and Objective	**2.75**
2	We have defined Incident Management's Scope	**2.95**
3	We have defined Incident Management's Value to the business	**2.85**
4	We have defined Incident Management's Policies, Principles, and Basic Concepts	**2.75**
5	Timescales are agreed for all incident handling stages	**2.90**
6	Incident Manager/Process Owner is in place	**3.15**
7	Incident Models are defined	**3.25**
8	Major Incidents are defined	**3.10**
9	A Major Incident Procedure has been developed	**3.65**
10	The "Incident Identification" process activity is specified	**3.65**
11	The "Incident Logging" process activity is specified	**3.65**
12	The "Incident Categorization" process activity is specified	**3.60**
13	The "Incident Prioritization" process activity is specified	**3.70**
14	The "Initial Diagnosis" process activity is specified	**3.60**
15	The "Incident Escalation" process activity is specified	**3.65**
16	The "Incident Identification" process activity is specified	**3.65**
17	The "Investigation and Diagnosis" process activity is specified	**3.55**
18	The "Resolution and Recovery" process activity is specified	**3.60**

19	The "Incident Closure" process activity is specified	**3.75**
20	We have defined Incident Management's Triggers, Inputs, Outputs, and Interfaces	**2.15**
21	We have defined Incident Management's Information Management Reporting	**3.35**
22	We have defined Incident Management's Challenges, Critical Success Factors and Risk	**2.85**
23	Self-service Incident logging is in place	**2.55**
24	Incident Tracking is in place	**2.80**
25	Incident Ownership is understood and in place	**3.00**
26	Data entered into incidents at all stages is checked for completeness	**3.60**
27	Incident Management Process review procedure is in place	**3.05**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Proses Manajemen Insiden menghasilkan rata-rata di angka **3,23**.

b. *Activities in Place Needed for the Success of Incident Management*

Tabel 0.3 Aktivitas Manajemen Insiden Saat ini

28	The Service Desk function is defined	**3.75**
29	The Service Desk is aware of their role at Tier 1 / Level 1 Incident Management	**3.95**
30	Tier 2 / Level 2 teams are aware of their role in Incident Management	**3.15**
31	Tier 3 / Level 3 teams are aware of their role in Incident Management	**2.90**
32	External Suppliers are aware of their role in Incident Management	**2.50**
33	Knowledge Bases are in place to support Incident Resolution at the Service Desk	**3.60**
34	Workarounds are documented and in the Knowledge Base	**3.55**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Aktivitas Manajemen Insiden menghasilkan rata-rata di angka **3,34**.

c. *Incident Management Metrics*

Tabel 0.4 Matriks Manajemen Insiden Saat ini

35	Incident Management's KPIs and Metrics are defined and in place	**2.90**
36	Incident Management Reports have been identified and put in place	**3.55**
37	Metrics have been defined and are in place for Major Incidents	**3.75**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Matriks Manajemen Insiden menghasilkan rata-rata di angka **3,40**.

d. *Incident Management Process Interactions*

Tabel 0.5 Interaksi Proses Manajemen Insiden Saat ini

38	Service Asset and Configuration Management is in place and available to support Incident Resolution	**3.95**
39	The Relationship between Incident Management and Problem Management is understood	**3.10**
40	A Root-Cause Procedure is in place as Problem Management as a process does not exist yet	**3.30**
41	The Incident Manager / The Incident Process Owner is consulted as part of Change Management	**3.90**
42	Incidents Related to releases are reported to the Change / Release Manager	**3.55**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Interaksi Proses Manajemen Insiden menghasilkan rata-rata di angka **3,56**.

Berdasarkan 4 tabel di atas, dapat terlihat dari keempat *service area* yang telah dilakukan penilaian menggunakan kuesioner, terlihat bagian "proses manajemen insiden" memiliki nilai rata-rata terendah yaitu 3.23 dibandingkan dengan 3 *service area* yang lain. Kemudian diikuti "aktivitas yang dibutuhkan untuk menyukseskan manajemen insiden" dengan nilai 3.34, "pengukuran manajemen insiden" dengan nilai 3.40, serta yang memiliki nilai paling tinggi adalah "interaksi proses manajemen insiden" dengan nilai 3.56. Hal ini menunjukkan manajemen insiden TI di Bank XYZ sudah cukup baik dan hanya berselisih sedikit antar satu *service area* dengan yang lainnya. Meskipun dari keempat *service area* ini memiliki nilai rata-rata yang cukup baik, namun terlihat ada beberapa sub proses yang perlu dibenahi yang memiliki nilai di bawah rata-rata.

4.2.3 Analisis Tingkat Kematangan yang Diharapkan

Berdasarkan hasil kuesioner yang telah dilakukan, telah disepakati oleh manajemen bahwa tingkat kematangan manajemen insiden TI di Bank XYZ adalah pendapat dari seluruh *stakeholder* yang terlibat dalam manajemen insiden TI di Bank XYZ yang direpresentasikan dari hasil kuesioner. Tingkat kematangan yang diharapkan berdasarkan domain *maturity level* menurut UCISA *self-aseessment tool.* Selanjutnya pendapat dari seluruh responden untuk setiap poin pertanyaan akan diambil rata-ratanya sebagai tingkat kematangan yang diharapkan, dan divalidasi ulang dengan hasil kuesioner penilaian tingkat kematangan yang diharapkan oleh *General Manager* Divisi TSI Bank XYZ. Berikut adalah tabel perhitungan tingkat kematangan manajemen insiden TI yang diharapkan di Bank XYZ :

a. *The Incident Management Process*

Tabel 0.6 Proses Manajemen Insiden Yang Diharapkan

1	We have defined Incident Management's Purpose, Goal, and Objective	**3.85**
2	We have defined Incident Management's Scope	**3.90**
3	We have defined Incident Management's Value to the business	**3.75**
4	We have defined Incident Management's Policies, Principles, and Basic Concepts	**3.95**
5	Timescales are agreed for all incident handling stages	**3.35**
6	Incident Manager/Process Owner is in place	**3.40**
7	Incident Models are defined	**3.90**
8	Major Incidents are defined	**3.45**
9	A Major Incident Procedure has been developed	**4.10**
10	The "Incident Identification" process activity is specified	**4.40**
11	The "Incident Logging" process activity is specified	**4.40**
12	The "Incident Categorization" process activity is specified	**4.30**
13	The "Incident Prioritization" process activity is specified	**3.95**
14	The "Initial Diagnosis" process activity is specified	**4.15**
15	The "Incident Escalation" process activity is specified	**4.20**
16	The "Incident Identification" process activity is specified	**4.15**
17	The "Investigation and Diagnosis" process activity is specified	**4.30**
18	The "Resolution and Recovery" process activity is specified	**4.25**
19	The "Incident Closure" process activity is specified	**4.25**
20	We have defined Incident Management's Triggers, Inputs, Outputs, and Interfaces	**4.10**
21	We have defined Incident Management's Information Management Reporting	**4.15**
22	We have defined Incident Management's Challenges, Critical Success Factors and Risk	**4.25**
23	Self-service Incident logging is in place	**4.10**
24	Incident Tracking is in place	**3.45**
25	Incident Ownership is understood and in place	**3.40**
26	Data entered into incidents at all stages is checked for completeness	**4.25**
27	Incident Management Process review procedure is in place	**4.20**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Proses Manajemen Insiden menghasilkan rata-rata di angka **4,00**.

b. *Activities in Place Needed for the Success of Incident Management*

Tabel 0.7 Aktivitas Manajemen Insiden Yang Diharapkan

28	The Service Desk function is defined	**4.40**
29	The Service Desk is aware of their role at Tier 1 / Level 1 Incident Management	**4.20**
30	Tier 2 / Level 2 teams are aware of their role in Incident Management	**3.85**
31	Tier 3 / Level 3 teams are aware of their role in Incident Management	**4.00**
32	External Suppliers are aware of their role in Incident Management	**5.00**
33	Knowledge Bases are in place to support Incident Resolution at the Service Desk	**4.00**
34	Workarounds are documented and in the Knowledge Base	**4.40**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Aktivitas Manajemen Insiden menghasilkan rata-rata di angka **4,26**.

c. *Incident Management Metrics*

Tabel 0.8 Matriks Manajemen Insiden Yang Diharapkan

35	Incident Management's KPIs and Metrics are defined and in place	**3.90**
36	Incident Management Reports have been identified and put in place	**4.15**
37	Metrics have been defined and are in place for Major Incidents	**4.15**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Matriks Manajemen Insiden menghasilkan rata-rata di angka **4,07.**

d. *Incident Management Process Interactions*

Tabel 0.9 Interaksi Proses Manajemen Insiden Yang Diharapkan

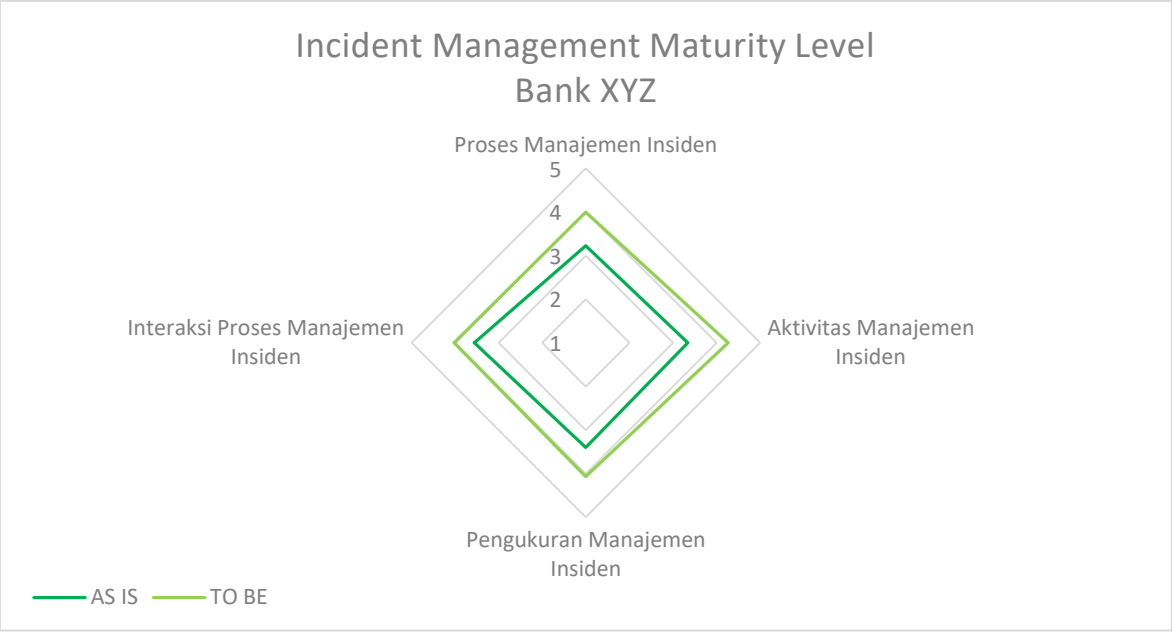
38	Service Asset and Configuration Management is in place and available to support Incident Resolution	**4.05**
39	The Relationship between Incident Management and Problem Management is understood	**4.00**
40	A Root-Cause Procedure is in place as Problem Management as a process does not exist yet	**3.90**
41	The Incident Manager / The Incident Process Owner is consulted as part of Change Management	**4.05**
42	Incidents Related to releases are reported to the Change / Release Manager	**4.10**

Berdasarkan penilaian keadaan manajemen insiden yang berjalan saat ini yang dilakukan *stakeholder* manajemen insiden TI di Bank XYZ, pada kategori Interaksi Proses Manajemen Insiden menghasilkan rata-rata di angka **4,02.**

Berdasarkan tabel di atas, dapat terlihat dari keempat *service area* yang telah dilakukan penilaian menggunakan kuesioner, hasilnya *stakeholder* manajemen insiden TI sepakat untuk memberikan nilai tingkat kematangan yang diharapkan dengan nilai di atas nilai 4 (*Managed and Measured* atau *pre-emptive*), dengan nilai untuk setiap domainnya adalah : "proses manajemen insiden" bernilai 4.00, "aktivitas yang dibutuhkan untuk menyukseskan manajemen insiden" bernilai 4.26, "pengukuran manajemen insiden" bernilai 4.07, serta "interaksi proses manajemen insiden bernilai" 4.02. Dari tabel di atas juga terlihat beberapa proses yang belum mencapai nilai yang diharapkan manajemen. Proses-proses ini yang perlu dibenahi dan dilakukan analisa prioritas untuk dapat dilakukan perbaikan demi meningkatkan layanan terutama layanan TI di Bank XYZ. Para *Stakeholder* sepakat bahwa proses manajemen insiden TI harus terdokumentasi dengan baik, serta dilakukan pengukuran sejauh mana efektivitasnya, dan dalam suatu kontrol kepatuhan terkait dengan peraturan yang ada. Sehingga komitmen manajemen terhadap proses manajemen insiden TI akan terlihat dengan jelas. Analisa kesenjangan untuk proses-proses yang belum tercapai akan dibahas pada sub-bab berikut :

4.2.4 Analisis Kesenjangan

Setelah dilakukan perhitungan tingkat kematangan manajemen insiden TI yang berjalan saat ini, serta telah ditentukan target nilai yang diperlukan untuk mencapai keadaan yang ideal yang diinginkan sesuai dengan kerangka kerja ITIL v3, selanjutnya dilakukan analisis kesenjangan antar keduanya. Analisis tingkat kesenjangan bertujuan untuk memberikan kemudahan perbaikan tata kelola manajemen insiden TI melalui atribut kematangan (Chandra, 2018). Dengan demikian dapat diketahui proses-proses mana saja yang memiliki kesenjangan tingkat kematangan dan membutuhkan perbaikan. Analisis kesenjangan dilakukan dengan membandingkan tingkat kematangan manajemen insiden TI yang berjalan saat ini (*as is*) dengan tingkat kematangan manajemen insiden TI yang diharapkan (*to be*). Dari perbandingkan tersebut akan diperoleh proses-proses mana saja yang belum sesuai dengan tingkat kematangan yang diinginkan. Sehingga dapat dilakukan perbaikan terhadap kekurangan yang ada. Analisis kesenjangan dapat dilihat pada Gambar 0.2 dan Tabel 0.10 berikut :



Gambar 0.2 Kesenjangan Tingkat Kematangan Manajemen Insiden pada Bank XYZ

Berdasarkan hasil rekap data kuesioner dan wawancara, secara umum manajemen insiden TI di Bank XYZ sudah cukup baik. Hal ini terlihat dari *maturity level* yang sudah mencapai angka 3 yaitu "*Defined*" atau "proactive". Artinya manajemen memiliki komitmen yang jelas terkait proses manajemen insiden TI di Bank XYZ yang dituangkan dan didokumentasikan dengan lengkap dalam bentuk *Standard Operating Procedure* (SOP) maupun Buku Panduan Perusahaan (BPP). Manajemen mulai memikirkan tindakan-tindakan proaktif dalam pencegahan dan penanggulangan insiden terkait teknologi informasi, meskipun pada praktiknya baik di kantor pusat maupun kantor cabang masih bersifat reaktif. Hal ini menimbulkan adanya waktu tunggu (*idle*) ketika insiden TI terjadi di kantor cabang, kemudian harus dilaporkan ke kantor pusat, sampai menunggu jawaban tindakan apa yang harus diambil.

Prosedur-prosedur yang ada sudah terstandarisasi dan dikomunikasikan melalui pelatihan. Namun sering kali pelatihan tersebut hanya melibatkan divisi TSI dan kantor pusat saja, jika ada perwakilan dari cabang hanya melibatkan kepala cabang (*Branch Manager*) atau perwakilannya saja. Dokumentasi sudah dilakukan secara *versioning* dalam ruang lingkup yang jelas, dan dalam suatu mekanisme pengendalian perubahan (*change control*). Artinya setiap revisi dari proses/fungsi dicatat mulai dari versi awal hingga yang terbaru. Terdapat mekanisme pengukuran kinerja berdasarkan metode tertentu.

Tabel 0.10 Rekap Kuesioner Kematangan Manajemen Insiden

No.	Atribut	*As Is*	*To Be*	STATUS
Proses Manajemen Insiden		**3.22**	**4.00**	
1	*We have defined Incident Management's Purpose, Goal, and Objective*	2.75	3.85	BELUM TERCAPAI
2	*We have defined Incident Management's Scope*	2.95	3.90	BELUM TERCAPAI
3	*We have defined Incident Management's Value to the bussiness*	2.85	3.75	BELUM TERCAPAI
4	*We have defined Incident Management's Policies, Principles, and Basic Concepts*	2.75	3.95	BELUM TERCAPAI
5	*Timescales are agreed for all incident handling stages*	2.90	3.35	TERCAPAI
6	*Incident Manager/Process Owner is in place*	3.15	3.40	TERCAPAI
7	*Incident Models are defined*	3.25	3.90	BELUM TERCAPAI
8	*Major Incidents are defined*	3.10	3.45	TERCAPAI
9	*A Major Incidenet Procedure has been developed*	3.65	4.10	TERCAPAI
10	*The "Incident Identification" process activity is specified*	3.65	4.40	TERCAPAI
11	*The "Incident Logging" process activity is specified*	3.65	4.40	TERCAPAI
12	*The "Incident Categorisation" process activity is specified*	3.60	4.30	TERCAPAI
13	*The "Incident Prioritisation" process activity is specified*	3.70	3.95	TERCAPAI
14	*The "Initial Diagnosis" process activity is specified*	3.60	4.15	TERCAPAI
15	*The "Incident Escalation" process activity is specified*	3.65	4.20	TERCAPAI
16	*The "Incident Identification" process activity is specified*	3.65	4.15	TERCAPAI
17	*The "Investigation and Diagnosis" process activity is specified*	3.55	4.30	TERCAPAI
18	*The "Resolution and Recovery" process activity is specified*	3.60	4.25	TERCAPAI
19	*The "Incident Closure" process activity is specified*	3.75	4.25	TERCAPAI
20	*We have defined Incident Management's Triggers, Inputs, Outputs, and Interfaces*	2.15	4.10	BELUM TERCAPAI
21	*We have defined Incident Management's Information Management Reporting*	3.35	4.15	BELUM TERCAPAI
22	*We have defined Incident Management's Challenges, Critical Success Factors and Risk*	2.85	4.25	BELUM TERCAPAI
23	*Self-service Incidenet logging is in place*	2.55	4.10	BELUM TERCAPAI
24	*Incident Tracking is in place*	2.80	3.45	TERCAPAI
25	*Incident Ownership is undestrood and in place*	3.00	3.40	TERCAPAI
26	*Data entered into incidents at all stages is checked for completeness*	3.60	4.25	TERCAPAI
27	*Incident Management Process review procedure is in place*	2.85	4.20	BELUM TERCAPAI
Aktivitas yang Dibutuhkan untuk Mensukseskan Manajemen Insiden		**3.34**	**4.26**	
28	*The Service Desk function is defined*	3.75	4.40	TERCAPAI
29	*The Service Desk is aware of their role at Tier 1 / Level 1 Incident Management*	3.95	4.20	TERCAPAI
30	*Tier 2 / Level 2 teams are aware of their role in Incident Management*	3.15	3.85	BELUM TERCAPAI
31	*Tier 3 / Level 3 teams are aware of their role in Incident Management*	2.90	4.00	BELUM TERCAPAI
32	*External Suppliers are aware of their role in Incidenet Management*	2.50	5.00	BELUM TERCAPAI
33	*Knowledge Bases are in place to support Incident Resolution at the Service Desk*	3.60	4.00	TERCAPAI
34	*Workarounds are documented and in the Knowledge Base*	3.55	4.40	TERCAPAI
Pengukuran Manajemen Insiden		**3.40**	**4.07**	
35	*Incident Management's KPIs and Metrics are defined and in place*	2.90	3.90	BELUM TERCAPAI
36	*Incident Management Reports have been identified and put in place*	3.55	4.15	TERCAPAI
37	*Metrics have been defined and are in place for Major Incidents*	3.75	4.15	TERCAPAI
Interaksi Proses Manajemen Insiden		**3.56**	**4.02**	
38	*Service Aset and Configuration Management is in place and available to support Incident Resolution*	3.95	4.05	TERCAPAI
39	*The Relationship between Incident Management and Problem Management is undestood*	3.10	4.00	BELUM TERCAPAI
40	*A Root-Cause Procedure is in place as Problem Management as a process does not exist yet*	3.30	3.90	BELUM TERCAPAI
41	*The Incident Manager / The Incident Process Owner is consulted as part of Change Management*	3.90	4.05	TERCAPAI
42	*Incidents Related to releases are reported to the Change / Release Manager*	3.55	4.10	TERCAPAI

Berdasarkan tabel di atas, terdapat 15 atribut manajemen insiden TI yang masih berada di bawah tingkat kematangan yang diharapkan manajemen. Dari 15 atribut yang belum memenuhi tingkat kematangan yang diharapkan, terdapat beberapa proses yang memiliki angka kematangan di atas nilai 3, hal ini menunjukkan proses tersebut sudah dapat dikatakan dijalankan dengan baik, namun manajemen beranggapan hal itu belum cukup. Hal ini dapat dilakukan analisis lebih lanjut mengapa manajemen beranggapan walaupun proses tersebut sudah memiliki nilai bagus, tetapi masih perlu diperbaiki. Prosedur dan aturan yang berkaitan dengan proses-proses ini perlu dilakukan pengkajian mengapa manajemen merasa proses ini belum mencapai target yang diharapkan, kemudian perlu dirumuskan langkah-langkah strategis untuk dapat mencapai tingkat kematangan yang diharapkan tersebut. Berikut adalah proses/fungsi yang belum memenuhi tingkat kematangan yang diharapkan :

1. *Incident Management's Purpose, Goal, and Objective*

   Permasalahan ini terkait dengan tujuan (*purpose*), sasaran (*goal*), dan target (*objective*) dari proses manajemen insiden tersebut. Seluruh insan Bank XYZ seharusnya menyadari pentingnya nilai (*value*) yang diberikan teknologi informasi terhadap bisnis bank serta pentingnya teknologi informasi dapat tersebut berjalan dengan lancar. Maka dari itu diperlukannya tata kelola teknologi informasi yang baik, khususnya yang berkaitan dengan Manajemen Insiden TI karena hal ini sangat berkaitan erat dengan ketersediaan layanan TI untuk mendukung operasional bank sehari-hari. Manajemen beranggapan belum tersedianya dokumen tertulis yang menjabarkan tujuan, sasaran, dan target manajemen insiden TI di Bank XYZ menjadi alasan belum terpenuhinya tingkat kematangan yang diharapkan.

2. *Incident Management's Scope*

   Ruang lingkup manajemen insiden TI mencangkup setiap peristiwa yang dapat mengganggu ketersediaan layanan TI, termasuk laporan dari pengguna baik melalui *Help Desk* maupun laporan dari perangkat deteksi otomatis.. Belum tersedianya dokumen tertulis yang menjabarkan seperti apa ruang lingkup, tugas dan tanggung jawab tiap-tiap PIC manajemen insiden TI menjadi salah satu faktor belum tercapainya tingkat kematangan yang diharapkan.

3. *Incident Management's Value to the bussiness*

   Manajemen berpendapat bahwa belum semua pegawai Bank XYZ memahami nilai/kontribusi teknologi informasi terhadap layanan perbankan. Sebagian besar pegawai Bank XYZ masih beranggapan bahwa teknologi informasi adalah alat pendukung (*supporting*) operasional perbankan. Hal ini menunjukkan perlu adanya perubahan pandangan (*paradigm shift*) bahwa teknologi informasi bukan lagi dipandang sebagai alat pendukung, melainkan sebagai inti perbankan (*core banking*). Manajemen mengharapkan seluruh pegawai Bank XYZ dapat memahami pentingnya ketersediaan layanan TI demi kelancaran kegiatan operasional perbankan sehari-hari.

4. *Incident Management's Policies, Principles, and Basic Concepts*

   Proses ini terkait dengan kebijakan-kebijakan pihak manajemen dalam penanganan insiden. Manajemen insiden seharusnya mencangkup seluruh kebijakan terkait fungsi *Help Desk* secara menyeluruh, prioritas dan eskalasi Insiden TI, penanganan dan jangka waktu (*timeframes*) penyelesaiannya, serta terkait pencatatan insiden (*incidentrecords*). Manajemen mengharapkan adanya dokumen pendukung yang menjabarkan konsep-konsep dasar manajemen insiden TI khususnya yang berdasarkan pada *framework* ITIL yang mencangkup model insiden, skala waktu (*timescales*), pelacakan status insiden, serta prosedur penanganan insiden besar (*Major Incidentsz).*

5. *Incident Models*

   Hasil pengukuran menunjukkan proses pelaporan manajemen insiden di Bank XYZ berada pada *maturity level* 3.25, artinya model insiden yang ada saat sudah cukup baik namun manajemen beranggapan model ini baru sebatas klasifikasi insiden berdasarkan jenisnya saja, serta belum tertuang dalam SOP/BPP yang sudah ada. Manajemen beranggapan dalam praktik manajemen insiden TI saat ini model insiden saat ini memang cukup baik dan mudah dipahami oleh PIC insiden. Namun ketika suatu saat terjadi perubahan PIC insiden, petugas baru akan sulit melakukan membedakan jenis insiden yang terjadi, yang menyebabkan penanganan insiden dapat tertunda. Model insiden tidak hanya mempermudah klasifikasi, namun juga harus menggambarkan langkah-langkah yang akan diambil untuk penanganannya. Model insiden terdiri dari : langkah-langkah penanganan, urutan kronologisnya, uraian tugas dan tanggung jawab setiap orang yang terlibat, skala waktu, prosedur eskalasi, dll.

6. *Incident Management's Triggers, Inputs, Outputs, and Interfaces*

   Keseluruhan proses manajemen Insiden TI diharapkan dapat dipahami oleh seluruh insan Bank XYZ, khususnya terkait *input* dan *output*-nya. *Input* manajemen insiden antara lain : informasi mengenai status sistem, komunikasi dan *feedback* mengenai insiden dan cara penanganannya, *feedback* dari nasabah terkait penanganan insiden dan tingkat kepuasan mereka. Sedangkan *output* dari manajemen insiden antara lain : insiden yang telah terselesaikan dan langkah-langkah penanganannya, pembaharuan *knowledge base* manajemen insiden, *feedback* kepuasan dari nasabah, dan lain-lain.

7. *Incident Management's Information Management Reporting*

   Hasil pengukuran menunjukkan proses pelaporan manajemen insiden di Bank XYZ berada pada *maturity level* 3.35, artinya proses ini sudah cukup baik namun manajemen beranggapan proses ini belum memenuhi tingkat kematangan yang mereka harapkan. Karakter perusahaan Bank XYZ yang merupakan bank umum sekaligus merupakan bank daerah menuntut adanya pelaporan yang komprehensif kepada pihak-pihak terkaitnya. Bukan hanya lembaga pengawas keuangan di Indonesia seperti OJK, BI, BPK, dan lain-lain tetapi Bank XYZ juga perlu melaporkan keadaan perusahaan mereka kepada *stakeholder* mereka yaitu kepala daerah dan gubernur. Maka dari itu manajemen beranggapan walaupun sudah mencapai level kematangan yang cukup baik, masih ada hal yang dapat ditingkatkan lagi dalam pelaporan mereka khususnya terkait ketersediaan layanan TI kepada pihak-pihak terkait tersebut. Pelaporan yang komprehensif menunjukkan bahwa Bank XYZ memahami dengan baik manfaat (*value*) dari teknologi informasi sekaligus mitigasi segala risikonya. Adanya dokumen pencatatan (*record*) insiden yang berdasarkan *framework* ITIL diharapkan manajemen dapat membantu administrasi pencatatan insiden yang lebih komprehensif. Menurut (Wardani et al., 2016) *framework* ITIL cocok diterapkan pada instansi pemerintahan yang bergerak di bidang pemberian layanan jasa, karena ITIL berfokus pada peningkatan efisiensi operasional teknologi informasi serta peningkatan standar kualitas layanan.

8. *Incident Management's Challenges, Critical Success Factors and Risk*

   Penerapan manajemen insiden tentunya memiliki tantangan dan risiko, terlebih lagi penerapan manajemen insiden yang berstandar pada *framework* ITIL. *Framework* ITIL

sudah menyediakan CSF yang dapat diadopsi dan diterapkan pada setiap organisasi tergantung kebutuhannya. Setiap organisasi harus mengembangkan KPI yang sesuai dengan tingkat kematangannya dan budaya organisasi tersebut. Pencapaian terhadap CSF harus dipantau dan digunakan untuk mengidentifikasi peluang perbaikan.

9. *Self-service Incidenet Logging*

   Manajemen berencana mengembangkan suatu mekanisme pencatatan insiden secara otomatis, yang diharapkan akan mempermudah proses penanganan insiden TI dan meminimalkan *downtime*, serta meningkatkan efisiensi PIC insiden.

10. *Tier 2 / Level 2 teams role in Incident Management*

    Hasil pengukuran menunjukkan proses pelaporan manajemen insiden di Bank XYZ berada pada *maturity level* 3.15, artinya proses ini sudah cukup baik namun manajemen beranggapan proses ini belum memenuhi tingkat kematangan yang mereka harapkan. Hasil penelitian (Pratomo, 2016) menunjukkan dengan metode pengukuran yang sama untuk studi kasus di salah satu bank BUMN bahwa mereka berada di *maturity level* 4 pada proses ini. Aritnya unsur pimpinan bank BUMN sudah memahami *value* teknologi informasi terhadap kelancaran kegiatan operasional mereka, serta sudah siap dalam penanganan insiden TI bila peran mereka diperlukan. Persaingan di dunia perbankan berpengaruh signifikan terhadap efisiensi dan stabilitas industri perbankan di Indonesia (Trinugroho et al., 2018). Penelitian menunjukkan bahwa bank syariah di Indonesia saat ini memiliki persaingan pasar yang lebih besar dari sebelumnya (Yildirim et al., 2021). Demi dapat bersaing dengan bank lain, manajemen Bank XYZ mengharapkan tidak hanya PIC insiden saja yang bertanggung jawab terhadap kelancaran sistem informasi dalam mendukung operasional bank, tetapi juga unsur pimpinan (*Branch Manager / General Manager*) terlibat aktif dalam pemantauannya. Unsur pimpinan juga harus menyadari pentingnya teknologi informasi dalam mendukung bisnis bank. Pimpinan juga minimal harus mengerti alur (*flow*) bagaimana teknologi informasi tersebut bekerja, sehingga dapat mengidentifikasi saat insiden terjadi dan memberikan saran tindakan yang harus diambil.

11. *Tier 3 / Level 3 teams role in Incident Management*

    Tidak hanya unsur pimpinan seperti *Branch Manager* dan *General Manager* yang harus memahami pentingnya teknologi informasi bagi bisnis bank, tetapi hal ini juga harus dipahami oleh unsur Eksekutif dalam organisasi . Sehingga mereka sebagai unsur pengambil keputusan dapat merumuskan dan mengembangkan tata kelola teknologi informasi yang baik sesuai kondisi organisasi saat ini, khususnya dalam hal ketersediaan layanan TI. Ketika unsur eksekutif sudah mengerti pentingnya teknologi informasi sebagai inti perbankan (*core banking*), maka teknologi informasi tidak akan dipandang sebagai hal beban pengeluaran (*cost*) melainkan sebagai investasi bagi pertumbuhan bank ke depannya.

12. *External Suppliers role in Incidenet Management*

    Kondisi saat ini di Bank XYZ, sistem informasi perbankan mereka masih menggunakan sistem dari pihak ketiga. Oleh karena itu manajemen mengharapkan komitmen penuh dari pihak vendor untuk membantu tersedianya layanan teknologi informasi setiap saat. Vendor juga perlu secara proaktif mengidentifikasi potensi-potensi terjadinya insiden TI, serta cepat tanggap terhadap laporan yang memerlukan campur tangan mereka sebagai pemegang sistem inti perbankan.

13. *Incident Management's KPIs and Metrics*

    Manajemen mengharapkan adanya metrik yang berdasarkan pada *framework* ITIL sebagai alat pengukuran sejauh mana tata kelola manajemen insiden TI berjalan. *Framework* ITIL v3 sudah menyediakan beberapa contoh metrik dengan masing-masing KPI-nya. Namun pemilihan KPI harus berdasarkan perimbangan yang matang. Perusahaan harus mengembangkan KPI sesuai dengan tingkat kematangan mereka.

14. *The Relationship between Incident Management and Problem Management*

    Hasil pengukuran menunjukkan proses pelaporan manajemen insiden di Bank XYZ berada pada *maturity level* 3.10, artinya berbedaan insiden (*incident*) dengan masalah (*problem*) dapat dibedakan dengan jelas. Namun manajemen beranggapan kedua hal ini masih menjadi satu kesatuan dalam praktiknya, khususnya pada manajemen masalah. Menurut *framework* ITIL Menurut definisi ITIL v3,manajemen insiden berkonsentrasi pada pemulihan layanan yang secara tidak terduga mengganggu (*disrupted*) pengguna

secepat mungkin, untuk meminimalkan dampak bisnis. Sedangkan Manajemen masalah melibatkan analisis akar penyebab permasalahan (*root cause analysis*) untuk menentukan dan menyelesaikan penyebab masalah yang mendasari insiden. Hal ini berhubungan erat dengan poin berikutnya, yaitu prosedur penelusuran akar penyebab masalah.

15. *A Root-Cause Procedure as Problem Management*

    Hasil pengukuran menunjukkan proses pelaporan manajemen insiden di Bank XYZ berada pada *maturity level* 3.30, namun manajemen beranggapan keadaan saat ini belum memenuhi keadaan ideal. Meskipun prosedur penelusuran akar permasalahan sudah termasuk dalam ranah Manajemen Masalah, tata kelola Manajemen Insiden TI juga harus mencangkup prosedur tersebut. Karena apabila akar permasalahan yang menyebabkan insiden sudah teridentifikasi, terlebih lagi sudah dihilangkan maka akan meminimalkan kemungkinan insiden yang sama akan terulang lagi.

Dari hasil data yang diperoleh dan dianalisis, menunjukkan bahwa sebagian besar struktur tata kelola manajemen insiden TI yang ada saat ini di Bank XYZ telah sesuai dengan kerangka kerja ITIL v3 yang diharapkan oleh pihak manajemen. Beberapa proses tata kelola manajemen insiden TI telah tersedia dan terdokumentasi dengan baik. Dari 15 proses yang belum memenuhi tingkat kematangan yang diharapkan, perlu dibuatkan usulan perbaikan tata kelola manajemen insiden TI sesuai dengan *best practice* ITIL v3 tentang Manajemen Insiden.

4.2.5 Kriteria Model Kematangan

Pengukuran model kematangan harus memiliki definisi kriteria yang dijabarkan secara kuantitatif. Selain itu perlu adanya validasi dari dokumen tata kelola yang sudah ada untuk membuktikan kebenaran hasil pengukuran tersebut. Hal ini bertujuan agar pengukuran yang akan dilakukan selanjutnya akan menghasilkan tingkat kematangan yang serupa dengan penelitian ini. Kriteria kuantitatif yang dibuat akan berdasarkan pada model kematangan ITIL v3 (AXELOS, 2013). Berikut ini akan kami rumuskan kriteria kuantitatif untuk model kematangan manajemen insiden TI berdasarkan ITIL v3 untuk tiap-tiap *service area*:

a) Proses Manajemen Insiden

Tabel 0.11 adalah penjabaran kriteria kuantitatif untuk model *service area "the incident management process"* :

Tabel 0.11 Kriteria Kematangan Proses Manajemen Insiden

The Incident Management Process	
Tingkat Kematangan	**Kriteria**
Level 0 *Absence* / *Chaos*	Proses atau fungsi sama sekali tidak ada dalam kegiatan operasional bank.
Level 1 *Initial / Reactive*	- Proses manajemen insiden masih bersifat reaktif. - Manajemen memiliki sedikit komitmen terhadap proses manajemen insiden. Manajemen belum mengerti nilai (*value*) proses manajemen insiden terhadap bisnis. - Proses manajemen insiden TI belum dirincikan dan didokumentasikan. Penanganan insiden TI masih bersifat sporadik. - Insiden besar (*major incident*) tidak terdefinisi. - Tidak ada prosedur *review*/audit insiden.
Level 2 *Repeatable / Active*	- Proses manajemen insiden masih bersifat aktif. - Sudah mulai terdapat komitmen dari manajemen terkait manajemen insiden. - Proses manajemen insiden TI mulai dirumuskan, dan disuarakan dalam forum-forum internal bank. - Telah dilakukan kategorisasi untuk insiden besar, namun masih ditangani dengan prosedur manajemen insiden secara keseluruhan. - Prosedur *review*/audit insiden telah dilakukan oleh internal *Help Desk/Service Desk*.
Level 3 *Defined / Proactive*	- Proses manajemen insiden masih bersifat proaktif. - Komitmen manajemen terhadap proses manajemen insiden jelas. Manajemen memiliki pandangan yang jelas terkait nilai manajemen insiden TI terhadap bisnis bank.

	- Proses manajemen insiden telah dirincikan dan didokumentasi, mulai dari proses identifikasi, pencatatan, kategorisasi, penentuan prioritas, diagnosa awal, eskalasi, investigasi, resolusi, sampai penutupan insiden TI. - Telah ditetapkan prosedur penanganan insiden besar yang terpisah dari prosedur insiden biasa. - Prosedur *review*/audit insiden dilakukan oleh unit terpisah, yaitu unit audit internal perusahaan, dilakukan setiap >1 tahun.
Level 4 *Managed / Pre-emptive*	- Proses manajemen insiden masih bersifat pre-emtif. - Komitmen manajemen tertuang dalam suatu *Service Level Agreement* (SLA) dan dengan matriks pengukuran yang jelas. - Proses manajemen insiden TI sudah dilakukan dengan konsistensi yang tinggi dan mengikuti SLA yang berlaku untuk tiap-tiap prosesnya. - Prosedur manajemen insiden besar sudah diterapkan secara formal beserta peran dan tanggung jawab masing-masing. - Prosedur *review*/audit insiden dilakukan per tahun dan pelaporannya langsung ditujukan kepada pimpinan perusahan.
Level 5 *Optimized*	- Proses manajemen insiden telah dilakukan secara konsisten di seluruh area perusahaan. - Komitmen manajemen mencangkup penerapan SLA proses manajemen insiden di seluruh unit kerja bank, tidak hanya pada unit *help desk*. Seluruh unit kerja memahami pentingnya nilai manajemen insiden terhadap bisnis. - Proses manajemen insiden sudah menerapkan standar-standar maupun praktik terbaik yang telah diterapkan perusahaan seluruh dunia dalam hal manajemen insiden TI yang sudah disesuaikan dengan karakteristik dan budaya perusahaan itu sendiri. - Prosedur insiden besar sudah mengikuti standar terbaru dan

	terbuka akan potensi pengembangan. - Prosedur *review*/audit insiden dilakukan secara berkala, mengikuti standar terbaru.
Validasi Dokumen Pendukung	
SOP Manajemen Teknologi Informasi Data Center - sub bab Incident Management DC	Bank XYZ sudah memiliki dokumen pendukung terkait proses manajemen insiden TI. Dalam dokumen ini sudah dijabarkan prosedur penanganan insiden mulai dari proses identifikasi, pencatatan, kategorisasi, penentuan prioritas, diagnosa awal, eskalasi, investigasi, resolusi, sampai penutupan insiden TI. Dokumen ini juga menjabarkan skala waktu bagi tiap-tiap proses tersebut, prosedur pelacakan insiden, serta peran dan tanggung jawab PIC insiden. Hasil kuesioner menunjukkan untuk proses manajemen insiden, Bank XYZ mendapat skor 3,22 artinya sudah berada pada level proaktif. Namun dokumen ini belum mencangkup hal-hal sekeliling penanganan insiden TI seperti definisi-definisi istilah, tujuan utama, sasaran, nilai bisnis, cakupan, *input*&*output* manajemen insiden TI. Maka dari itu dokumen ini perlu dilakukan penambahan yang berdasarkan pada ITIL v3.

b) Aktivitas Manajemen Insiden

Tabel 0.12 adalah penjabaran kriteria kuantitatif untuk model *service area "Activities in Place Needed for the Success of Incident Management"* :

Tabel 0.12 Kriteria Kematangan Aktivitas Manajemen Insiden

Activities in Place Needed for the Success of Incident Management	
Tingkat Kematangan	**Kriteria**
Level 0 *Absence* / *Chaos*	Proses atau fungsi sama sekali tidak ada dalam kegiatan operasional bank.
Level 1 *Initial / Reactive*	- Tidak terdapat suatu unit khusus yang menangani pelaporan dan penyelesaian insiden TI.

	- Tidak adanya prosedur eskalasi. Insiden hanya diselesaikan oleh orang yang menerima. Peran dan tanggung jawab terkait insiden TI tidak jelas. - Tidak adanya basis pengetahuan insiden (*incident knowledge base*).
Level 2 *Repeatable / Active*	- Sudah dibentuk suatu unit yang bertanggung jawab untuk menerima, melaporkan, melakukan eskalasi, serta menyelesaikan insiden TI bagi seluruh unit kerja bank. Unit ini disebut *Help Desk/Service Desk*. - Insiden TI hanya ditangani oleh *Help Desk/Service Desk* terkait penggunaan sistem, sementara penanganan insiden yang menyangkut *core banking* lebih banyak ditangani pihak ketiga (vendor). - Basis pengetahuan insiden sudah mulai didokumentasikan, namun tidak ada prosedur yang menjadi acuan sehingga pencatatan insiden berbeda dari satu petugas ke petugas yang lain.
Level 3 *Defined / Proactive*	- *Help Desk/Service Desk* sebagai *level/tier 1 incident team* telah memahami peran dan tanggung jawab mereka sebagai unit pertama yang bersentuhan (*first point of contact*) dengan insiden TI, termasuk cara penanganan awal insiden (*workaround*). - Sudah terdapat suatu prosedur eskalasi insiden. Vendor sudah mengerti peran dan tanggung jawabnya terkait insiden TI dan telah menetapkan SLA terkait sistem yang mereka kelola. - Basis pengetahuan insiden, meskipun bentuknya masih sederhana (contoh: *incident records*) telah digunakan sebagai dokumen pendukung *Help Desk/Service Desk* dalam upaya penyelesaian/resolusi insiden. begitu menerima laporan.
Level 4 *Managed / Pre-emptive*	- Tugas dan fungsi *Help Desk/Service Desk* sudah diformalkan dalam bentuk SOP.

	- Unsur supervisi (*level*/*tier* 2) sudah mengerti peran dan tanggung jawab mereka terkait eskalasi manajemen insiden TI dengan baik. Mereka sudah memahami pentingnya manajemen insiden terhadap operasional bank sehari-hari. - Aturan mengenai basis pengetahuan insiden sudah diformalkan dalam aturan tertulis, termasuk juga format alternatif solusi sementara (*workaround*).
Level 5 *Optimized*	- Terdapat metrik pengukuran terkait kinerja *Help Desk/Service Desk* termasuk waktu penyelesaian insiden, persentase penyelesaian insiden, waktu respon, hasil survei kepuasan, dan lain-lain. - Unsur pimpinan yaitu *Sub-Branch Manager, Branch Manager,* hingga *General Manager* (*level*/*tier* 3) sudah mengerti peran dan tanggung jawab mereka terkait eskalasi manajemen insiden TI dengan baik. Mereka sudah memahami nilai (*value*) manajemen insiden terhadap bisnis bank secara keseluruhan. - Basis pengetahuan terus dilakukan pembaharuan dan mengacu pada standar-standar praktik terbaik manajemen insiden TI yang terbarukan.
Validasi Dokumen Pendukung	
SOP Manajemen Teknologi Informasi Data Center - sub bab Penanganan Permasalahan Pengguna	Bank XYZ sudah memiliki dokumen yang menjelaskan peran dan tanggung jawab setiap PIC yang terlibat dalam penanganan insiden TI di perusahaan mereka. Dokumen ini sudah menjelaskan peran dan tanggung jawab Help Desk sebagai unit penanganan insiden TI. Dokumen juga telah menjelaskan prosedur pencatatan basis pengetahuan insiden beserta solusi sementaranya (*workaround*). Namun, dokumen ini belum menjelaskan peran dan tanggung jawab pihak lain selain *Help Desk,* seperti pejabat supervisi (*level 2*), pejabat pimpinan (*level 3*), serta peran dan tanggung jawab pihak ketiga dalam proses manajemen insiden TI di Bank XYZ.

c) Pengukuran Manajemen Insiden

Tabel 0.13 adalah penjabaran kriteria kuantitatif untuk model *service area "Incident Management Metrics"* :

Tabel 0.13 Kriteria Kematangan Pengukuran Manajemen Insiden

Incident Management Metrics	
Tingkat Kematangan	**Kriteria**
Level 0 *Absence* / *Chaos*	Proses atau fungsi sama sekali tidak ada dalam kegiatan operasional bank.
Level 1 *Initial / Reactive*	- Manajemen sudah mulai menyadari pentingnya suatu metrik pengukuran sejauh mana penerapan manajemen insiden yang berjalan saat ini. - Pelaporan manajemen insiden TI tidak didokumentasikan
Level 2 *Repeatable / Active*	- Gagasan/ide metrik pengukuran sudah mulai dirumuskan dalam forum internal bank. - Prosedur pelaporan manajemen insiden TI sudah mulai dirumuskan.
Level 3 *Defined / Proactive*	- Metrik pengukuran sudah dituangkan dalam suatu dokumen formal, meskipun masih dalam tahap rancangan awal, dan disosialisasikan melalui pelatihan formal bagi pegawai di seluruh area kerja bank. - Tahap awal rancangan format pelaporan manajemen insiden TI sudah dibuat namun hanya dikomunikasikan dengan unit terkait yaitu *Help Desk* dan *Call Center*.
Level 4 *Managed / Pre-emptive*	- Metrik pengukuran sudah diformalkan dalam bentuk SOP dan mencangkup *Key Performance Indicator* (KPI) serta *Critical Success Factor* (CSF) untuk setiap KPI tersebut. - Format pelaporan insiden TI baik melalui *Help Desk* atau *Call Center* sudah diformalkan dan diterapkan di seluruh unit kerja bank.
Level 5 *Optimized*	- Pencapaian KPI dan CSF selalu dilakukan pemantauan untuk mengidentifikasi peluang pengembangan. Metrik

	pengukuran dapat diterapkan pada insiden besar (*major incident*). - Pelaporan manajemen insiden telah memenuhi standar-standar maupun praktik terbaik layanan TI yang terkini, serta selalu terbuka dengan perbaikan di masa depan.
Validasi Dokumen Pendukung	
BPP Manajemen Risiko Teknologi Informasi	Dokumen terkait pengukuran/metrik kinerja manajemen insiden TI di Bank XYZ sudah didefinisikan. Dokumen ini menjelaskan SLA untuk penanganan insiden serta aturan mengenai pelaporan insiden kepada manajemen. Namun dokumen ini belum menjelaskan CSF serta KPI untuk masing-masing atributnya. Dokumen ini perlu disempurnakan dengan menambahkan CSF dan KPI yang berdasarkan pada ITIL v3, dengan tetap mempertimbangkan budaya perusahaan Bank XYZ sendiri.

d) Interaksi Proses Manajemen Insiden

Tabel 0.14 adalah penjabaran kriteria kuantitatif untuk model *service area "Incident Management Process Interactions"* :

Tabel 0.14 Kriteria Kematangan Interaksi Proses Manajemen Insiden

Incident Management Process Interactions	
Tingkat Kematangan	**Kriteria**
Level 0 *Absence* / *Chaos*	Proses atau fungsi sama sekali tidak ada dalam kegiatan operasional bank.
Level 1 *Initial / Reactive*	- Tidak adanya perbedaan antara manajemen insiden, manajemen masalah (*problem management*), dan pemenuhan permintaan (*request fulfilment*). Semua dikerjakan oleh help desk tanpa adanya pembeda klasifikasinya. - Tidak adanya manajer insiden (*incident manager*) dan manajer perubahan (*change manager*) yang terlibat dalam

	keseluruhan proses manajemen insiden TI.
Level 2 *Repeatable / Active*	- Manajemen sudah mulai menyadari pentingnya pembagian tugas dan wewenang untuk membedakan prosedur manajemen insiden, manajemen masalah, maupun pemenuhan permintaan. Sudah dirumuskan dokumen awal untuk setiap prosedur tersebut. - Usulan penunjukan manajer insiden dan manajer perubahan sudah mulai disuarakan pada forum-forum internal bank. Termasuk pendefinisian tugas dan tanggung jawab masing-masing.
Level 3 *Defined / Proactive*	- *Service Desk/Help Desk* memiliki prosedur terpisah bagi penanganan insiden, masalah, serta pemenuhan permintaan. Prosedur penelusuran akan permasalahan (*root-casuse procedure*) adalah prosedur yang termasuk dalam manajemen masalah TI. - Telah ditunjuk petugas yang bertanggung jawab terhadap penanganan insiden di seluruh unit kerja bank yang dinamakan manajer insiden. Manajer insiden terpisah dari manajer operasional.
Level 4 *Managed / Pre-emptive*	- Prosedur-prosedur *Service Desk/Help Desk* terkait pelaporan insiden maupun masalah dan permintaan sudah diformalkan dalam bentuk SOP dan memiliki SLA untuk masing-masing prosedur. - Telah ditunjuk petugas yang bertanggung jawab mengusulkan dan menjalankan segala bentuk perubahan sistem TI, termasuk manajemen insiden TI menjadi tugas dan tanggung jawabnya. Manajer perubahan senantiasa berkoordinasi dengan manajer insiden terkait proses manajemen insiden TI.
Level 5 *Optimized*	- Seluruh unit kerja bank memahami prosedur manajemen insiden, manajemen masalah, dan pemenuhan permintaan. Prosedur-prosedur tersebut telah memenuhi standar-standar praktik terbaik yang terbarukan.

	- Manajer insiden dan manajer perubahan senantiasa melakukan koordinasi dan berkomitmen tinggi terkait proses manajemen insiden TI. Pelatihan mengenai standar-standar terbaru terkait manajemen insiden tetap dilakukan untuk memperluas wawasan mereka.
Validasi Dokumen Pendukung	
SOP BCP & DRP Teknologi Informasi	Dokumen ini sudah menjelaskan tentang interaksi manajemen insiden TI dengan proses terkait ketersediaan layanan yang lainnya, termasuk menjelaskan aset terkait yang digunakan untuk penanganan insiden TI. Dokumen juga telah menjelaskan peran dan tanggung jawab manajer insiden serta manajer perubahan. Namun dalam dokumen ini hanya menjelaskan prosedur manajemen insiden secara keseluruhan, belum ada prosedur terpisah untuk menangani manajemen masalah (*problem management*) serta pemenuhan permintaan (*request fulfilment*).

4.2.6 Usulan Perbaikan Tata Kelola Manajemen Insiden TI

Berdasarkan hasil penilaian melalui wawancara dan kuesioner, dapat disimpulkan bahwa kondisi yang tidak terpenuhi, yaitu kesenjangan tingkat kematangan antara kondisi saat ini (*as is*) dengan kondisi yang diinginkan (*to be*) perlu dilakukan adanya usulan pembuatan *draft* tata kelola manajemen insiden TI yang sesuai dengan kerangka kerja ITIL v3. Diharapkan dengan adanya prosedur tertulis yang terdokumentasi dengan baik dan dikomunikasikan melalui pelatihan yang menyeluruh dapat meningkatkan kinerja layanan TI di Bank XYZ terutama pada layanan TI. Rekomendasi dokumen tata kelola manajemen insiden TI yang berdasarkan *framework* ITIL akan berisikan hal-hal sebagai berikut :

- BAB 1 : Proses Manajemen Insiden

  Bagian ini akan membahas definisi-definisi istilah, tujuan utama, sasaran, nilai bisnis, cakupan, *input&output* manajemen insiden TI.

- BAB 2 : Peran dan Tanggung Jawab

  Bagian ini akan membahas terkait peranan dan tanggung jawab bagi setiap personil *Help Desk, Person in Charge* (PIC) insiden, serta pihak ketiga (vendor).

- BAB 3 : Kategori, Target Waktu, Prioritas, dan Eskalasi Insiden

  Bagian ini akan membahas kategori insiden, penentuan prioritas, target waktu, *Critical Success Factor*, serta *Key Performance Indikator* Manajemen Insiden TI.

- BAB 4 : Alur Proses Manajemen Insiden Teknologi Informasi

  Bagian ini akan membahas alur proses manajemen insiden TI yang berdasarkan *framework* ITIL mulai dari identifikasi, pencatatan, kategorisasi, prioritas, diagnosa awal, eskalasi, investigasi, resolusi, sampai penutupan insiden TI.

- BAB 5 : Pelaporan Insiden

  Bagian ini akan membahas bagaimana prosedur dan format dasar dalam pelaporan insiden baik melalui *Help Desk* maupun melalui *Call Center*.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Telah dilakukan proses Penilaian Tingkat Kematangan (*Maturity Level Assesment*) berdasarkan *framework* ITIL v3 pada Manajemen Insiden yang diterapkan pada sektor perbankan, khususnya bank daerah. Proses penilaian yang telah dilakukan menghasilkan kesenjangan tingkat kematangan antara proses manajemen insiden yang berjalan saat ini (*as is*) dengan keadaan ideal yang diinginkan (*to be*). Hasil penilaian menunjukkan Bank XYZ sudah memenuhi sebagian besar proses tata kelola manajemen insiden pada *framework* ITIL v3 pada tingkat kematangan level 3 yaitu "*defined*/*proactive*". Sedangkan tingkat kematangan yang diharapkan manajemen berada pada level 4 yaitu "*managed*/*preemptive*". Hasil pengukuran menunjukkan terdapat 15 dari 42 proses manajemen insiden yang dianggap manajemen belum memenuhi harapan mereka. Dari 15 proses tersebut, dilakukan analisis dan penelusuran mengapa proses-proses ini belum memenuhi keadaan yang diinginkan, kemudian akan dibuatkan usulan tata kelola manajemen insiden TI yang berdasarkan pada *framework* ITIL v3 dengan harapan apabila proses-proses ini sudah mengikuti *best practice* ITIL akan mencapai keadaan ideal yang diinginkan manajemen.

Dewasa ini, teknologi informasi khususnya pada bidang layanan TI bukan lagi membahas/mempertanyakan tentang "apabila" layanan TI akan terganggu, melainkan tentang "kapan" hal itu akan terjadi. Tata kelola teknologi informasi yang baik, khususnya dalam hal Manajemen Insiden akan membantu organisasi membantu dalam menjawab pertanyaan : "apa" yang terjadi, "di mana" area yang terdampak, "siapa" saja yang memiliki tugas dan tanggung jawab terhadapnya, "mengapa" hal itu bisa terjadi, serta "bagaimana" cara meminimalkan dampak yang ditimbulkan serta menyelesaikan permasalahannya.

5.2 Saran

Saran pengembangan penelitian selanjutnya adalah pengembangan tata kelola manajemen layanan TI di bidang lainnya, seperti *Event Management*, *Problem Management*, *Request Fulfilment* yang menggunakan ITIL v3 sebagai *framework* acuan dalam pengembangannya, khususnya diterapkan dalam studi kasus di Perbankan Daerah.

Daftar Pustaka

Aguiar, J. F. F. (2017). *Maturity Model of Incident Management*. Instituto Universitario de Lisboa.

Aguiar, J., Pereira, R., Vasconcelos, J. B., & Bianchi, I. (2018). An overlapless incident management maturity model for multi-framework assessment (ITIL, COBIT, CMMI-SVC). *Interdisciplinary Journal of Information, Knowledge, and Management*, *13*, 137–163. https://doi.org/10.28945/4083

Alansari, Y., & Musleh Al-Sartawi, A. M. A. (2021). IT governance and E-banking in GCC listed banks. *Procedia Computer Science*, *183*, 844–848. https://doi.org/10.1016/j.procs.2021.03.008

Alshathry, O. (2016). Maturity Status of ITIL Incident Management Process among Saudi Arabian Organizations. *International Journal of Applied Science and Technology*, *6*(1), 40–46. http://www.ijastnet.com/journals/Vol_6_No_1_February_2016/7.pdf

Amorim, A. C., Mira da Silva, M., Pereira, R., & Gonçalves, M. (2021). Using agile methodologies for adopting COBIT. *Information Systems*, *101*, 101496. https://doi.org/10.1016/j.is.2020.101496

Arisenta, R., Suharjito, & Sukmandhani, A. A. (2020). Evaluation Model of Success Change Management in Banking Institution Based on ITIL V3 (Case Study). *2020 International Conference on Information Management and Technology*, 470–475. https://doi.org/10.1109/ICIMTech50083.2020.9211191.

AXELOS. (2013). *ITIL Maturity Model [White paper]*. *October*. https://www.axelos.com/getmedia/37940a44-addb-4c16-9e11-08d7773b07de/ITIL-Maturity-Model.aspx

Beisse, F. (2015). *A GUIDE TO COMPUTER USER & SUPPORT SPECIALISTS SIXTH EDITION*. Cengage Learning.

Chandra, A. (2018). *PENERAPAN TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 4-1 DENGAN MODEL MATURITY LEVEL STUDI KASUS DI PT . TELKOM WITEL YOGYAKARTA*. Universitas Islam Indonesia.

Chi, M., Zhao, J., George, J. F., Li, Y., & Zhai, S. (2017). The influence of inter-firm IT governance strategies on relational performance: The moderation effect of information technology ambidexterity. *International Journal of Information*

Management, *37*(2), 43–53. https://doi.org/10.1016/j.ijinfomgt.2016.11.007

De Barros, M. D., Salles, C. A. L., Gomes, C. F. S., Da Silva, R. A., & Costa, H. G. (2015). Mapping of the scientific production on the ITIL application published in the national and international literature. *Procedia Computer Science*, *55*, 102–111. https://doi.org/10.1016/j.procs.2015.07.013

Febriananingsih, N. (2012). Keterbukaan Informasi Publik Dalam Pemerintahan Terbuka Menuju Tata Pemerintahan Yang Baik. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *1*(1), 135. https://doi.org/10.33331/rechtsvinding.v1i1.110

Fukuyama, F. (2013). What is Governance? *SSRN Electronic Journal*, *January 2013*. https://doi.org/10.2139/ssrn.2226592

Gangopadhyay, P., & Nilakantan, R. (2021). Peer effects and social learning in banks' investments in information technology. *International Review of Economics and Finance*, *75*(April), 456–463. https://doi.org/10.1016/j.iref.2021.03.024

Gërvalla, M., Preniqi, N., & Kopacek, P. (2018). IT infrastructure library (ITIL) framework approach to IT governance. *IFAC-PapersOnLine*, *51*(30), 181–185. https://doi.org/10.1016/j.ifacol.2018.11.283

Haryanti, T., & Pribadi, A. (2019). E-commerce service design readiness using ITIL framework with IT balanced scorecard objective (Case Study: University e-Commerce). *Procedia Computer Science*, *161*, 283–290. https://doi.org/10.1016/j.procs.2019.11.125

Lucio-Nieto, T., Colomo-Palacios, R., Soto-Acosta, P., Popa, S., & Amescua-Seco, A. (2012). Implementing an IT service information management framework: The case of COTEMAR. *International Journal of Information Management*, *32*(6), 589–594. https://doi.org/10.1016/j.ijinfomgt.2012.08.004

Marrone, M., & Kolbe, L. M. (2011a). Impact of IT Service Management Frameworks on the IT Organization. *Business & Information Systems Engineering*, *3*(1), 5–18. https://doi.org/10.1007/s12599-010-0141-5

Marrone, M., & Kolbe, L. M. (2011b). Uncovering ITIL claims: IT executives' perception on benefits and Business-IT alignment. *Information Systems and E-Business Management*, *9*(3), 363–380. https://doi.org/10.1007/s10257-010-0131-7

Naim, A. B., Wibawa, A. S., Yude, A. K., Akbar, B. K., Rahmadani, V. S., Shihab, M. R., & Ranti, B. (2021). Changes in IT governance and its impact on organizational business process: Case study at Indonesia Supreme Audit Institution (BPK). *Procedia*

Computer Science, *197*(2021), 734–742. https://doi.org/10.1016/j.procs.2021.12.195

Orta, E., Ruiz, M., Hurtado, N., & Gawn, D. (2014). Decision-making in IT service management: A simulation based approach. *Decision Support Systems*, *66*, 36–51. https://doi.org/10.1016/j.dss.2014.06.002

Palilingan, V. R., & Batmetan, J. R. (2018). Incident Management in Academic Information System using ITIL Framework. *IOP Conference Series: Materials Science and Engineering*, *306*(1), 0–9. https://doi.org/10.1088/1757-899X/306/1/012110

Pratomo, V. B. (2016). *PERANCANGAN TATA KELOLA MANAJEMEN INSIDEN TI BERDASARKAN KERANGKA KERJA ITIL 2011 (STUDI KASUS PADA PT. BANK ABC)*. INSTITUT TEKNOLOGI SEPULUH NOPEMBER.

Rizun, N., Revina, A., & Meister, V. G. (2021). Analyzing content of tasks in Business Process Management. Blending task execution and organization perspectives. *Computers in Industry*, *130*, 103463. https://doi.org/10.1016/j.compind.2021.103463

Ruiz, M., Moreno, J., Dorronsoro, B., & Rodriguez, D. (2018). Using simulation-based optimization in the context of IT service management change process. *Decision Support Systems*, *112*(June), 35–47. https://doi.org/10.1016/j.dss.2018.06.004

Samopa, F., Astuti, H. M., & Lestari, M. A. (2017). The Development of Work Instruction as a Solution to Handle IT Critical Incidents in Units within an Organization. *Procedia Computer Science*, *124*, 593–600. https://doi.org/10.1016/j.procs.2017.12.194

Selig, G. J. (2008). *Implementing IT Governance - A Pocket Guide: Vol. First edit*. Van Haren Publishing. http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=1557996&amp%0Alang=pt-pt&site=eds-live&authtype=sso

Silitonga, T. P., & Ali, A. H. N. (2010). SISTEM MANAJEMEN INSIDEN PADA PROGRAM MANAJEMEN HELPDESK DAN DUKUNGAN TI BERDASARKAN FRAMEWORK ITIL V3 (STUDI KASUS PADA BIRO TEKNOLOGI INFORMASI BPK-RI). *Seminar Nasional Informatika 2010 (SemnasIF 2010)*, *2010*(semnasIF), 210–218.

Tadesse, B., & Bakala, F. (2021). Effects of automated teller machine service on client satisfaction in Commercial Bank of Ethiopia. *Heliyon*, *7*(3), e06405. https://doi.org/10.1016/j.heliyon.2021.e06405

The Stationery Office, G. B. (2011). *ITIL Service Operation*. http://books.google.com/books?id=w382YAAACAAJ&pgis=1

Trinugroho, I., Risfandy, T., & Ariefianto, M. D. (2018). Competition, diversification, and bank margins: Evidence from Indonesian Islamic rural banks. *Borsa Istanbul Review*, *18*(4), 349–358. https://doi.org/10.1016/j.bir.2018.07.006

UCISA. (2015). *ITIL – Introducing service operation*. 1–20.

Verdegay, J. L., & Rodríguez, Z. (2020). A new decision support system for knowledge management in archaeological activities". *Knowledge-Based Systems*, *187*, 104843. https://doi.org/10.1016/j.knosys.2019.07.014

Wardani, L. A. K., Murahartawaty, & Ramadani, L. (2016). Perancangan Tata Kelola Layanan Teknologi Informasi Menggunakan ITIL versi 3 Domain Service Transition Dan Service Operation Di Pemerintah Kota Bandung. *Journal of Information Systems Engineering and Business Intelligence*, *2*(2), 81. https://doi.org/10.20473/jisebi.2.2.81-87

Widianto, A., & Subriadi, A. P. (2021). IT service management evaluation method based on content, context, and process approach: A literature review. *Procedia Computer Science*, *197*(2021), 410–419. https://doi.org/10.1016/j.procs.2021.12.157

Yamamoto, S. (2017). A Continuous Approach to Improve IT Management. *Procedia Computer Science*, *121*, 27–35. https://doi.org/10.1016/j.procs.2017.11.005

Yandri, R., Suharjito, Utama, D. N., & Zahra, A. (2019). Evaluation model for the implementation of information technology service management using fuzzy ITIL. *Procedia Computer Science*, *157*, 290–297. https://doi.org/10.1016/j.procs.2019.08.169

Yildirim, C., Kasman, A., & Hamid, F. S. (2021). Impact of foreign ownership on market power: Do regional banks behave differently in ASEAN countries? *Economic Modelling*, *105*(September), 105654. https://doi.org/10.1016/j.econmod.2021.105654

LAMPIRAN A

Lampiran A. Latar Belakang Kuesioner Penilaian Proses Manajemen Insiden

LATAR BELAKANG KUESIONER PENELITIAN

Penerapan teknologi informasi membawa perubahan positif dalam kegiatan operasional bank khususnya pada pengelolaan data bank sehingga dapat dilakukan dengan lebih efisien dan efektif serta menghasilkan informasi yang lebih cepat dan akurat. Layanan TI pada perbankan merupakan suatu hal yang sangat krusial karena layanan TI dituntut untuk selalu beroperasi dengan baik setiap saat. Mengingat bahwa teknologi informasi merupakan aset penting dalam operasional dan dapat meningkatkan nilai tambah dan daya saing bank, sementara dalam penyelenggaraannya mengandung berbagai risiko, maka bank perlu menerapkan tata kelola teknologi informasi (IT *Governance*). Bank harus menjamin bahwa kinerja layanan TI dapat berjalan dengan maksimal dan juga mampu melakukan pengelolaan dan pencegahan setiap insiden yang muncul guna mendukung keberlangsungan proses bisnis perusahaan.

Berdasarkan hal tersebut dapat disimpulkan sebagai berikut :

- **INSIDEN** adalah sebuah interupsi atau pengurangan kualitas layanan TI. Suatu kesalahan konfigurasi pada sistem juga dapat dianggap sebagai insiden walaupun belum menimbulkan masalah yang berarti pada sistem tersebut.

- **MANAJEMEN INSIDEN** adalah serangkaian proses yang dilakukan untuk menyelesaikan suatu insiden, mulai dari pelaporan hingga penutupan insiden.
  1. **Tujuan (*Purpose*) :** Mengembalikan kondisi layanan TI ke keadaan normal.
  2. **Sasaran (*Goals*) :** Meminimalkan dampak yang ditimbulkan insiden dan mencegah terulangnya insiden yang sama.
  3. **Target (*Objective*) :** Memastikan terdapat prosedur standar dalam penanganan insiden yang efisien dan cepat. Menyelaraskan aktivitas dan prioritas manajemen insiden dengan tujuan bisnis. Meningkatkan kepuasan nasabah terhadap kualitas layanan TI.
  4. **Ruang Lingkup (*Scope*) :** Mencangkup setiap peristiwa yang dapat mengganggu suatu layanan. Termasuk laporan dari pengguna baik melalui *Help Desk* maupun laporan dari perangkat deteksi otomatis.

- **Nilai (*Value*) Terhadap Bisnis :** manajemen insiden dapat memberikan nilai tambah bagi perusahaan dengan cara :
  1. Mengurangi pekerjaan yang tidak direncanakan (*unplanned labour)* dan biaya yang disebabkan oleh insiden.
  2. Meningkatkan ketersediaan layanan dengan cara mengurangi waktu henti (*downtime*) yang dibutuhkan untuk mendeteksi dan menyelesaikan suatu insiden.
  3. Penyelarasan aktivitas TI dengan prioritas bisnis secara *real-time* dengan cara mengidentifikasi prioritas bisnis dan secara dinamis mengalokasikan sumber daya yang diperlukan.
  4. Mengidentifikasi potensi peningkatan layanan.

- **Model Insiden** dapat mencakup beberapa hal berikut :
  1. Tahapan-tahapan yang harus dilakukan.
  2. Urutan kronologis bagaimana tahapan-tahapan tersebut dilakukan
  3. Uraian Tanggung jawab setiap orang yang terlibat
  4. Tindakan pencegahan yang dilakukan sebelum penyelesaian insiden (contoh : *backup data*)

5. Skala waktu (*timescales*) untuk penyelesaian tindakan
6. Prosedur eskalasi

- **Insiden Besar :** suatu insiden yang memerlukan prosedur yang terpisah, skala waktu yang lebih pendek, serta urgensi yang lebih penting**.**

Berikut adalah beberapa contoh **Critical Success Factors** berserta dengan **Key Performance Indicator**-nya dalam Manajemen insiden yang berdasarkan pada framework ITIL v3 :

No.	Critical Success Factors	Key Performance Indicator
1	Menyelesaikan insiden secepat mungkin dengan meminimalkan dampaknya terhadap bisnis	Waktu rata-rata yang dibutuhkan untuk mencapai resolusi insiden
		Perincian (*breakdown*) insiden pada setiap tahapan
		Persentase insiden yang dapat diselesaikan oleh *Help Desk* tanpa melakukan eskalasi ke tingkat yang lebih tinggi (*first point of contact*)
		Jumlah dan persentase insiden yang dapat diselesaikan secara *remote* atau tanpa melakukan kunjungan
		Jumlah insiden yang diselesaikan tanpa memberi dampak pada bisnis (mis. insiden dideteksi oleh *event management tools dan* diselesaikan sebelum dapat berdampak pada bisnis)
2	Memelihara kualitas layanan TI	Jumlah total Insiden
		Backlog insiden untuk setiap layanan TI
		Jumlah dan persentase insiden besar untuk setiap layanan TI
3	Menjaga kepuasan nasabah dengan layanan TI	Hasil skor rata-rata survei pengguna/nasabah (total dan berdasarkan kategori pertanyaan)
		Persentase survei kepuasan yang dijawab berbanding jumlah total survei kepuasan yang dikirim
4	Meningkatkan visibilitas dan komunikasi insiden kepada staf pendukung bisnis dan TI	Jumlah rata-rata pelaporan insiden melalui Help Desk atau kontak lain dari pengguna bisnis.
		Jumlah keluhan atau masalah pengguna bisnis tentang konten dan kualitas komunikasi insiden
5	Menyelaraskan aktivitas manajemen insiden dengan tujuan bisnis	Persentase insiden yang ditangani sesuai dengan waktu respons yang disepakati (target waktu respons insiden dapat ditentukan dalam SLA, misalnya, berdasarkan kode dampak dan urgensi)
		Biaya rata-rata per insiden
6	Memastikan bahwa metode dan prosedur standar digunakan untuk respons, analisis, dokumentasi, manajemen berkelanjutan dan pelaporan insiden yang efisien dan cepat untuk menjaga kepercayaan bisnis pada kapabilitas TI	Jumlah dan persentase insiden yang salah penugasan
		Jumlah dan persentase insiden yang salah dikategorikan
		Jumlah dan persentase insiden yang diproses per petugas Help Desk
		Jumlah dan persentase insiden yang terkait dengan perubahan dan rilis.

LAMPIRAN B

Lampiran B. Form Kuesioner Penilaian Proses Manajemen Insiden

Assalamualaikum Warahmatullahi Wabarakatuh

Bapak/Ibu partisipan yang terhormat,

Dengan segala kerendahan hati, peneliti memahami terkait kesibukan Bapak/Ibu partisipan. Bersama ini izinkan peneliti memohon bantuan Bapak/Ibu agar dapat memberikan masukan terhadap kuesioner berikut yang bertujuan untuk menilai tingkat kematangan Tata Kelola Manajemen Insiden TI di Bank XYZ yang sedang berjalan saat ini, serta keadaan ideal yang Bapak/Ibu harapkan.

Berikut tabel keterangan Indikator Tingkat Kematangan Manajemen Insiden TI :

Maturity Level	**Keterangan**
0 - *Absence*	Pada level ini, proses/fungsi tidak ada sama sekali pada operasional Bank.
1 - *Initial*	Pada level ini, proses/fungsi yang ada bersifat *ad-hoc* atau tidak terorganisir atau tidak terdefinisikan pada Bank.
2 - *Repeatable*	Pada level ini, proses/fungsi telah tersedia pada Bank, namun proses/fungsi hanya mengikuti pola-pola yang ada.
3 - *Defined*	Pada level ini, proses/fungsi yang ada telah terkendali. Prosedur yang ada telah sesuai standar, terdokumentasi, dan diberikan melalui pelatihan oleh Bank.
4 - *Managed*	Pada level ini, proses/fungsi telah sepenuhnya dikenali dan disetujui dalam proses TI yang ada.
5 - *Optimized*	Pada level ini, proses/fungsi telah menjadi aktivitas rutin oleh Bank. Proses/fungsi telah terintegrasi secara otomatis dengan alur kerja Bank. Proses berkelanjutan dari pengembangan telah dilakukan.

KUESIONER PENILAIAN MANAJEMEN INSIDEN TEKNOLOGI INFORMASI													
No	**Pernyataan**	**Keadaan Saat Ini**						**Keadaan yang Diharapkan**					
		0	**1**	**2**	**3**	**4**	**5**	**0**	**1**	**2**	**3**	**4**	**5**
Proses Manajemen Insiden													
1	Kami telah menerapkan Tujuan, Sasaran dan Target dalam proses Manajemen Insiden *We have defined Incident Management's Purpose, Goal, and Objective*												
2	Kami telah menetapkan Ruang Lingkup dari proses Manajemen Insiden *We have defined Incident Management's Scope*												
3	Kami telah menetapkan nilai dari proses Manajemen Insiden terhadap bisnis												

	We have defined Incident Management's Value to the bussiness												
4	Kami telah menetapkan kebijakan, prinsip dan konsep-konsep dasar dari proses Manajemen Insiden												
	We have defined Incident Management's Policies, Principles, and Basic Concepts												
5	Kami telah memiliki skala waktu untuk setiap tahapan penyelesaian insiden												
	Timescales are agreed for all incident handling stages												
6	Kami telah memiliki seorang Manajer Insiden (PIC)												
	Incident Manager/Process Owner is in place												
7	Kami telah mendefinisikan Model insiden												
	Incident Models are defined												
8	Kami telah mendefinisikan Insiden Besar												
	Major Incidents are defined												
9	Kami telah mengembangkan suatu prosedur untuk penanganan Insiden Besar												
	A Major Incidenet Procedure has been developed												
10	Kami telah menentukan aktivitas dalam proses "Identifikasi Insiden"												
	The "Incident Identification" process activity is specified												
11	Kami telah menentukan aktivitas dalam proses "Pecatatan Insiden"												
	The "Incident Logging" process activity is specified												
12	Kami telah melakukan aktivitas dalam proses "Pengelompokan Insiden"												
	The "Incident Categorisation" process activity is specified												
13	Kami telah melakukan aktivitas dalam proses "Prioritas Insiden"												
	The "Incident Prioritisation" process activity is specified												
14	Kami telah melakukan aktivitas dalam proses "Diagnosa Awal Insiden"												
	The "Initial Diagnosis" process activity is specified												
15	Kami telah melakukan aktivitas dalam proses "Eskalasi Insiden"												
	The "Incident Escalation" process activity is specified												
16	Kami telah melakukan aktivitas dalam proses "Identifikasi Insiden"												
	The "Incident Identification" process activity is specified												
17	Kami telah melakukan aktivitas dalam proses "Investigasi dan Diagnosa Insiden"												
	The "Investigation and Diagnosis" process activity is specified												
18	Kami telah melakukan aktivitas dalam proses "Penyelesaian dan Pemulihan Insiden"												
	The "Resolution And Recovery" process activity is specified												
19	Kami telah melakukan aktivitas dalam proses "Penutupan Insiden"												

	The "Incident Closure" process activity is specified												
20	Kami telah menetapkan pemicu, input, output, dan tampilan dari Manajemen Insiden												
	We have defined Incident Management's Triggers, Inputs, Outputs, and Interfaces												
21	Kami telah menetapkan informasi pelaporan dari proses manajemen insiden												
	we have defined Incident Management's Information Management Reporting												
22	Kami telah menetapkan tantangan manajemen, faktor penentu kesuksesan dan risiko dari manajemen insiden												
	We have defined Incident Management's Challenges, Critical Success Factors and Risk												
23	Kami telah memiliki Sistem Pencatatan Insiden Otomatis												
	Self-service Incidenet logging is in place												
24	Kami telah memiliki prosedur penelusuran insiden												
	Incident Tracking is in place												
25	Kami telah mengerti dan menerapkan konsep Kepemilikan Insiden												
	Incident Ownership is undestrood and in place												
26	Data yang diinputkan pada seluruh tahapan insiden telah diperiksa kelengkapannya												
	Data entered into incidents at all stages is checked for completeness												
27	Kami telah melakukan peninjauan terhadap prosedur Manajemen Insiden yang ada												
	Incident Management Process review procedure is in place												
Aktivitas yang Dibutuhkan untuk Menyukseskan Manajemen Inside													
28	Kami telah menetapkan fungsi dari "Service Desk/Help Desk"												
	The Service Desk function is defined												
29	Help Desk mengetahui perannya pada Manajemen Insiden di Tier/Level 1												
	The Service Desk is aware of their role at Tier 1 / Level 1 Incident Management												
30	Help Desk mengetahui perannya pada Manajemen Insiden di Tier/Level 2												
	Tier 2 / Level 2 teams are aware of their role in Incident Management												
31	Help Desk mengetahui perannya pada Manajemen Insiden di Tier/Level 3												
	Tier 3 / Level 3 teams are aware of their role in Incident Management												
32	Pihak supplier eksternal telah mengetahui peran mereka pada manajemen insiden di perusahaan kami												

	External Suppliers are aware of their role in Incidenet Management												
33	Kami telah memiliki basis pengetahuan dasar untuk mendukung penyelesaian insiden pada Help Desk												
	Knowledge Bases are in place to support Incident Resolution at the Service Desk												
34	Kami telah memiliki basis pengetahuan untuk alternatif solusi (sementara) penyelesaian insiden												
	Workarounds are documented and in the Knowledge Base												
Matriks Manajemen Insiden													
35	Kami telah menentukan KPI (Key Performance Indicator) dari proses manajemen insiden												
	Incident Management's KPIs and Metrics are defined and in place												
36	Kami telah melakukan identifikasi dan pelaporan manajemen insiden												
	Incident Management Reports have been identified and put in place												
37	Kami telah menentukan metrik untuk Manajemen Insiden Besar (Major)												
	Metrics have been defined and are in place for Major Incidents												
Interaksi Proses Manajemen Insiden													
38	Kami telah memiliki Manajemen konfigurasi dan layanan aset yang mampu mendukung penyelesaian insiden												
	Service Aset and Configuration Management is in place and available to support Incident Resolution												
39	Kami telah mengerti tentang hubungan Manajemen Insiden degan Manajemen Masalah												
	The Relationship between Incident Management and Problem Management is undestood												
40	Kami telah memiliki prosedur penelusuran akar permasalahan untuk permasalahan yang belum pernah muncul												
	A Root-Cause Procedure is in place as Problem Management as a process does not exist yet												
41	Kami telah melakukan pemeriksaan (audit) terhadap Manajer Insiden												
	The Incident Manager / The Incident Process Owner is consulted as part of Change Management (Post Implementation Review)												
42	Kami telah melaporkan insiden terkait peluncuran produk baru kepada Manajer Perubahan												
	Incidents Related to releases are reported to the Change / Release Manager												

LAMPIRAN C

Draft Saran Perbaikan
Manajemen Insiden Teknologi Informasi
Bank XYZ

Saleh Firdausi
18917223

Nomor Dokumen	: BPP/BXYZ/TI/000/V1.0/2022
Tanggal	: 12 April 2022
Versi Dokumen	: v 1.00*

**Draft ini masih dalam proses pengembangan dan memerlukan pengembangan lebih lanjut*

BAB 1

Proses Manajemen Insiden

1.1 Definisi Istilah Manajemen Insiden

- **Tata Kelola :**

  Dalam perspektif umum, tata kelola (*governance*) adalah kemampuan pemerintah (*goverment*) untuk membuat aturan dan menegakkannya, serta untuk pemberian layanan kepada masyarakatnya, terlepas pemerintah tersebut apakah demokratis ataupun tidak.

- **Tata Kelola Teknologi Informasi :**

  Tata kelola TI adalah sekumpulan aturan yang mencangkup mulai dari manajemen, perencanaan, kebijakan penilaian kinerja, proses dan penerapan; hal-hal yang terkait dengan hak keputusan, kewenangan, kendali, dan ukuran kinerja terhadap investasi, perencanaan, anggaran belanja, komitmen, layanan, perubahan besar, keamanan, privasi, keberlangsungan bisnis agar sesuai dengan hukum dan kebijakan organisasi

  Struktur tata kelola TI menjelaskan tentang berbagai hak dan tanggung jawab serta aturan dan prosedur dalam pengambilan keputusan yang terkait TI. Tata kelola TI yang ada pada suatu organisasi disesuaikan dengan kebutuhan organisasi tersebut. Pengembangan tata kelola TI di berbagai organisasi, terdapat berbagai kerangka kerja (*framework*) yang dapat digunakan sebagai acuan dalam pembuatannya. Beberapa contoh diantaranya adalah : COBIT 5, ITIL v3 2011 *Edition*, ISO/IEC 38500:2008, ISO 17799 / ISO 27000 *Series*, ISO/IEC 20000, CMMI/SPICE (ISO/IEC 15504), *Balanced Scorecard*, dan AS 8015-2005.

- **Insiden :**

  Adalah sebuah interupsi atau pengurangan kualitas layanan TI. Suatu kesalahan konfigurasi pada sistem juga dapat dianggap sebagai insiden walaupun belum menimbulkan masalah yang berarti pada sistem tersebut.

- **Manajemen Insiden :**

  Adalah serangkaian proses yang dilakukan untuk menyelesaikan suatu insiden, mulai dari

pelaporan hingga penutupan insiden.

- **Major Incident**

  Insiden besar adalah suatu insiden yang memerlukan prosedur yang terpisah, skala waktu yang lebih pendek, serta urgensi yang lebih penting**.**

- **Model Insiden**

  Dapat mencakup beberapa hal berikut :

  1. Tahapan-tahapan yang harus dilakukan.
  2. Urutan kronologis bagaimana tahapan-tahapan tersebut dilakukan
  3. Uraian Tanggung jawab setiap orang yang terlibat
  4. Tindakan pencegahan yang dilakukan sebelum penyelesaian insiden (contoh : *backup data*)
  5. Skala waktu (*timescales*) untuk penyelesaian tindakan
  6. Prosedur eskalasi

1.2 Tujuan Utama Manajemen Insiden

Tujuan utama (*Purpose*) dari manajemen insiden teknologi informasi adalah Mengembalikan kondisi layanan TI ke keadaan normal secepat mungkin.

1.3 Sasaran Manajemen Insiden

Sasaran (*Goals*) manajemen insiden teknologi informasi adalah meminimalkan dampak yang ditimbulkan insiden dan mencegah terulangnya insiden yang sama.

1.4 Target Manajemen Insiden

Target (*Objective*) manajemen insiden adalah memastikan terdapat prosedur standar dalam penanganan insiden yang efisien dan cepat. Menyelaraskan aktivitas dan prioritas manajemen insiden dengan tujuan bisnis. Meningkatkan kepuasan nasabah terhadap kualitas layanan TI.

1.5 Nilai Bisnis Manajemen Insiden

Manajemen insiden dapat memberikan nilai tambah bagi perusahaan dengan cara :

1. Mengurangi pekerjaan yang tidak direncanakan (unplanned labour) dan biaya yang disebabkan oleh insiden.
2. Meningkatkan ketersediaan layanan dengan cara mengurangi waktu henti (downtime) yang dibutuhkan untuk mendeteksi dan menyelesaikan suatu insiden.
3. Penyelarasan aktivitas TI dengan prioritas bisnis secara real-time dengan cara mengidentifikasi prioritas bisnis dan secara dinamis mengalokasikan sumber daya yang diperlukan.
4. Mengidentifikasi potensi peningkatan layanan.

1.6 Cakupan Manajemen Insiden

Mencangkup setiap peristiwa yang dapat mengganggu suatu layanan. Termasuk laporan dari pengguna baik melalui *Help Desk* maupun laporan dari perangkat deteksi otomatis.

1.7 Input & Output Manajemen Insiden

- *Input* manajemen insiden antara lain :
  informasi mengenai status sistem, komunikasi dan *feedback* mengenai insiden dan cara penanganannya, *feedback* dari nasabah terkait penanganan insiden dan tingkat kepuasan mereka.
- Sedangkan *output* dari manajemen insiden antara lain : insiden yang telah terselesaikan dan langkah-langkah penanganannya, pembaharuan *knowledge base* manajemen insiden, *feedback* kepuasan dari nasabah, dan lain-lain.

BAB 2

Peran dan Tanggung Jawab

2.1 Help Desk

Help Desk bertanggung jawab atas pelaporan insiden yang terjadi di divisi GSIT. Help Desk merupakan first level support / tier-1 dalam penanganan insiden. Berikut ini tugas dan tanggung jawab yang dimiliki:

5. Single Point of Contact untuk penanganan masalah yang berhubungan dengan komputerisasi baik di Data Center maupun di Cabang atau unit kerja Kantor Pusat.
6. Melakukan pencatatan setiap call yang masuk yang berhubungan dengan insiden yang terjadi.
7. Melakukan determinasi dan bertindak sebagai First Level Support untuk masalah di Cabang atau unit kerja Kantor Pusat dan mencatat langkah-langkah yang telah dilakukan di incident log serta mengubah status menjadi resolved.
8. Melakukan eskalasi masalah yang tidak dapat ditangani Helpdesk ke Second Level Support / Tier-2 serta memonitor hasil penanganannya.
9. Melakukan eskalasi dan notifikasi ke level support yang lebih tinggi (Third Level Support – Tier 3) untuk masalah yang belum terselesaikan oleh Second Level Support/Tier-2 dalam kurun waktu yang telah ditentukan.
10. Merekapitulasi insiden yang terjadi setiap bulannya, serta menginformasikan ke Problem Management Controller agar ditindak lanjuti dan didapat solusi permanen.

2.2 Person in Charge (PIC) Insiden

PIC bertanggung jawab terhadap penyelesaian insiden yang dilaporkan oleh first level support/tier-1 atau Help Desk. Tugas dan tanggung jawab PIC dibagi menjadi 2 bagian, diantaranya:

a. PIC Aplikasi / tier-2

Bertanggung jawab terhadap penyelesaian masalah yang dilaporkan oleh first level support/tier-1.

b. Supervisor Aplikasi / tier-3

Bertanggung jawab terhadap penyelesaian masalah yang diinformasikan oleh second level support/tier-2.

2.3 Pihak Ketiga (Vendor)

Vendor memiliki peran sebagai penyedia solusi alternatif, sebagai sarana dalam penyelesaian masalah maupun pencegahan terhadap terjadinya gangguan/masalah dikemudian hari. Vendor dihadirkan dalam rangkaian penyelesaian insiden atas inisiatif PIC insiden.

BAB 3

Kategori, Skala Waktu, Prioritas, dan Eskalasi Insiden

3.1 Kategori Insiden

Insiden teknologi informasi dikelompokkan menjadi 4 kategori yaitu :

Kategori	Sub-Kategori
Aplication	• ATM system • Mobile Banking • SMS Banking • Corporate Management System • E-channel • Host to Host System
Infrastructure	• ATM machine • Server • Storage • Air Conditioner • Electric • Cabling
Network	• TELKOM • LINTAS ARTHA
Major Incident	• Core Banking • OLIBS 724 Front End • OLIBS 724 Back End

*Catatan:

Kategori dan Sub-Kategori dapat bertambah sesuai perkembangan.

3.2 Penentuan Prioritas

Berikut adalah penentuan prioritas insiden TI :

Incident Priority		*Tingkat Kerugian (Severity)*		
		3 - Low	*2 - Medium*	*1 - High*
Dampak (Impact)	*Tidak Online*	*3 - Low*	*2- Medium*	*2 - Medium*
	Online	*2 - Medium*	*2 - Medium*	*1 - High*

Insiden yang memiliki dampak online, tidak dapat dilakukan penundaan (pending) terhadap penyelesaian gangguan/masalah. Sedangkan insiden yang tidak berdampak online, apabila PIC meminta untuk dilakukan penundaan (pending) terhadap penyelesaian, maka hal tersebut diizinkan.

3.3 Target Waktu

Pelayanan manajemen insiden TI diselenggarakan selama 24 jam sehari, 7 hari seminggu, dan 365 hari setahun. Berikut ini merupakan target waktu yang digunakan dalam penyelesaian masalah yang terkait dengan prioritas.

Prioritas	Target	
	Response	Resolve
3 - Low	90% - 10 menit	90% - 1 days
2 - Medium	90% - 3.5 menit	90% - 4 hours
1 - High	95% - 1 menit	90% - 2 hours

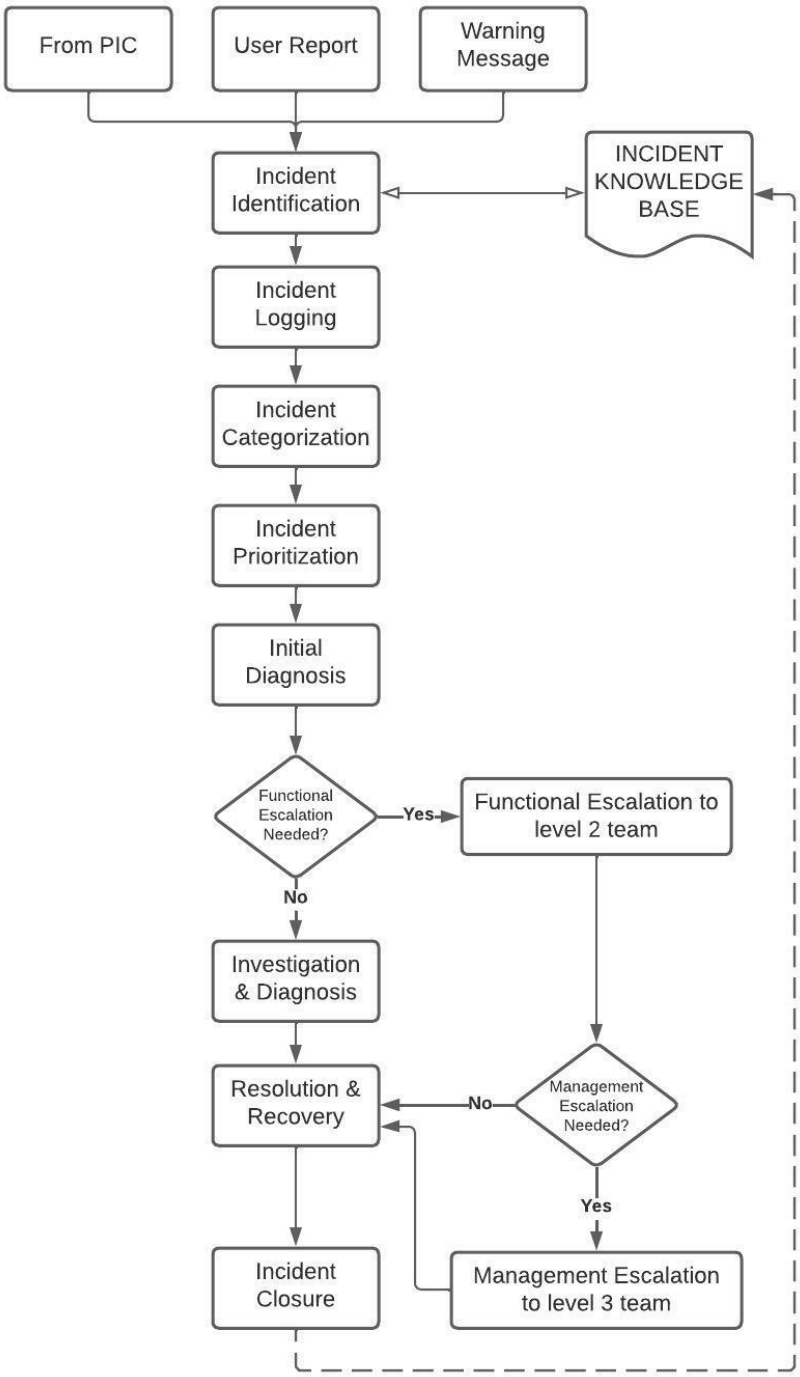
3.4 Critical Success Factors dan Key Performance Indicatior

Berikut adalah beberapa contoh **Critical Success Factors** berserta dengan **Key Performance Indicator**-nya dalam Manajemen insiden yang berdasarkan pada framework ITIL v3 :

No.	Critical Success Factors	Key Performance Indicator
1	Menyelesaikan insiden secepat mungkin dengan meminimalkan dampaknya terhadap bisnis	Waktu rata-rata yang dibutuhkan untuk mencapai resolusi insiden
		Perincian (*breakdown*) insiden pada setiap tahapan
		Persentase insiden yang dapat diselesaikan oleh *Help Desk* tanpa melakukan eskalasi ke tingkat yang lebih tinggi (*first point of contact*)
		Jumlah dan persentase insiden yang dapat diselesaikan secara *remote* atau tanpa melakukan kunjungan
		Jumlah insiden yang diselesaikan tanpa memberi dampak pada bisnis (mis. insiden dideteksi oleh *event management tools dan* diselesaikan sebelum dapat berdampak pada bisnis)
2	Memelihara kualitas layanan TI	Jumlah total Insiden
		Backlog insiden untuk setiap layanan TI
		Jumlah dan persentase insiden besar untuk setiap layanan TI
3	Menjaga kepuasan nasabah dengan layanan TI	Hasil skor rata-rata survei pengguna/nasabah (total dan berdasarkan kategori pertanyaan)
		Persentase survei kepuasan yang dijawab berbanding jumlah total survei kepuasan yang dikirim
4	Meningkatkan visibilitas dan komunikasi insiden kepada staf pendukung bisnis dan TI	Jumlah rata-rata pelaporan insiden melalui Help Desk atau kontak lain dari pengguna bisnis.
		Jumlah keluhan atau masalah pengguna bisnis tentang konten dan kualitas komunikasi insiden
5	Menyelaraskan aktivitas manajemen insiden dengan tujuan bisnis	Persentase insiden yang ditangani sesuai dengan waktu respons yang disepakati (target waktu respons insiden dapat ditentukan dalam SLA, misalnya, berdasarkan kode dampak dan urgensi)
		Biaya rata-rata per insiden
6	Memastikan bahwa metode dan prosedur standar digunakan untuk respons, analisis, dokumentasi, manajemen berkelanjutan dan pelaporan insiden yang efisien dan cepat untuk menjaga kepercayaan bisnis pada kapabilitas TI	Jumlah dan persentase insiden yang salah penugasan
		Jumlah dan persentase insiden yang salah dikategorikan
		Jumlah dan persentase insiden yang diproses per petugas Help Desk
		Jumlah dan persentase insiden yang terkait dengan perubahan dan rilis.

BAB 4

Alur Proses Manajemen Insiden Teknologi Informasi



4.1 Identifikasi Insiden

Proses manajemen insiden (*incident management*) dimulai dengan identifikasi.

Identifikasi yang paling umum dilakukan adalah melalui layanan *service desk* dan laporan dari staf teknisi. Selain itu identifikasi insiden dapat dilakukan secara otomatis oleh *tool event management*. *Tool* ini akan mengidentifikasi masalah sesaat ketika insiden terjadi. Kondisi ideal dari langkah identifikasi adalah insiden dapat teridentifikasi sebelum terjadi implikasi terhadap *user*.

4.2 Pencatatan Insiden

Langkah ini wajib dilakukan untuk setiap jenis insiden baik yang berskala besar maupun kecil. Beberapa informasi yang harus dicatat terkait suatu insiden adalah ID, kategori insiden, waktu terjadi, deskripsi insiden, nama orang/grup yang bertanggung jawab atas penanganan, implikasi insiden, dan waktu penutupan tiket insiden.

4.3 Kategorisasi Insiden

Pembuatan kelompok/kategori insiden membutuhkan sebuah proses khusus antara pengelola TI dan pihak manajemen organisasi. Hal ini bertujuan untuk menghasilkan kategori insiden dan prioritas penanganannya yang sejalan dengan proses bisnis organisasi. Kategori insiden dapat dibuat berdasarkan perkiraan lamanya penanganan, implikasi terhadap proses bisnis organisasi, dan jumlah staf teknis terkait.

4.4 Prioritas Insiden

Langkah prioritas insiden dilakukan berdasarkan kategorisasi yang telah dibuat sebelumnya. Prioritas penanganan insiden dapat dilakukan berdasarkan besarnya implikasi insiden terhadap kegiatan bisnis utama organisasi, ataupun berdasarkan lamanya penanganan insiden. Insiden yang memiliki prioritas paling tinggi ditangani terlebih dahulu.

4.5 Diagnosa Awal

Diagnosa awal terhadap insiden wajib dilakukan oleh setiap pihak yang pertama kali berhubungan dengan insiden baik itu *service desk*, staf teknis, maupun perangkat otomatis seperti *tool event management*. Jika insiden ditemukan oleh *service desk* melalui telepon dari *user*, maka diusahakan *service desk* tersebut yang menyelesaikan insiden selama *user* masih berhubungan melalui telepon.

4.6 Eskalasi Insiden

Eskalasi insiden adalah tindakan menaikkan level penanganan insiden. Hal ini berkaitan erat dengan hasil diagnosa awal terhadap insiden. Jika dari diagnosa ditemukan insiden yang tidak dapat ditangani, maka wajib dilakukan eskalasi insiden. Eskalasi insiden ada 2 macam, yaitu eskalasi fungsi dan eskalasi hierarki. Eskalasi fungsi adalah tindakan menaikkan level penanganan kepada satu level di atasnya. Sedangkan eskalasi hierarki adalah tindakan menaikkan level penanganan melintasi hierarki organisasi misalnya kepada manajer IT atau manajer bisnis yang terkait.

4.7 Investigasi Insiden

Tindakan investigasi dilakukan untuk menemukan sumber penyebab insiden. Dalam melakukan investigasi, setiap tindakan wajib dilaporkan juga ke dalam formulir insiden. Hal ini berguna sebagai data historis tindakan penanganan suatu insiden.

4.8 Resolusi Insiden

Langkah ini merupakan tindakan penyelesaian suatu insiden. Resolusi dapat dilakukan oleh *service desk* sebagai pihak yang pertama menemukan insiden dari *user*, staf teknisi yang sedang mengerjakan kegiatan konfigurasi, maupun oleh *supplier* terhadap perangkat yang masih dalam garansi.

4.9 Penutupan Insiden

Langkah penutupan adalah langkah yang dilakukan oleh *service desk* maupun staf teknisi terkait untuk memastikan apakah insiden telah benar selesai ditangani. Yang harus diperhatikan dalam langkah penutupan ini adalah dokumentasi proses penanganan insiden, perkiraan terhadap perulangan insiden, dan survei kepuasan *user* atas penanganan insiden.

BAB 5

Pelaporan Insiden

5.1 Format Pelaporan Melalui Help Desk

Pelaporan insiden melalui Help Desk divisi TSI dapat diakses dengan mengirimkan pesan dari aplikasi Telegram menggunakan Chat Bot HelpDesk-NTBS dengan format pesan sebagai berikut :

/REPORT INC : Kantor_Cabang/Cabang_Pembantu_Asal NOMOR_PEGAWAI : "deskripsi insiden"

5.2 Format Pelaporan Melalui Call Center

Pelaporan insiden melalui Call Center 24 jam Bank XYZ dapat diakses dengan mengirimkan pesan dari aplikasi Telegram menggunakan Chat Bot HelpDesk-NTBS dengan format pesan sebagai berikut :

/REPORT INC : NAMA_NASABAH No._REKENING : "deskripsi insiden"