Pengukuran Tingkat Kematangan Manajemen Risiko Sistem X pada PT. Y Menggunakan Framework Risk IT Domain Risk Governance

Triyani Sylvia Ferrore
Jurusan Sistem Informasi Fakultas Teknologi Informasi
Universitas Kristen Maranatha
Bandung, Indonesia
tryani_sylvia@yahoo.com

Diana Trivena Yulianti
Jurusan Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Maranatha
Bandung, Indonesia
diana.ty@itmaranatha.org

Abstrak—**Information technology has long been used in business processes at the PT.Y and are expected to provide added value to the achievement of enterprise goals. In addition to its benefits, the application of information technology also contains risks that may affect the business process itself, causing losses for the enterprise. Therefore, enterprise must understand and anticipate any potential risks that may occur. Application of good information technology risk management aim to reduce the negative impacts of risk that may arise. To find out the extent to which enterprise manage the risks associated with information technology it needs to be evaluated. The research will use the Risk IT framework with Risk Governance domain approach as an information technology risk management standards issued by ISACA to evaluate the implementation of risk management governance at the PT. Y. The evaluation process will be based on a maturity model that has been defined by the Risk IT framework to measure the maturity level of information technology risk management governance conditions at the PT. Y.**

Kata kunci—IT Risk Management; Risk Governance; Risk IT Framework.

I. PENDAHULUAN

PT. Y merupakan salah satu perusahaan yang bergerak di bidang jasa yang menjalankan bisnis layanan pengiriman dokumen dan barang serta misi sosial demi memenuhi kebutuhan masyarakat Indonesia. PT. Y berupaya untuk meningkatkan mutu pelayanan yang berorientasi pada kepuasan pelanggan dengan memperhatikan efisiensi dan efektifitas sumber daya, serta kemampuan meningkatkan laba usaha melalui pemanfaatan ilmu pengetahuan dan teknologi.

Dalam menjalankan bisnisnya teknologi informasi telah berperan sangat baik karena mampu memberikan nilai tambah guna pencapaian tujuan instansi, PT. Y menyadari tentang risiko-risiko yang mungkin terjadi terhadap teknologi informasi yang bisa menyebabkan kegagalan dalam menjalankan fungsi sistem informasi sehingga bisa menyebabkan kerugian-kerugian bagi perusahaan.

Jika risiko-risiko tersebut tidak dikelola dengan baik maka akan menimbulkan dampak yang merugikan bagi perusahaan dalam mencapai tujuannya. Manajemen risiko akan meningkatkan nilai perusahaan sekaligus mendukung pertumbuhan ekonomi dengan menurunkan biaya modal serta mengurangi ketidakpastian aktivitas sosial. Penerapan manajaemen risiko oleh perusahaan ini bertujuan untuk mengidentifikasi, mengukur, dan mengatasi risiko perusahaan pada level toleransi tertentu [1].

Framework risk IT menyediakan kerangka kerja komprehensif untuk mengontrol dan mengelola bisnis berbasis teknologi informasi. Risk IT menyediakan kerangka kerja untuk membantu perusahaan dalam mengidentifikasi, menentukan, dan mengelola risiko teknologi informasi.[2] Oleh karena itu dilakukan analisis manajemen risiko pada PT. Y dengan menggunakan framework risk IT domain Risk Governance.

Rumusan masalahnya adalah seberapa matang manajemen risiko sistem X di PT. Y?

Tujuan penelitian yang dilakukan adalah melakukan pengukuran tingkat kematangan manajemen risiko sistem X di PT. Y menggunakan framework Risk IT domain Risk Governance.

II. METODE PENGUMPULAN DATA

Analisis tingkat kematangan manajemen risiko sistem X dilakukan dengan cara mengumpulkan data melalui :

1. Observasi

   Observasi dilakukan di PT. Y bertujuan untuk memahami ruang lingkup sistem X serta proses bisnis berhubungan dengan pemanfaatan sistem X.

2. Wawancara

   Wawancara dilakukan pada bagian helpdesk sistem X dan manajer dan manajer manajemen risiko PT. Y.

3. Dokumen

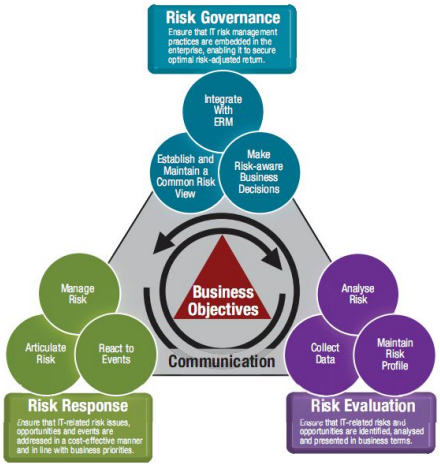
Dokumen yang dikumpulkan adalah dokumen yang berhubungan dengan aktivitas manajemen risiko, yaitu executive summary, struktur organisasi manajemen risiko, tugas & wewenang divisi manajemen risiko, toleransi risiko, kebijakan risiko teknologi informasi, pedoman penerapan manajemen risiko, materi pelatihan sistem X, struktur organisasi pengelolaan teknologi informasi, penanganan keamanan informasi, petunjuk teknis sistem X, dan petunjuk pelaksanaan sistem X.

III. RISK IT FRAMEWORK

Dengan perkembangan teknologi yang semakin meningkat sebuah perusahaan perlu melakukan proses pengolahan data yang mana memerlukan dukungan peralatan komputer/jaringan komunikasi dan alat pendukung lainnya yang berarti sebuah perusahaan harus menggunakan sistem berbasis teknologi informasi. Pengolahan data sendiri memiliki tujuan untuk menghasilkan sebuah informasi yang diperlukan untuk menambah pengetahuan tentang kondisi yang dihadapi, atau mengurangi ketidakpastian yang dihadapi oleh perusahaan [3]

Risk IT framework digunakan untuk membantu menerapkan tata kelola teknologi informasi, dan perusahaan yang telah diadopsi COBIT sebagai kerangka tata kelola teknologi informasi yang dapat digunakan oleh Risk IT untuk meningkatkan manajemen risiko. Proses-proses yang ada harus tergabung dengan hal-hal di bagian internal maupun eksternal perusahaan. Hal-hal internal dapat meliputi insiden yang ada di bagian operasional TI, kegagalan dalam proyek, dan pergantian dari sebuah strategi TI. Hal-hal eksternal sendiri dapat meliputi perubahan keadaan yang ada di pasar, adanya teknologi baru dan menyebabkan regulasi pada TI. Risiko TI sendiri dapat dikatakan adalah risiko bisnis yang mana risiko bisnis mencakup dalam pengguna, pemilik, cara mengoperasikan, keterlibatan, pengaruh dan adopsi TI tersebut di dalam perusahaan.

Model proses pada Risk IT framework memiliki tiga domain Risk Governance (RG), Risk Evaluation (RE) and Risk Response (RR) seperti yang dijelaskan pada Gambar 1.



Gambar 1 Risk IT Framework [2]

A. *Risk Governance*

Pada tahap ini harus dipastikan bahwa paktek manajemen risiko TI telah disampaikan dalam perusahaan, untuk memungkinkan dalam penyesuaian risiko secara optimal. Risk Governance terdiri dari tiga proses yaitu:

1. RG1 Establish and maintain a common risk view
2. RG2 Integrate with ERM
3. RG3 Make risk-aware business decisions

B. *RG 1 Establish and maintain a common risk view*

Memastikan bahwa aktivitas manajemen risiko selaras dengan kapasitas tujuan perusahaan yang berkaitan dengan kerugian TI dan kepemimpinan memiliki toleransi yang subjektif terhadap hal tersebut. Berikut adalah key activities RG1:

RG1.1 Perform enterprise IT risk assessment
RG1.2 Propose IT risk tolerance thresholds
RG1.3 Approve IT risk tolerance
RG1.4 Align IT risk policy
RG1.5 Promote IT risk-aware culture
RG1.6 Encourage effective communication of IT risk

C. *RG2 Integrate with ERM*

Mengintegrasikan strategi risiko TI dan operasi dengan keputusan risiko strategi bisnis yang telah dibuat. Berikut adalah key activities RG2:

RG2.1 Establish and maintain accountability for IT risk management
RG2.2 Co-ordinate IT risk strategy and business risk strategy
RG2.3 Adapt IT risk practices to enterprise risk practice
RG2.4 Provide adequate resources for IT risk management
RG2.5 Provide independent assurance over IT risk management

D. *RG3 Make risk-aware business decisions*

Memastikan bahwa pengambilan keputusan oleh perusahaan berdasarkan dari peluang dan konsekuensi. Berikut adalah key activities RG3:

RG3.1 Gain management buy-in for the IT risk analysis approach
RG3.2 Approve IT risk analysis
RG3.3 Embed IT risk considerations in strategic business decision making
RG3.4 Accept IT risk
RG3.5 Prioritise IT risk response activities

IV. MODEL KEMATANGAN (*MATURITY MODELS*) [2]

Untuk setiap domain Risk IT, sudah disediakan versi tingkat tinggi dan rinci dari model kematangan. Versi rinci dibangun di sekitar atribut-atributnya, yang masing-masing berkembang melalui kategori:

1. Kepedulian dan Komunikasi (Awareness dan Communication).
2. Tanggung Jawab dan Akuntabilitas (Responsibility and Accountability).

3. Penetapan Tujuan dan Pengukuran (Goal setting and Measurement).
4. Kebijakan, Standar dan Prosedur (Policies, Standards and Procedures).
5. Keterampilan dan keahlian (Skills and Expertise).
6. Perangkat bantu dan otomatisasi (Tools and Automation).

Model Kematangan dapat membantu manajemen memahami dimana kekurangan yang ada dan menetapkan target yang diperlukan. Model kematangan adalah yang paling tepat untuk suatu perusahaan karena dipengaruhi oleh tujuan bisnis perusahaan, lingkungan operasi dan praktik industri.

A. Tingkat kematangan :

1) Level 0 : Non-existent

Perusahaan tidak mengakui adanya kebutuhan untuk mempertimbangkan dampak bisnis dari risiko TI. Keputusan yang melibatkan risiko TI kurang memiliki informasi yang kredibel. Tidak ada kesadaran tentang persyaratan eksternal untuk manajemen risiko TI dan integrasi dengan manajemen risiko perusahaan.

2) Level 1 : Initial

Ada pemahaman yang muncul bahwa risiko TI adalah penting dan perlu dikelola, tetapi perusahaan hanya memandang sebagai masalah teknis dan bisnis utamanya hanya mempertimbangkan kerugian risiko TI. Kriteria identifikasi risiko TI bervariasi di seluruh perusahaan dan organisasi TI. Secara default, TI bertanggung jawab untuk masalah manajemen, ketersediaan, akses sistem, dll. Risk appetite / selera risiko dan toleransi risiko yang diterapkan hanya berjalan selama penilaian risiko. Kebijakan risiko perusahaan dan standar, yang minimal harus terbaik, mungkin tidak lengkap dan / atau hanya mencerminkan persyaratan external dan kurangnya pemikiran dipertahankan dan mekanisme penegakan hukum. Keterampilan manajemen Risiko TI mungkin ada atas dasar ad hoc, tetapi mereka tidak aktif mengembangkan. Persediaan control ad hoc, yang tidak terkait dengan risiko, tersebar di aplikasi desktop.

3) Level 2 : Repeatable

Ada kesadaran akan kebutuhan untuk secara aktif mengelola risiko TI, tetapi fokusnya adalah pada kepatuhan teknis dengan tidak ada antisipasi nilai tambah. Adanya pemimpin untuk manajemen risiko TI dalam bagian yang memikul tanggung jawab dan biasanya bertanggung jawab sekalipun tidak secara resmi disetujui. Toleransi risiko diatur secara lokal dan mungkin sulit untuk di agregasi. Investasi difokuskan pada isu-isu risiko tertentu dalam bagian fungsional dan bisnis (misalnya keamanan, kelangsungan bisnis, operasi). Ada dewan yang mengeluarkan pedoman manajemen risiko. Minimum adanya persyaratan keterampilan, yang meliputi kesadaran risiko TI, identifikasi daerah yang berisiko dan paling penting di perusahaan. Fungsional dan TI hanya spesifik berdasarkan isu-isu risiko yang ada.

4) Level 3 : Defined

Manajemen risiko TI dipandang sebagai masalah bisnis, dan kedua sisi buruk dan sisi baik risiko TI diakui. Adanya pemimpin yang ditunjuk untuk risiko TI di seluruh perusahaan, Pemimpin ini bergerak dengan komite risiko perusahaan, di mana risiko TI ada dalam ruang lingkup dan dibahas dalam perusahaan. Bisnis memahami bagaimana TI termasuk dalam risiko perusahaan dan adanya pandangan untuk portofolio risiko. Toleransi risiko perusahaan berasal dari toleransi lokal dan kegiatan pengelolaan risiko TI selaras di seluruh perusahaan. Kategori risiko formal telah diidentifikasi dan dijelaskan dengan yang jelas. Pelatihan akan kesadaran risiko meliputi situasi dan skenario luar dalam kebijakan dan struktur yang spesifik dan mempromosikan bahasa umum untuk mengkomunikasikan risiko. Persyaratan yang ditentukan ada untuk persediaan terpusat masalah risiko. Tersedianya alat alur kerja yang digunakan untuk mengatur masalah risiko dan langkah pengambilan keputusan.

5) Level 4 : Managed

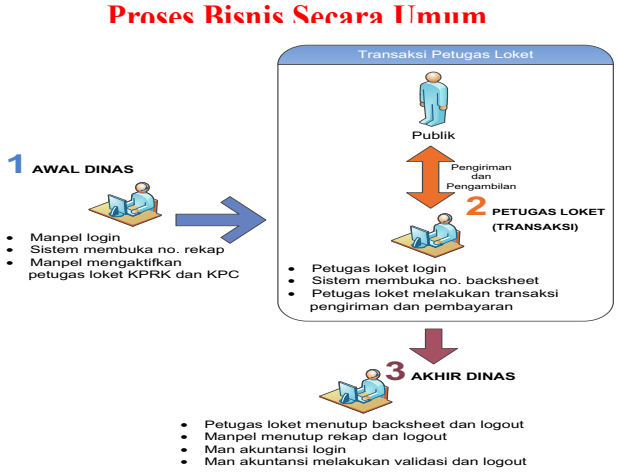
Manajemen risiko TI dipandang sebagai business enabler, dan kedua sisi buruk dan sisi baik risiko TI sudah dipahami. Pemimpin yang ditunjuk untuk risiko TI di perusahaan sepenuhnya terlibat dengan komite risiko perusahaan yang mengharapkan nilai dari TI termasuk ke dalam keputusan. Peran departemen TI dalam manajemen risiko secara operasional dan ERM (Enterprise Risk Management) secara luas dipahami dengan baik. Dewan mendefinisikan risk appetite / selera risiko dan toleransi risiko sebagai bagian risiko, termasuk risiko TI. Kebijakan perusahaan dan standar mencerminkan toleransi risiko bisnis. Skenario risiko jauh ke depan dan perusahaan mempertimbangkan risiko TI di seluruh perusahaan. Keputusan bisnis penting sepenuhnya dipertimbangkan dalam kemungkinan kerugian dan kemungkinan keuntungan. Persyaratan ketrampilan secara rutin diperbarui untuk semua bidang, kemahiran dipastikan untuk semua bidang manajemen risiko dan didorong adanya sertifikasi. Adanya alat yang memungkinkan perusahaan memiliki portofolio manajemen risiko, otomatisasi TI, alur kerja manajemen risiko, dan pemantauan kegiatan kritis dan kontrol.

6) Level 5 : Optimised

Para senior eksekutif membuat titik untuk mempertimbangkan semua aspek risiko TI dalam keputusan mereka. Pemimpin risiko TI dianggap sebagai penasihat terpercaya selama desain, implementasi dan perningkatan operasi. Departemen TI adalah pemain utama dalam bisnis-line untuk upaya risiko secara operasional perusahaan. Tujuan strategis didasarkan pada pemahaman tingkat eksekutif pada ancaman bisnis yang berkaitan dengan skenario risiko TI dan berdasarkan peluang kompetitif. Kebijakan perusahaan dan standar terus mencerminkan toleransi risiko bisnis sambil meningkatkan efisiensi. Perusahaan secara resmi membutuhkan perbaikan terus-menerus dalam keterampilan manajemen risiko TI, berdasarkan tujuan pribadi dan perusahaan yang jelas. Real-time monitoring kejadian risiko insiden dan kontrol ada, seperti halnya otomasi kebijakan manajemen.

V. PROSES BISNIS YANG BERKAITAN DENGAN PENGGUNAAN SISTEM X DI PT. Y

Sistem X merupakan salah satu produk dari yang ada di PT Y, layanannya berupa layanan pengiriman uang baik dari maupun ke kota dan ke desa yang pasti sampai ke alamat tujuan dalam waktu seketika. Secara umum proses bisnis yang dijalankan memiliki 3 tahap yaitu tahap awal dinas, tahap petugas loket (transaksi), dan tahap akhir dinas seperti yang terlihat pada gambar 2.



Gambar 2 Risk IT Framework

VI. ANALISIS DOMAIN RISK GOVERNANCE

Domain Risk Governance adalah langkah perusahaan untuk memastikan bahwa praktek-praktek manajemen risiko TI telah ada di dalam perusahaan, memungkinkan perusahaan untuk mengoptimalkan tindakan terhadap risiko yang ada.

A. Analisis RG1 Establish and Maintain a Common Risk View:

1) RG1.1 Perform enterprise IT Risk Assessment

PT Y telah menerapkan IT *risk assessment* dan mempersiapkan tenaga IT nya dalam melakukan risk assessment. PT. Y pernah mengadakan pelatihan, materi pelatihan mengenai *awareness* (risiko & *threat*), cara mengidentifikasi, *threat*, *vulnerability assesstment*, risiko dan penjelasan mengenai standar COBIT yang akan digunakan PT. Y

2) RG1.2 Propose IT risk tolerance thresholds

Risiko-risiko TI yang berhubungan dengan rencana strategis teknologi informasi PT. Y dituangkan dalam dokumen executive summary pada rencana strategis teknologi informasi PT Y. Perkembangan teknologi yang cepat, khususnya dalam bidang telekomunikasi dan sistem informasi PT. Y memberikan solusi yang bersifat terbuka dan fleksibel terutama untuk membuat pilihan dan akibat implementasinya. Perbedaan pendekatan teknis yang dilakukan pihak ketiga yang juga menyumbang risiko teknis terhadap pekerjaan PT. Y membangun tim perubahan dan mengakomodasi apa yang bisa ditolerir untuk meminimalisir hal tersebut.

Kurangnya skill dan knowledge SDM PT. Y, serta penguasaan terhadap berbagai alternatif solusi atau terhadap standar yang telah ditentukan sehingga memberikan risiko terhadap teknologi PT. Y memberikan pelatihan yang sesuai untuk meminimalkan risiko tersebut. Platform yang berbeda baik itu antara sistem yang telah berjalan, maupun dengan alternatif yang akan diimplementasikan PT. Y memberikan kontribusi terhadap risiko teknis yang cukup tinggi.

3) RG1.3 Approve IT risk tolerance

PT. Y sangat terbuka terhadap risiko TI yang ada dan telah mempertimbangkan efek-efek dari risiko-risiko tersebut terhadap perusahaan, toleransi risiko sendiri ditetapkan dalam rencana strategis teknologi informasi yang dituangkan dalam executive summary di PT. Y.

4) RG1.4 Align IT risk policy

Risiko TI dijabarkan dalam penerapan sistem keamanan informasi. Salah satu kebijakan risiko TI yang ada di PT. Y tertuang pada dokumen Kebijakan Risiko TI PT. Y selain itu pada dokumen mekanisme standar dalam pengelolaan teknologi dan Struktur Organisasi dan Pengelolaan Teknologi

5) RG1.5 Promote IT risk-aware culture

Untuk penyebaran budaya dalam memahami risiko yang ada PT. Y melakukan trainning terhadap staf-staf TI dan unit bisnis yang bersangkutan dengan teknologi informasi. Salah satu pelatihan yang pernah dilakukan oleh PT. Y untuk mengurangi risiko teknologi informasi. Untuk penanganan risiko sendiri PT. Y membuat petunjuk teknis dan petunjuk pelaksanaan Sistem X yang diberikan kepada pihak-pihak yang menjalankan bisnis.

6) RG1.6 Encourage effective communication of IT risk

PT. Y akan melakukan security awareness program dan campaign, lalu melakukan pelatihan masalah security yang diadakan oleh direktorat teknologi dan jasa keuangan dimana sampai saat ini masih berjalan di PT. Y dan sudah dilaksanakan di 11 area diikuti oleh internal masih dalam jabatan manajer.

B. Analisis RG2 Integrate With ERM:

Berikut ini adalah hasil analisis proses RG2 pada domain RG berdasarkan key activities yang telah diterapkan dengan melakukan wawancara dan observasi secara langsung pada PT. Y:

1) RG2.1 Establish and maintain accountability for IT risk management

Pertanggungjawaban terhadap manajemen risiko TI di PT. Y secara lisan dijelaskan menjadi tanggung jawab dari pihak-pihak terkait dengan teknologi informasi tersebut dalam hal ini pihak-pihak yang terkait. Direktorat teknologi dan jasa keuangan sendiri memiliki bagian yang mengatur risiko TI yang melakukan kegiatan untuk mengurangi risiko-risiko TI pada perusahaan.

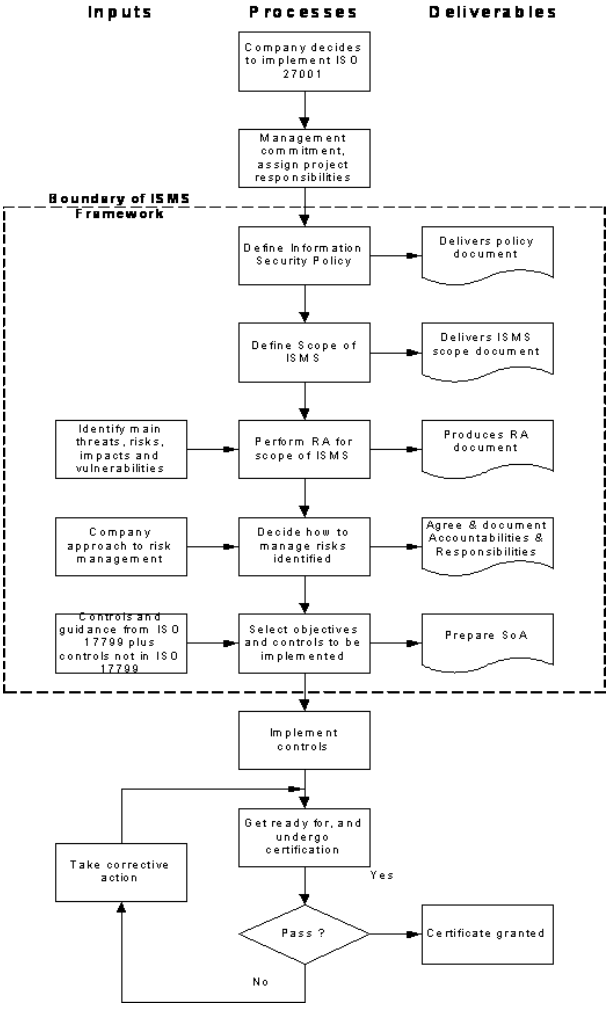
2) RG2.2 Co-ordinate IT risk strategy and business risk strategy

Berdasarkan arahan strategis manajemen yang dimana terdapat lonjakan target pendapatan yang signifikan, maka PT. Y memerlukan persiapan komprehensif agar sumber daya terutama teknologi informasi dapat diintegrasikan dan

diimplementasikan dengan baik dan berdasarkan bahwa keamanan informasi merupakan kebutuhan organisasi untuk mengurangi risiko seperti pencurian data, percobaan hacking, tindakan vandalisme, dan lainnya maupun ancaman kejadian lainnya seperti bencana alam yang berpengaruh bagi kelangsungan organisasi dan bisnis serta meraih kesempatan untuk mengembangkan bisnis yang lebih besar serta bahwa berdasrkan kajian bahwa sistem keamanan informasi mampu mendeteksi ketidaksesuaian sistem teknologi secara signifikan dan mengurangi inefesiensi proses kerja menjadi lebih baik.

3) RG2.3 Adapt IT risk practices to enterprise risk practice

Praktek Risiko TI pada PT. Y memakai standar ISO27001 berdasarkan KD No. 20 Tahun 2012. Penanganan Keamanan Informasi dengan certification process [4] yang terlihat pada gambar 3



Gambar 3 Certification Process

4) RG2.4 Provide adequate resources for IT risk management

PT. Y pada bagian direktorat teknologi jasa keuangan memiliki bagian yang mengatur risiko TI yaitu bagian security dan quality assurance, menggunakan standar ISO27001 dalam prakteknya dan PT. Y menggunakan website monitoring risiko yang ada agar bisnis yang ada tetap berjalan sebagaimana mestinya. Website monitoring yang digunakan di PT. Y

5) RG2.5 Provide independent assurance over IT risk management

Untuk memonitor perencanaan dalam aksi risiko TI PT. Y memiliki pengendalian akan risiko TI yang terjadi yaitu:

1. Risk Acceptance yaitu menerima risiko tanpa melakukan tindakan apapun.
2. Risk Avoidance yaitu menghindari sepenuhnya risiko.
3. Risk Reduction yaitu mengurangi efek negatif dari ancaman hingga pada tingkat yang diterima oleh organisasi.
4. Risk Transfer yaitu memindahkan efek dari ancaman kepada pihak lain seperti mengasuransikan semua aset perusahaan pada asuransi.

Sampai saat ini secara lisan dijelaskan PT. Y banyak melakukan pengendalian risiko pada tahap risk reduction. Dan pengontrolan dilakukan secara periodik untuk menjamin manajemen risiko TI.

C. Analisis RG3 Make Risk-aware Business Decisions

Proses ini untuk memastikan bahwa pengambilan keputusan oleh perusahaan berdasarkan dari peluang dan konsekuensi berdasarkan kepercayaan untuk kesuksesan TI di perusahaan.

Berikut ini adalah hasil analisis proses RG3 pada domain RG berdasarkan key activities dengan melakukan wawancara dan observasi secara langsung pada PT. Y

1) RG3.1 Gain management buy-in for the IT risk analysis approach

Bagian risiko TI pada direktorat teknologi dan jasa keuangan akan melakukan analisis risiko TI secara umum dijelaskan secara lisan dimulai dengan klasifikasi data terhadap unit-unit bisnis yang terkait dan memeriksa apakah unit-unit bisnis tersebut telah menyimpan data secara baik dan benar sehingga muncul risiko-risiko yang muncul, lalu dilakukan vulnerability *assessment* yang akan didokumentasikan dalam dokumen *executive summary*. Hasil-hasil dari analisis risiko TI tersebut akan dijadikan ke dalam *security awareness program* dan manajer-manajer akan mengikuti pelatihan masalah *security* yang sampai saat ini masih dilakukan. Hal-hal tersebut adalah untuk meningkatkan keamanan informasi yang ada dalam perusahaan untuk mengurangi risiko seperti pencurian data, percobaan hacking, tindakan vandalisme, serta ancaman bencana alam yang berpengaruh bagi kelangsungan organisasi dan bisnis.

2) RG3.2 Approve IT risk analysis

Laporan analisis risiko-risiko TI yang ada di PT. Y tertuang dalam dokumen executive summary yang berisi sumber-sumber risiko TI, pengendalian risiko yang mengikuti standar ISO270001, penanganan Keamanan Informasi .

3) RG3.3 Embed IT risk considerations in strategic business decision making

Dalam dokumen executive summary akan menyimpulkan pertimbangan-pertimbangan yang akan menyimpulkan efek-efek dari risiko TI itu sendiri, maka dibutuhkan sebuah tindakan penanganan keamanan informasi di linkungan PT. Y yang mana penerapan keamanan informasi yang ada di PT. Y tertuang dalam dokumen Keamanan Informasi bahwa lonjakan target pendapatan yang signifikan, keamanan informasi sebagai kebutuhan, dan sistem keamanan informasi mampu mendeteksi ketidaksesuaian sistem teknologi menjadi pertimbangan-pertimbangan yang didiskusikan dalam rapat perusahaan.

4) RG3.4 Accept IT risk

Dalam dokumen executive summary akan ditampilkan risiko-risiko teknologi dan daftar kejadian yang berdampak paling merugikan yang sampai saat ini masih mungkin terjadi di PT. Y.

5) RG3.5 Prioritise IT risk response activities

Pengendalian risiko PT. Y dibagi menjadi empat tahapan yaitu, risk acceptance, risk avoidance, risk reduction, dan risk transfer. Secara lisan dijelaskan dalam PT. Y sendiri sampai saat ini kejadian-kejadian risiko yang disebabkan pihak external jarang sekali terjadi bahkan belum pernah, maka untuk risiko yang terjadi pun sampai saat ini pengendalian yang dilakukan adalah dengan melakukan risk reduction. Untuk tindakan pengendalian risiko PT. Y menempatkan helpdesk yang ditempatkan dalam setiap area yang jabatan dan tugasnya adalah sebagai berikut:

1. Helpdesk Teknis adalah kelompok pengendali sistem yang bertugas memberi bantuan untuk menyelesaikan setiap masalah teknis.
2. Helpdesk Proses Bisnis adalah kelompok pengendali di unit bisnis yang bertugas memberi bantuan untuk menyelesaikan setiap masalah operasional.
3. Helpdesk WilY adalah kelompok pengendali yang berada di wilayah dan bertanggung jawab terhadap seluruh unit pelaksana teknis di wilayahnya.

Kegiatan pemonitoran selalu dilakukan melalui website monitoring yang dimiliki oleh PT. Y. PT. Y juga memiliki standar kebijakan untuk menjaga aset TI perusahaan secara umum.

VII. Evaluasi Tingkat Kematangan

A. Evaluasi proses RG1 Establish and Maintain a Common Risk View:

Pada proses ini PT. Y sudah memiliki aktivitas manajemen risiko dimana sudah adanya workshop mengenai penilaian risiko TI yang ada tetapi masih belum diikuti oleh seluruh area PT. Y, PT. Y juga sudah membuat toleransi risiko dan kebijakan untuk risiko TI, PT. Y juga sudah melakukan pelatihan terhadap unit-unit bisnis terkait untuk meningkatkan kepedulian akan risiko, tetapi untuk kegiatan diskusi risiko TI sendiri secara lisan dijelaskan dilakukan apabila risiko terjadi pada saat itu, tidak ada perencanaan khusus yang dilakukan setiap periodik untuk mendiskusikan risiko. Kegiatan program yang ada pun masih hanya diikuti oleh jabatan tingkat manajer belum secara keseluruhan pihak yang terkait bisnis.

Tingkat kematangan proses RG1 adalah Level 2 Repeatable, sebab sudah adanya kesadaran perusahaan dalam mendiskusikan dan menyampaikan risiko TI di perusahaan namun toleransi risiko yang dibahas masih hanya berdasarkan pada perkembangan teknologi, kebutuhan, dan keterampilan yang dibutuhkan di perusahaan saat ini dan belum adanya perencanaan secara teratur untuk kegiatan komunikasi yang membahas risiko TI di perusahaan.

B. Evaluasi proses RG2 Integrate With ERM:

Pada proses ini PT. Y sudah menspesifikasikan tanggung jawab terhadap manajemen risiko TI yang ada pada perusahaan dan sudah mempertimbangkan efek risiko TI terhadap strategi bisnis yang ada serta sudah menggunakan metode untuk menangani risiko yang ada dengan menggunakan ISO27001, serta memiliki website monitoring yang memonitor kegiatan pada bisnis, tetapi unit bisnis terkait tidak memiliki dokumen pengukuran risiko yang seharusnya dilaporkan kepada pihak yang menangani manajemen risiko yaitu divisi manajemen risiko dan good corporate governance yang ada dikarenakan pada saat kejadian terjadi unit bisnis terkait terkadang bisa menyelesaikan masalah yang ada. Untuk masalah atau kejadian yang terjadi juga dijelaskan secara lisan merupakan tanggung jawab pihak terkait.

Tingkat kematangan proses RG2 adalah Level 2 Repeatable, sebab sudah adanya bagian yang menangani risiko TI di perusahaan dan komite manajemen risiko perusahaan yang menyediakan pedoman manajemen risiko dan sumber-sumber untuk menangani risiko TI namun risiko TI masih difokuskan pada isu-isu risiko yang ada pada perusahaan dan bagian risiko TI yang ada masih belum sepenuhnya bergerak bersama dengan komite manajemen risiko yang ada di perusahaan.

C. Evaluasi proses RG3 Make Risk-aware Business Decisions:

Pada proses ini PT. Y sudah mengadakan pelatihan-pelatihan mengenai pentingnya analisis risiko TI tetapi belum sepenuhnya diikuti oleh seluruh pemimpin yang ada, pemimpin yang ada memberikan tugas kepada bagian security and quality assurance di direktorat teknologi dan jasa keuangan sepenuhnya untuk mempertimbangkan kegiatan risiko. Analisis risiko PT. Y ada pada executive summary dan juga sudah mempertimbangkan keamanan, dan sudah ada penanganan terhadap kejadian yang ada seperti menempatkan helpdesk di setiap area yang terkait dengan PT. Y dengan mengikuti aturan yang ada pada petunjuk teknis dan petunjuk pelaksanaan yang diberikan kepada setiap pihak terkait bisnis.

Tingkat kematangan proses RG3 adalah Level 3 Defined, sebab PT. Y sudah mempertimbangkan efek-efek dari risiko TI dan menentukan tindakan-tindakan yang harus dilakukan dalam menyikapi risiko TI namun untuk diskusi dalam melakukan analisis risiko masih diserahkan ke bagian TI di perusahaan dan pertimbangan risiko yang ada masih berdasarkan isu-isu risiko yang ada serta hanya pada yang paling sering terjadi di perusahaan.

VIII. KESIMPULAN

Berdasarkan hasil dari analisis dari Risk IT Framework domain Risk Governance didapatkan jawaban dari rumusan masalah yaitu sebagai berikut:

- Tingkat kematangan proses RG1 *Establish and Maintain a Common Risk View* adalah level 2 Repeatable
- Tingkat kematangan proses RG2 *Integrate With ERM* adalah level 2 Repeatable
- Tingkat kematangan proses RG3 *Make Risk-aware Business Decisions* adalah level 3 Defined

DAFTAR PUSTAKA

[1] Pramana, T. (2011). Manajemen Risiko Bisnis. Jawa Timur: Sinar Ilmu Publishing.

[2] ISACA. (2009). The Risk IT Framework. Diakses pada 15 April 2013, tersedia online di http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

[3] Gondodiyoto, S. (2007). Audit Sistem Informasi dan Pendekatan Cobit. Jakarta: Mitra Wacana Media.

[4] The ISO 27000 Directory 2007. (2007). The ISO27001 Certification Process. Diakses pada 2 Mei 2013, tersedia online di http://www.27000.org/ismsprocess.htm