Analisa Risiko Pengelolaan Data, Keamanan Sistem dan Pengelolaan Vendor TI di PT. X

Zefania Wahjudi[1], Adi Wibowo[2], Ibnu Gunawan[3]
Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Kristen Petra
Jl. Siwalankerto 121 – 131
Surabaya 60236
Telp. (031) – 2983455
Fax. (031) - 8417658
E-mail: zefania.wahjudi@yahoo.com[1], adiw@petra.ac.id[2], ibnu@petra.ac.id[3]

ABSTRAK

Departemen *Procurement* PT. X adalah sebuah departemen dari sebuah perusahaan manufaktur yang berpusat di Surabaya, bertugas sebagai penyedia kebutuhan yang diperlukan oleh seluruh departemen di PT. X. IT di *Procurement* sudah digunakan secara penuh untuk menunjang kegiatan dan proses bisnis perusahaan. Namun tidak pernah dilakukan analisa risiko sehingga menyebabkan perusahaan tidak mengetahui dampak apa saja yang mungkin akan terjadi yang dapat menghambat kinerja *Procurement*. Untuk itu dibutuhkan suatu analisis risiko yang bertujuan menganalisis faktor-faktor risiko apa saja yang dapat mengganggu proses bisnis *Procurement* dan memberikan respon terhadap risiko yang paling kritikal.

Pada penelitian ini dilakukan analisa risiko terhadap IT dan proses bisnis dalam lingkup *Procurement* PT. X. Langkah-langkah dalam melakukan analisa risiko tersebut yaitu dengan menggunakan standar COBIT 4.1 untuk menentukan proses dalam analisa, ISO 31000 sebagai *framework* langkah-langkah kerja, dan *Risk Rating Methodology OWASP* sebagai acuan penilaian dan perhitungan risiko. Berdasarkan wawancara yang telah dilakukan, ditemukan beberapa faktor-faktor risiko yang ada di *Procurement* PT. X. Risiko-risiko yang ditemukan antara lain data kontrak tidak disimpan dalam sistem *database*, tidak ada perjanjian tertulis mengenai PIC *vendor* yang dikhususkan untuk menangani *project* terkait, perusahaan tidak mempunyai rencana cadangan jika ada masalah dalam proses pembuatan barang/jasa oleh *vendor*, belum ada manajemen risiko IT di *Procurement*, tidak ada dokumentasi khusus berupa pencatatan risiko akan setiap *vendor*, tidak ada penyeragaman format laporan *vendor progress* sehingga adanya poin-poin informasi yang tidak disampaikan oleh *vendor*, serta tidak ada keharusan bagi *vendor* untuk memberikan pelaporan *vendor progress*.

Respon yang diusulkan kepada perusahaan yaitu sebaiknya menyalin kontrak (di-*scan*) dan menyimpannya kedalam sistem, kemudian melakukan *backup* secara rutin, mengidentifikasi dan mendokumentasikan individu-individu yang terlibat dalam proyek, beserta personil *back-up* dan menanyakan kontak dengan detil, menyediakan rencana cadangan jika seandainya salah satu pihak membatalkan kontrak sebelum akhir dari masa kontrak tersebut, membuat analisa manajemen risiko IT, melakukan pencatatan atau dokumentasi khusus terkait risiko akan setiap *vendor* dan meninjau kembali secara teratur setidaknya setiap tahun dan disetujui oleh manajemen, membuat standar laporan khusus untuk pelaporan *vendor progress*, serta menjadwalkan komunikasi secara berkala antara *Procurement* dan *vendor* untuk membahas *vendor progress*.

Kata Kunci: Analisa risiko, COBIT 4.1, ISO 31000, OWASP, metode kualitatif

ABSTRACT

Procurement Department in PT. X is a department from a manufacturing company based in Surabaya, it provides needs of all departments in PT. X. Information Technology in Procurement is completely utilized to support the company's business activities and processes. However, this company has not done any risk assessment, that might causing the company does not know what impact that might occur that can choke Procurement's performance. Therefore, a risk assessment is required to analyze the risk factors that could interfere Procurement's business processes and provide a response to the most critical risks.

This research is about to assess risks that might have happened in Information Technology and Procurement's business processes. The steps in this risk assessment are using COBIT 4.1 standard to define the processes in the analysis, ISO 31000 as a framework in risk assessment steps, and Risk Rating Methodology OWASP as a reference for valuation and risk calculations. Based on the interview that has done, 14 risk factors have been found in PT. X Procurement. Some of them are data contracts is not stored in a database system, no written agreement regarding to devoted vendor PIC to handle related project, company does not have any contingency plan if there is a problem in the manufacture of goods/services by the vendor, Procurement has not performed IT risk assessment yet, so there is no analysis of the events might occur, no special documentation such as risk recording of each vendor, no uniformity of vendors progress report format so their points of information might not delivered completely, and no requirement for vendors to provide vendor reporting progress.

The proposed response to the company are company should copy the contract and scan then store it into the system, identify and document the individuals involved in the project, providing a contingency plan in case either party to cancel the contract before the end of the contract period, make IT risk assessment, taking notes or special documentation related risk will each vendor, make format report for vendor reporting progress, and regularly schedule communication between Procurement and vendors to discuss the vendor progress.

Keywords: *Risk assessment, COBIT 4.1, ISO 31000, OWASP, qualitative research method*.

1. PENDAHULUAN

Departemen *Procurement* PT. X adalah sebuah departemen dari sebuah perusahaan manufaktur yang berpusat di Surabaya. Departemen tersebut tersebar di beberapa kota di Indonesia, seperti Surabaya, Jakarta, Denpasar dan lain-lain. PT. X adalah sebuah perusahaan yang sudah menggunakan sistem yang terintegrasi dalam kesehariannya mengolah data perusahaan. Mengingat besarnya peran departemen *Procurement* dalam menjalankan kegiatan usaha PT. X maka diperlukan pengolahan data yang optimal, baik dalam pengelolaan maupun maintenance data-data dalam lingkup *Procurement*.

Dalam menjalankan kegiatan perusahaan, departemen *Procurement* terbagi ke dalam dua subkategori, yaitu *Procurement Category* dan *Purchasing*. Dalam kesehariannya, *Procurement* berhubungan dengan banyak data rahasia perusahaan. Oleh karena itu dibutuhkan adanya proses perawatan, pemeliharaan dan perbaikan data, seperti perencanaan penghapusan data secara baik dan berkala termasuk proses *backup* data.

Penggunaan IT di dalam PT. X sangat berpengaruh terhadap kesehariannya dalam menjalanakan kegiatan usaha. Semua proses dalam *Procurement* sudah berbasis TI. TI sangat berperan penting dalam proses bisnis yang berlangsung di *Procurement* PT. X. Selain itu, TI dibutuhkan untuk *backup data* agar jika suatu saat terjadi hal hal yang tidak diinginkan, seperti *server down*, kegiatan bisnis perusahaan tetap dapat berjalan dengan baik.

Mengingat pentingnya peranan TI dalam mendukung proses bisnis *Procurement*, maka perlu dilakukan suatu *risk assessment* terhadap risiko TI yang bisa berdampak terhadap proses bisnis *Procurement*. Melalui *risk assessment*, pihak *Procurement* dapat terbantu dalam mengetahui risiko-risiko apa saja yang bisa terjadi, mengukur seberapa mungkin risiko tersebut terjadi dan apa dampaknya. Dari hasil perhitungan risiko, dapat ditunjukkan manakah yang menjadi prioritas yang butuh penanganan segera dan manakah risiko yang dapat ditangani kedalam penangan berikutnya. Melalui proses tersebut, *Procurement* diharapakan dapat menggunakan hasil dari risk assessment untuk mengambil kebijakan dalam menangani risiko agar tidak menghambat kinerja perusahaan maupun meningkatkan kinerja dalam menjalankan proses bisnisnya.

2. LANDASAN TEORI

2.1 ISO 31000

Metode ini menyediakan prinsip-prinsip dan pedoman terhadap *risk management.* Metode ini dapat diaplikasikan terhadap seluruh aktivitas yang ada dalam sebuah perusahaan, dan dalam berbagai aktivitas dalam sebuah perusahaan, termasuk strategi dan keputusan, operasi, proses, fungsi, *project*, produk, *service*, dan aset. Metode ini juga dapat diaplikasikan terhadap semua tipe risiko, baik yang memiliki dampak positif maupun negatif.

Risk Management mengacu kepada arsitektur (*principles, framework,* dan *process*) agar dapat mengatur risiko secara efektif. *Managing Risk* mengacu kepada pengaplikasian arsitektur risiko tertentu [4].

- *Process for managing risk*
  - *Communication and Consultation*
    Komunikasi dan konsultasi dengan *internal* dan *external stakeholder* harus ada dalam setiap tingkatan dari proses *risk management.*
  - *Establishing the context*
    Saat membuat konteks untuk proses manajemen risiko, perusahaan perlu mempertimbangkan secara rinci pengaturan ruang lingkup dan kriteria risiko untuk proses yang tersisa, dan konteksnya harus mencakup parameter baik internal maupun eksternal yang relevan untuk perusahaan.
  - *Risk Assessment*
    a. Risk Identification
    Tahap awal dari *risk assessment* dimana seorang analis menganalisa sumber risiko, alasan munculnya risiko, serta apakah dampak potensial bagi perusahaan terkait dengan risiko tersebut. Informasi yang didapat haruslah informasi yang relevan dan *up–to–date.*
    b. Risk Analysis
    Tahap kedua dalam *risk assessment*, yaitu tahap pengembangan dari risiko–risiko yang telah ada di dalam *risk identification*. *Risk analysis* memberikan masukan untuk *risk evaluation* dan keputusan tentang apakah risiko perlu di-*treatment* dan metode apa yang paling tepat untuk *risk treatment*.
    c. Risk Evaluation
    Tahap risiko bertujuan untuk membantu dalam pengambilan keputusan, berdasarkan hasil *risk analysis*, tentang risiko yang membutuhkan penanganan dengan segera
  - *Risk Treatment*
    Risk Treatment adalah tahapan pemilihan apakah risiko dapat diterima atau ditolak.
  - *Monitoring and Review*
    Monitoring and review harus dijadwalkan dalam proses risk management. Proses ini dapat melibatkan pemeriksaan biasa atau pengawasan dari apa yang sudah ada atau bisa periodik. Keduanya harus dijadwalkan.
  - *Recording the risk management process*
    Aktivitas *risk management* harus dicatat, sehingga dari catatan tersebut dapat dijadikan perbaikan dari risiko-risiko yang ada.

2.2 COBIT 4.1

Control Objectives for Information and related Technology (COBIT) adalah kerangka kerja yang dikeluarkan oleh *IT Governance Institute* (ITGI) sebagai acuan dan control bagi manajemen dalam pengelolaan proses IT.

COBIT digunakan sebagai standar dalam menilai dan mengukur proses dalam manajemen untuk memastikan bahwa proses IT dapat berlangsung dengan baik baik [2].
Proses COBIT untuk *Procurement* PT.X :

- DS 2 (*Manage Third-party Services*)
  Proses ini dilakukan dengan mendefinisikan secara jelas peran, tanggung jawab dan harapan dalam perjanjian *third-*party (*suppliers*, *vendors* dan *partners*) serta meninjau dan pemantauan perjanjian tersebut untuk efektivitas dan kepatuhan.

Manage Third-party Services memenuhi kebutuhan bisnis TI dengan menyediakan layanan pihak ketiga yang memuaskan yang transparan tentang manfaat, biaya dan risiko.
Dalam analisa risiko berdasarkan DS 2 terdapat 4 *control objective* yang akan dianalisa berdasarkan pertanyaan-pertanyaan wawancara berdasarkan *control practices*. 11 *control objective* tersebut yaitu:

- *Identification of All Supplier Relationships*
- *Supplier Relationship Management*
- *Supplier Risk Management*
- *Supplier Performance Monitoring*

- DS 5 (*Ensure Systems Security*)
  Kebutuhan untuk menjaga integritas informasi dan melindungi aset TI membutuhkan proses manajemen keamanan. Proses ini meliputi pembangunan dan mempertahankan peran keamanan dan responsibilties, kebijakan, standar, dan prosedur IT. Keamanan manajemen juga mencakup pemantauan keamanan dan pengujian berkala dan melaksanakan tindakan korektif untuk suatu kelemahan atau insiden. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis dari kerentanan keamanan dan insiden.

  Dalam analisa risiko berdasarkan DS 2 terdapat 11 *control objective* yang akan dianalisa berdasarkan pertanyaan-pertanyaan wawancara berdasarkan *control practices*. 11 *control objective* tersebut yaitu:
  - *Management of IT Security*
  - *IT Security Plan*
  - *Identity Management*
  - *User Account Management*
  - *Security Testing, Surveillance and Monitoring*
  - *Security Incident Definition*
  - *Protection of Security Technology*
  - *Cryptographic Key Management*
  - *Malicious Software Prevention, Detection and Correction*
  - *Network Security*
  - *Exchange of Sensitive Data*
- DS 11 (*Manage Data*)
  Manajemen data yang efektif memerlukan identifikasi kebutuhan data. Proses manajemen data juga mencakup pembentukan prosedur yang efektif untuk pengelolaan data, *backup* dan pemulihan data, dan pembuangan data. Manajemen data yang efektif membantu menjamin kualitas, ketepatan waktu dan ketersediaan data bisnis.
  Dalam analisa risiko berdasarkan DS 11 terdapat 6 *control objective* yang akan dianalisa berdasarkan pertanyaan-pertanyaan wawancara berdasarkan *control practices*. 6 *control objective* tersebut yaitu:
  - *Business Requirements for Data Management*
  - *Storage and Retention Arrangements*
  - *Media Library Management System*
  - *Disposal*
  - *Backup and Restoration*
  - *Security Requirements for Data Management*

2.3 Kriteria Penilaian Risiko Berdasarkan Analisa Risiko di Perpustakaan Universitas Kristen Petra

Teori analisa pemberian nilai untuk setiap likelihood dan impact juga mengacu berdasarkan IT Risk Assessment pada tahun 2011 di Perpustakaan Universitas Kristen Petra [1]. Berikut kriteria *likelihood*:

- *Skill Level*
  Pengukuran seberapa tingginya *technical skill* (keahlian secara teknis) yang dimiliki oleh *staff* perusahaan. *Skill* dapat mempengaruhi apakah suatu risiko dapat terjadi atau bahkan dibuat hampir mustahil. Pengetahuan yang dimiliki *staff* menjadi *skill* yang dinilai. Semakin tinggi *skill* atau pengetahuan yang dimiliki *staff* maka semakin rendah pula kemungkinan risiko tersebut muncul [1].
  - *Staff* mempunyai pengetahuan untuk memahami dan melaksanakan tindakan pencegahan risiko secara detail (1)
  - *Staff* hanya mempunyai sedikit pemahaman terkait pencegahan risiko (5)
  - Tidak ada pengetahuan sama sekali yang dimiliki oleh staff terkait pencegahan risiko (9)
- *Management and Stakeholder Suppport*
  Pengukuran seberapa besar dukungan manajemen atau perusahaan terhadap penanganan risiko. Sekalipun ada keahlian yang dimiliki oleh *staff*, tanpa adanya dukungan tertentu berupa suatu kebijakan atau wewenang yang diijinkan untuk melakukan maka pengetahuan terhadap risiko tidak memungkinkan untuk diaplikasikan [1]
  - *Management* dan *Stakeholder* mendukung atau menyetuji adanya kebijakan penanganan risiko (1)
  - *Management* dan *Stakeholder* mendukung namun kurang menganggap pentingnya penanganan risiko (5)
  - *Management* mempersulit pengerjaan untuk penanganan risiko (9)
- *Teamwork*
  Pengukuran seberapa baik kerjasama tim dalam mencegah terjadinya risiko. *Teamwork* yang buruk dapat mengakibatkan keseluruhan bisnis terkena dampak akibat terjadinya risiko. *Teamwork* meliputi pembagian kerja dalam menangani risiko, pelaksanaan dan inisiatif bersama, serta komunikasi antar pihak di dalamnya [1].
  - Adanya prosedur pembagian kerja, pelaksanaan, inisiatif dan komunkasi yang baik antar pihak penanganan risiko (1)
  - Adanya prosedur pembagian kerja dan inisiatif untuk penanganan risiko, namun belum ada pelaksanaan dan komunikasi yang berjalan untuk penaganan risiko tersebut (5)
  - Pembagian kerja, pelaksanaan dan inisiatif tidak jelas dalam penanganan risiko, juga tidak ada komunikasi untuk penanganan risiko (9)
- *Project Management*
  Pengukuran seberapa mampu *project management* yang dibuat dalam menangani risiko. *Project management* diukur dari adanya requirement yang jelas dalam menangani risiko, jangka waktu, biaya ruang lingkup, dan target yang ingin dicapai [1].
  - *Requirement*, waktu, biaya ruang lingkup dan target yang jelas (1)

- Ada *requirement*, namun jangka waktu dan target belum jelas dan ada tendensi *scope creep* (5)
- Tidak adanya *requirement*, batas waktu, target dan biaya yang jelas, dan adanya tendensi *scope creep* (9)

- *Awareness*
  Pengukuran seberapa tinggi kesadaran semua pihak terhadap risiko yang terjadi, dan kesadaran terkait tindakan yang harus diambil untuk mengatasi risiko tersebut [1].
  - Adanya kesadaran dan dorongan untuk melakukan tindakan dalam meminimalkan risiko (1)
  - Kecilnya kesadaran dan minimnya tindakan yang dilakukan untuk mencegah terjadinya risiko tersebut (5)
  - Tidak adanya kesadaran dalam meminimalkan risiko (9)

Kriteria penilaian *likelihood* risiko diatas berdasarkan Analisa Risiko di Perpustakaan Universitas Kristen Petra. Berikut kriteria *impact* berdasarkan OWASP.

2.4 Kriteria Penilaian Risiko Berdasarkan OWASP

Dalam OWASP ada dua kriteria penilaian, yaitu *likelihood* dan *impact*. Dari setiap kriteria tersebut, akan diberikan nilai berdasarkan tingkat keparahaannya sesuai dengan Gambar 1. Setelah itu, nilai yang diberikan kepada masing-masing kriteria dimasukkan ke dalam tabel seperti dalam Gambar 2 dan Gambar 3. Setelah menentukan nilai dari setiap kriteria yang ada, dilakukan perhitungan terhadap *likelihood* dan *impact* untuk mendapatkan nilai *risk severity* yang dikelompokkan dalam empat macam tingkat keparahan (*note*, *low*, *medium*, dan *high*) seperti dalam Gambar 4.

Berikut kriteria *impact* berdasarkan OWASP:

- *Technical Impact Factors*
  - *Loss of confidentiality*
    Loss of confidentiality adalah pengukuran seberapa banyak data yang terungkap dan seberapa sensitif data tersebut [9].
  - *Loss of integrity*
    Loss of integrity adalah kehilangan integritas sebuah data atau informasi. Hilangnya integritas data diukur berdasarkan seberapa banyak data yang dapat rusak (*corrupt*) dan seberapa parah kerusakannya [9].
  - *Loss of availability*
    Pengukuran seberapa banyak jasa atau layanan yang tidak dapat berjalan dan seberapa penting hal tersebut [9].
  - *Loss of accountability*
    Loss of accountability adalah pengukuran seberapa besar kemungkinan pelaku dapat terungkap [9].
- *Business Impact Factors*
  - *Financial damage*
    Pengukuran seberapa banyak kerusakan finansial (kerugian) yang dialami dari adanya kejadian tersebut. Semakin besar nominal yang yang harus dikeluarkan oleh perusahaan maka akan semakin besar risiko yang harus ditanggung [9].
  - *Reputation damage*
    Pengukuran seberapa besar kerusakan reputasi dapat membahayakan bisnis [9].
  - *Non-compliance*
    Pengukuran seberapa besar pelanggaran yang diakibatkan dengan timbulnya kejadian atau risiko tersebut. Semakin besar pelanggaran yang terjadi maka semakin besar risiko yang harus ditanggung [9].

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Gambar 1. *Likelihood and Impact Levels* [9]

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

Gambar 2. Overall Likelihood[9]

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=3.25 (LOW)			

Gambar 3. Overall Impact[9]

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Gambar 4. Overall Risk Severity[9]

3. PENILAIAN RISIKO

3.1 Kriteria Penilaian Risiko yang Dipakai

Kriteria penilaian untuk aspek *likelihood* dan *impact* risiko menggunakan penilaian berdasarkan OWASP dan Analisa Risiko di Universitas Kristen Petra. Namun ada beberapa kriteria yang dikembangkan sesuai dengan kondisi yang ada dalam perusahaan. Kriteria penilaian risiko yang telah dikembangkan dapat dilihat di Tabel 1.

Tabel 1. Kriteria Penilaian Risiko

Kriteria Penilaian Risiko		
Kriteria	**Sumber**	**Keterangan**
Skill Level	Chrisdiyanto, 2013	Sesuai dengan sumber
Management and Stakeholder Support	Chrisdiyanto, 2013	Sesuai dengan sumber
Teamwork	Chrisdiyanto, 2013	Sesuai dengan sumber
Project Management	Chrisdiyanto, 2013	Sesuai dengan sumber
Awareness	Chrisdiyanto, 2013	Sesuai dengan sumber

Sambungan Tabel 1. Kriteria Penilaian Risiko

Kriteria Penilaian Risiko		
Kriteria	**Sumber**	**Keterangan**
Confidentiality	Pengembangan analisa OWASP	Kehilangan kerahasiaan sebuah data atau informasi, yaitu dengan adanya gangguan seperti rusaknya data, kerahasiaan data terungkap atau bocor, atau hilangnya data atau informasi. Semakin sedikit data sensitif yang terungkap (bisa data sensitif maupun tidak sensitif) maka semakin kecil dampak yang ditimbulkan. −Hampir tidak ada data sensitif yang terbongkar (1) −Sedikit data sensitif terbongkar (5) −Sebagian data sensitif terbongkar (7) −Hampir semua data tidak aman atau terbongkar (9)
Integrity	OWASP	Sesuai dengan sumber
Availability	Pengembangan analisa OWASP	Pengukuran seberapa banyak jasa atau layanan yang tidak dapat berjalan akibat risiko tersebut, dan seberapa penting hal tersebut. −Semua layanan tetap tersedia dan berfungsi dengan normal (0) −Hampir tidak ada layanan yang terganggu (1) −Sebagian kecil layanan utama yang terganggu (3) −Sebagian besar layanan tambahan terganggu (5) −Sebagian besar layanan utama terganggu (7) −Hampir semua aspek layanan terganggu akibat terjadinya risiko tersebut (9)

Sambungan Tabel 1. Kriteria Penilaian Risiko

Kriteria Penilaian Risiko		
Kriteria	**Sumber**	**Keterangan**
Accountability	Pengembangan analisa OWASP	Pengukuran seberapa besar kemungkinan pihak-pihak yang bertanggung jawab terhadap risiko. Dalam hal ini dilakukan penilaian baik terhadap
Accountability	Pengembangan analisa OWASP	pihak yang akan bertanggung jawab sampai kepada individu. −Dapat sepenuhnya dilacak (1) −Pihak yang bertanggung jawab ada, namun belum ditemukan individu yang sepenuhnya bertanggung jawab (6) −Pihak yang seharusnya bertanggung jawab sama sekali tidak dapat ditemukan atau anonim (9)
Financial	OWASP	Sesuai dengan sumber
Reputation	Pengembangan analisa OWASP	Pengukuran seberapa besar kerusakan reputasi akan membahayakan bisnis akibat terjadinya sebuah risiko. −Kerusakan kecil (1) −Kerusakan yang cukup besar (4) −Kehilangan nama baik perusahaan (9)
Non-compliance	OWASP	Sesuai dengan sumber

3.2 Risk Severity

Berdasarkan hasil penilaian *likelihood* dan *impact*, dilakukan perhitungan untuk mendapatkan *risk severity* dengan mengalikan tiap-tiap aspek *likelihood* dan *impact*. Melalui hasil perhitungan *risk severity*, didapatkan *level* dari tiap-tiap risiko. Setelah itu maka dapat ditentukan prioritas untuk masing-masing risiko. Sembilan risiko terbesar yang ditemukan pada *Procurement* PT. X dapat dilihat pada Tabel 2.

Tabel 2. Risk Severity

Risk Severity					
Rank	**No.**	**Risiko**	**Risk Severity**	**Level**	**Overall Level**

Sambungan Tabel 2. Risk Severity

Risk Severity					
Rank	**No.**	**Risiko**	**Risk Severity**	**Level**	**Overall Level**
1	11.	Tidak ada pembatasan untuk mencolokkan *flashdisk*.	25.52	MH	*High*
2	10.	Tidak ada proses *login* untuk beberapa aplikasi yang digunakan oleh *Procurement* PT. X.	15.99	MM	*Medium*
3.	14.	SFTP (*Secure File Transfer Protocol*) tidak dapat dikonfigurasi khusus agar pesan tidak dapat diteruskan kepada *user* lain.	12.15	MM	*Medium*
4.	12.	*User access* tidak di-*maintain* dengan baik sesuai status yang terbaru.	10.82	LM	*Low*
5.	9.	Tidak ada IT *security plan*.	10.10	LM	*Low*
6.	4.	Belum ada manajemen risiko IT di *Procurement*, sehingga tidak ada analisa kejadian-kejadian yang mungkin timbul.	8.98	LM	*Low*
7.	13.	*Update antivirus* tidak otomatis sehingga ada virus terbaru yang mungkin dapat menyebabkan laptop terinfeksi virus.	8.12	LL	*Note*
8.	3.	Perusahaan tidak mempunyai rencana cadangan jika ada masalah dalam proses pembuatan barang/jasa oleh *vendor*.	2.86	LL	*Note*
9.	1.	Data-data kontrak tidak disimpan dalam sistem *database*.	2.15	LL	*Note*

3.3 Risk Response

Risk response merupakan cara perusahaan sebaiknya bereaksi terhadap risiko tersebut. Dari 9 risiko tertinggi yang ada, maka dapat disimpulkan *risk response planning* yang disarankan adalah sebagai berikut:

1. Tidak ada pembatasan untuk mencolokkan *flashdisk*.
   Risk severity: *High*
   Risk Response: *Avoid*
   Respon terhadap risiko ini adalah risiko jangan sampai terjadi. Anjurannya adalah dengan membatasi akses dalam bentuk fisik yaitu dalam hal ini adalah *flashdisk* sesuai dengan standar ISO 27002.
2. Tidak ada proses *login* untuk beberapa aplikasi yang digunakan oleh *Procurement* PT. X.
   Risk severity: *Medium*
   Risk Response: *Lessen*
   Respon terhadap risiko ini bertujuan untuk mengurangi *likelihood* risiko dengan memberikan *login* untuk pembatasan dan kontrol pada aplikasi sesuai dengan standar ISO 27002. Disebutkan bahwa:
   - hak akses yang terkait dengan setiap sistem produk (sistem operasi, database sistem manajemen dan setiap aplikasi, dan *user*) harus teridentifikasi dan di-*maintain*.
   - hak akses harus diberikan kepada *user* atas dasar kebutuhan dan hanya bila diperlukan, dan perusahaan sebaiknya mengendalikan hak akses *user* (membaca, merubah, menghapus, dan menjalankan).
3. SFTP (*Secure File Transfer Protocol*) tidak dapat dikonfigurasi khusus agar pesan tidak dapat diteruskan kepada *user* lain.
   Risk severity: *Medium*
   Risk Response: *Lessen*
   Respon dari risiko ini ini bertujuan untuk mengurangi *likelihood* risiko dengan menunjuk perwakilan yang dapat melihat dan memantau detail dari informasi insiden (NIST SP800-61). Berbagi informasi atau data perusahaan seharusnya ditujukan hanya kepada orang atau pihak yang tepat atau hanya yang membutuhkan dengan mempertimbangkan dampak bisnis dan teknis.
4. *User access* tidak di-*maintain* dengan baik sesuai status yang terbaru.

Risk severity: *Low*
Risk Response: *Avoid*
Sesuai standar ISO 27002, disebutkan bahwa perusahaan harus secepatnya menghapus atau menghalangi akses *user* yang jabatan atau *role* nya berubah ataupun yang sudah mengundurkan diri dari perusahaan, melakukan pemeriksaan serta menghapus ataupun menghalangi *user* ID atau akun yang mempunyai akses berlebihan (mubazir) secara berkala, serta memastikan bahwa *user* ID yang berlebihan tersebut tidak diberikan kepada *user* lainnya.

5. Tidak ada IT *security plan*.
Risk severity: *Low*
Risk Response: *Lessen*
Respon terhadap risiko ini bertujuan untuk mengurangi *likelihood* risiko dengan mengimplementasikan suatu rencana insiden (NIST SP800-61). Rencana tersebut harus mencakup misi, strategi, dan tujuan untuk respon insiden harus membantu dalam merespon insiden. Setelah sebuah perusahaan mempunyai persetujuan rencana dan sudah disetujui oleh manajemen, perusahaan harus melaksanakan rencana tersebut dan meninjau setidaknya setiap tahun untuk memastikan perusahaan berjalan sesuai dengan visi untuk mengembangkan kemampuan dan memenuhi tujuan untuk merespon akan adanya suatu insiden.
6. Belum ada manajemen risiko IT di *Procurement*, sehingga tidak ada analisa kejadian-kejadian yang mungkin timbul.
Risk severity: *Low*
Risk Response: *Lessen*
Respon dari risiko ini bertujuan untuk mengurangi *likelihood* risiko, anjurannya adalah *Procurement* seharusnya memiliki analisa terkait manajemen risiko IT yang dapat diacu sesuai dengan ISO 31000 atau NIST SP800-30.
7. *Update antivirus* tidak otomatis sehingga ada virus terbaru yang mungkin dapat menyebabkan laptop terinfeksi virus.
Risk severity: *Note*
Risk Response: *Assume*
Risiko yang termasuk dalam kategori *note* adalah risiko yang dapat diterima oleh perusahaan. Namun, jika ingin mengurangi terjadinya risiko tersebut anjurannya adalah sebaiknya *Procurement* ataupun perusahaan mempunyai sebuah sistem informasi yang mempunyai kemampuan untuk *update antivirus* secara otomatis (NIST SP800-53).
8. Perusahaan tidak mempunyai rencana cadangan jika ada masalah dalam proses pembuatan barang/jasa oleh *vendor*.
Risk severity: *Note*
Risk Response: *Assume*
Risiko yang termasuk dalam kategori *note* adalah risiko yang dapat diterima oleh perusahaan. Namun, jika ingin mengurangi terjadinya risiko tersebut anjurannya adalah sebaiknya *Procurement* menyediakan kondisi untuk renegosiasi atau penghentian kontrak, yaitu dengan mempunyai rencana cadangan jika seandainya salah satu pihak membatalkan kontrak sebelum akhir dari masa kontrak tersebut. Hal ini sesuai dengan standar ISO 27002.
9. Data-data kontrak tidak disimpan dalam sistem *database*.
Risk severity: *Note*
Risk Response: *Assume*
Risiko yang termasuk dalam kategori *note* adalah risiko yang dapat diterima oleh perusahaan. Namun, jika ingin mengurangi terjadinya risiko tersebut anjurannya adalah menyalin kontrak tersebut (di *scan*) dan menyimpannya kedalam sistem, kemudian melakukan *backup* secara rutin.

4. KESIMPULAN

Berdasarkan analisa dan observasi yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. Dalam proses analisa risiko ini, ditemukan satu risiko yang termasuk dalam kategori tinggi, dua yang termasuk dalam ketegori menengah, tiga dalam kategori rendah, dan delapan masuk dalam kategori sangat rendah.
2. Risiko-risiko dalam bidang IT yang termasuk dalam kategori tinggi dan menengah yang mungkin terjadi selama berjalannya proses bisnis dan tindakan mitigasi yang dapat dilakukan oleh PT. X adalah :
   - Tidak ada pembatasan untuk mencolokkan *flashdisk*.
     Response: *Avoid* menggunakan standar ISO 27002 dengan membatasi akses dalam bentuk fisik.
   - Tidak ada proses *login* untuk beberapa aplikasi yang digunakan oleh *Procurement* PT. X.
     Response: *Lessen* menggunakan standar ISO 27002 dengan memberikan *login* untuk pembatasan dan kontrol pada setiap aplikasi.
   - SFTP (*Secure File Transfer Protocol*) tidak dapat dikonfigurasi khusus agar pesan tidak dapat diteruskan kepada *user* lain.
     Response: *Lessen* menggunakan standar NIST SP800-61 [7].
3. Untuk risiko-risiko dalam bidang IT yang termasuk dalam kategori rendah dan sangat rendah yang mungkin terjadi selama berjalannya proses bisnis dalam *Procurement* PT. X adalah mengenai *security* dan *vendor management*. Tindakan pencegahan yang mungkin dapat dilakukan oleh perusahaan adalah dengan menggunakan standar ISO 27002, ISO 31000, NIST SP800-61, NIST 800-30 dan NIST 800-61 untuk risiko yang termasuk dalam lingkup *security* dan PCI DSS 3.0 untuk risiko yang termasuk dalam lingkup *vendor mangement*.

5. DAFTAR PUSTAKA

[1] Chrisdiyanto, I. 2013. *IT Risk Assessment di Perpustakaan Universitas Kristen Petra*. Surabaya: Universitas Kristen Petra.

[2] IT Governance Institute. 2007. *COBIT 4.1*. USA: ISACA.

[3] International Organization for Standardization. 2005. *Information technology — Security techniques — Code of practice for information security management*, USA: ISO.

[4] International Organization for Standardization. 2008. *Risk management — Principles and guidelines on implementation*, USA: ISO.

[5] National Institute of Standards and Technology. 2002. *Computer Security*, USA: NIST.

[6] National Institute of Standards and Technology. 2005. *Information Security*, USA: NIST.

[7] National Institute of Standards and Technology. 2012. *Computer Security*, USA: NIST.

[8] Payment Card Industry. 2014. *Information Supplement: Third-Party Security Assurance*, USA: PCI.

[9] The OWASP Risk Rating Methodology. Retrieved May 23, 2014, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.