PENILAIAN RISIKO KEAMANAN INFORMASI APLIKASI ONLINE TRAVEL AGENT: STUDI KASUS PT XYZ

Hendra Dwi Hadmanto [a,1,*], Rizal Fathoni Aji [b,2], Jihan Prama Nurahman [c,3]

[a, b, c] Fakultas Ilmu Komputer Universitas Indonesia Jakarta, Indonesia
[1] hendra.dwi91@ui.ac.id *; [2] rizal@cs.ui.ac.id; [3] jihan.prama94@ui.ac.id
* Hendra Dwi Hadmanto

ABSTRAK

PT XYZ adalah perusahaan milik swasta yang bergerak di bidang Online Travel Agent (OTA). PT XYZ menggunakan Aplikasi OTA berupa web dan mobile apps untuk menjalankan bisnis utamanya menjual produk untuk kebutuhan perjalanan dan pariwisata, baik penjualan tiket transportasi, akomodasi dan Event. Aplikasi OTA sebagai aset penting dari PT XYZ harus dilindungi dari segala ancaman yang dapat mengganggu proses bisnis dan memberikan kerugian bagi perusahaan. Adanya berbagai ancaman dan kerentanan terhadap aplikasi OTA membutuhkan adanya hasil Penilaian Risiko Keamanan Informasi (PRKI) yang mampu mendeteksi risiko-risiko beserta dampaknya bagi perusahaan dan seperti apa penanganan terhadap risiko-risiko tersebut. Penentuan metode PRKI pada penelitian ini menggunakan Core Unified Risk Framework (CURF) untuk melakukan evaluasi terhadap sembilan metode PRKI yang dipilih berdasarkan kriteria pemilihan metode PRKI dan dengan melakukan studi literatur terhadap metode PRKI dengan skor tertinggi berdasarkan hasil evaluasi menggunakan CURF. Berdasarkan hasil evaluasi, metode ISO 27005 dipilih untuk menjalankan PRKI aplikasi OTA PT XYZ. Penilaian Risiko aplikasi OTA menggunakan ISO 27005 menghasilkan 16 risiko yang kemudian dipetakan dengan 18 penanganan risiko

KATA KUNCI
ISO 27007
Resiko Keamanan Informasi
Asesmen

ABSTRACT

PT XYZ is a private company engaged in Online Travel Agent (OTA) Business. It provide OTA Applications in the form of web and mobile apps to run it's main business, selling products for travel and tourism needs such as transportation tickets, accommodation, and events. As an important asset for PT XYZ, OTA Applications must be protected from any threats that can disrupt business process and cause losses for company. The existence of various threats and vulnerabilities to OTA Applications require evaluation from Information Security Risk Assessment (ISRA) that can identify any risks including impacts to company and what treatments need to prepare for it. In this research, we used Core Unified Risk Framework (CURF) to evaluate nine ISRA methods selected based on criteria then reevaluate selected method by reviewing relevant study on selected method. Based on evaluation process, ISO 27005 is selected to run ISRA for OTA applications. OTA Application risk assessment with ISO 27005 generated 16 risks that map to 18 treatments promoted.

KEYWORD
ISO 27007
Information Security Risk Assessment

1. Pendahuluan

PT XYZ adalah perusahaan yang berdiri lebih dari sepuluh tahun yang menjalankan bisnis *Online Travel Agent* (OTA). Dimulai dengan menjual tiket kereta api melalui web secara daring, mereka kemudian merambah ke bidang bisnis perjalanan lainnya seperti tiket pesawat, sewa kamar hotel, sewa mobil, dll. Sebagai perusahaan yang memanfaatkan data dan informasi sebagai inti dari bisnis mereka, PT XYZ harus mampu mendeteksi dan mengelola setiap risiko keamanan informasi yang dapat memberikan kerugian bagi perusahaan.

PT XYZ menjual produknya dengan menyediakan aplikasi OTA berbasis web, *mobile apps* (Android dan iOS). Aplikasi OTA PT XYZ menyediakan mesin pencarian berdasarkan kategori produk yang diinginkan yaitu tiket pesawat, kereta api, *Event*, dan penyewaan kamar akomodasi seperti hotel dan vila. Aplikasi OTA juga memberikan kemudahan dalam melakukan transaksi, perubahan jadwal, pembatalan, dan

pengembalian dana dalam satu aplikasi. Agar bisa menjaga kepercayaan dari pelanggannya semua layanan yang diberikan dari aplikasi ini harus berjalan cepat dan tanpa kendala.

Sebagai perusahaan yang berorientasi profit, tidak dapat dipungkiri bahwa XYZ memiliki aset-aset khususnya aset teknologi informasi seperti proses bisnis, informasi, perangkat lunak, perangkat keras, dll. yang perlu dilindungi dari segala risiko yang dapat merugikan bisnis perusahaan. Serangan terhadap teknologi informasi dapat menyebabkan hilangnya kesempatan, hilangnya kapitalisasi pasar, dan hancurnya nama baik yang telah dibangun oleh perusahaan [1].

Sejak pandemi COVID 19 terjadi pada awal tahun 2020, tidak hanya Pemerintah Indonesia tetapi hampir pemerintah di semua negara membuat kebijakan pembatasan kegiatan sosial dan perjalanan. Kebijakan ini memberikan dampak negatif pada bisnis utama XYZ yang mengakibatkan penurunan pendapatan perusahaan. Kebijakan ini juga berdampak pada lingkungan kerja perusahaan dari bekerja di kantor (WFO) menjadi bekerja dari rumah (WFH) yang membuat komunikasi terkait pekerjaan menjadi lebih lambat. WFH juga berarti bahwa tim infrastruktur harus memastikan semua akses ke dokumen, aplikasi, dan server basis data dikonfigurasi dengan benar sehingga hanya karyawan yang berhak yang dapat mengaksesnya. Semua kondisi ini tentu saja menghasilkan jenis risiko baru yang perlu ditangani ketika mengelola Manajemen Risiko Keamanan Informasi (MRKI)

Risiko keamanan informasi tidak hanya datang dari luar namun ada juga risiko yang datang dari dalam baik risiko yang disengaja maupun tidak disengaja. Risiko yang datang dari luar seperti pencurian data, usaha intrusi ke dalam sistem serta risiko yang datang dari dalam seperti *error* pada aplikasi dan kesalahan konfigurasi memiliki kemungkinan dan dampak yang berbeda kepada PT XYZ. Untuk mengelola risiko pada PT XYZ dibutuhkan sebuah Manajemen Keamanan Risiko yang mampu mendeteksi dan menangani risiko-risiko tersebut.

Sistem Manajemen Risiko di perusahaan XYZ dikelola oleh tim IT Security yang dievaluasi secara berkala minimal setahun sekali. Perencanaan MRKI pada perusahaan XYZ dimulai dengan melakukan Penilaian Risiko Keamanan Informasi (PRKI) untuk menilai semua risiko yang perlu dimitigasi, dialihkan, dihindari, atau diterima. Meskipun ada dokumen pedoman mengenai MRKI di perusahaan XYZ tidak disebutkan metode PRKI mana yang harus digunakan pada proses PRKI yang menghasilkan pertanyaan penelitian "Apa Metode PRKI paling sesuai untuk menjalankan proses PRKI di perusahaan XYZ? Bagaimana hasil PRKI berdasarkan metode yang dipilih?"

2. Tinjauan Pustaka

A. Online Travel Agent

Perusahaan OTA, merupakan perusahaan yang memanfaatkan internet untuk menjual produk perjalanan dan pariwisata yang lahir pada tahun 1990, Memiliki peranan krusial terhadap distribusi daring [2]. Pada awal tahun 2004, perjalanan dan pariwisata diakui sebagai industri teratas dalam hal volume transaksi daring [3]. Wisatawan modern lebih memahami akan peluang yang ditawarkan oleh internet [4], mereka meluangkan waktu untuk menemukan informasi yang akurat di internet, memeriksa penyedia informasi yang berbeda [5] sebelum memilih produk yang paling sesuai dan akhirnya melakukan reservasi daring [6]. Berbeda dengan agen tradisional yang berperan sebagai perantara menghubungkan wisatawan kepada hotel, pesawat dan penyedia transportasi lainnya, OTA beroperasi lebih dari sekedar perantara tetapi juga sebagai mitra bisnis atau vendor[7]. Dengan memanfaatkan jaringan dan kecepatan teknologi informasi OTA membuka peluang bagi perusahaan lain untuk menjual produk mereka melalui rekan bisnisnya (B2B).

B. Penilaian Risiko Keamanan Informasi

Penilaian Risiko Keamanan Informasi (PRKI) secara umum merupakan metode yang digunakan untuk menghasilkan estimasi risiko. Risiko adalah kemungkinan kejadian dan konsekuensi yang berdampak pada organisasi [8]. Sampai jurnal ini disusun sudah ada ratusan metode PRKI yang tersedia. Penulismenggunakan Core Unified Risk Framework (CURF) yang dibangun oleh Wangen, et. al [9] karena cocok untuk membandingkan aktivitas dan proses dalam metode PRKI juga memberikan penilaian untuk kelengkapan metode PRKI [10]. Alasan lainnya adalah karena CURF sejalan dengan pedoman penilaian risiko di tempat studi kasus yang menyatakan proses penilaian risiko dibagi menjadi 3 proses, identifikasi risiko, estimasi risiko dan evaluasi risiko.

Untuk memilih metode PRKI yang akan dievaluasi menggunakan CURF, penulismenggunakan kriteria yang serupa dengan penelitian dari Wangen et, al (2017) untuk menentukan 10 metode PRKI yang akan dievaluasi, kriteria tersebut adalah sebagai berikut:

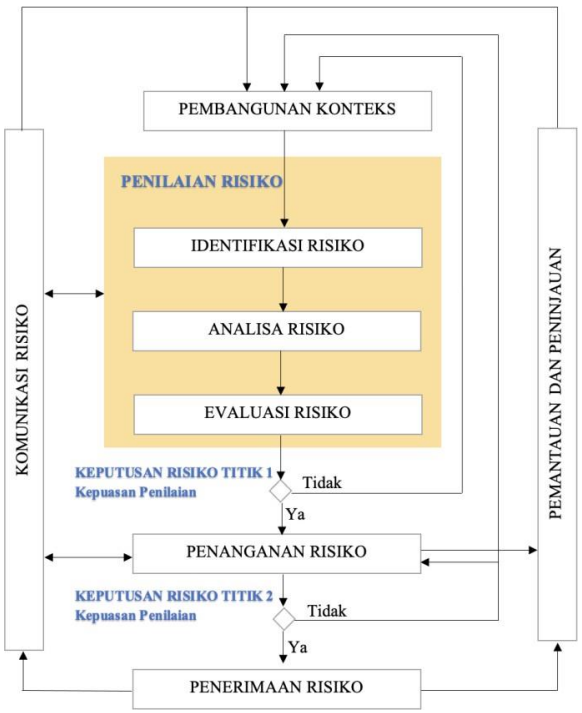
a. Disitasi lebih dari 50 kali di dalam literatur akademik
b. Merupakan industry best practice
c. Metode PRKI yang membahas topik tertentu: risiko insentif dan risiko privasi
d. Memiliki deskripsi dari identifikasi risiko, estimasi, Langkah-langkah evaluasi dan lain – lain
e. Tidak lebih tua dari lima belas tahun pada saat diulas

Penulis memilih CRAMM, FAIR, CIRA, CORAS, OCTAVE A, ISO 27005, RISK IT, NIST SP 800-30 dan RAIS dengan skor akhir dapat dilihat pada Tabel I. Hasil penilaian dibagi menjadi 3 proses, Identifikasi Risiko (IR) Estimasi Risiko (EsR) dan Evaluasi Risiko (EvR).

Untuk mendukung penggunaan metode ISO 27005 penulis melakukan studi literatur terdahulu dengan studi kasus yang berasal dari Indonesia. Dari beberapa penelitian ditemukan NIST SP 800-30 digunakan sebagai pelengkap proses analisa risiko pada ISO 27005 [11][12][13]

Tabel 2.1 . Evaluasi Metode PRKI Menggunakan CURF

Metode PRKI	IR	EsR	EvR	Total	Total Tanpa Output
CIRA	24	17	5	46	36
CORAS	33	12	3	48	34
CRAMM	29	10	4	58	43
FAIR	26	30	2	58	43
OCTAVE A	32	14	5	51	37
ISO 27005	38	27	3	68	51
RISK IT	29	22	4	55	42
NIST SP 800 30	24	26	2	52	38
RAIS	18	20	4	42	31



Gambar 2.1 Proses Manajemen Keamanan Informasi pada ISO 27005:2018

C. ISO 27005:2018

Berdasarkan hasil evaluasi menggunakan CURF pada studi yang dilakukan oleh Wangen (2017) [9], penulismenemukan bahwa ISO 27005 menerima skor tertinggi. ISO 27005 juga dapat digunakan sesuai dengan kondisi [11] untuk semua tipe organisasi [13].

ISO 27005:2018 adalah sebuah standar internasional untuk MRKI yang dibangun oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commissio*n (IEC). Menyediakan pedoman untuk penilaian risiko keamanan informasi di dalam sebuah organisasi, terutama penilaian risiko berdasarkan ISO/ IEC 27001 [8]. Hal ini sesuai dengan PT XYZ yang wajib dan sudah bersertifikasi ISO 27001 sebagai perusahaan penyedia transaksi melalui internet.

Penilaian Risiko pada ISO 27005, digambarkan dengan persegi berwarna kuning pada Gambar I, merupakan proses inkremental yang dimulai dari Identifikasi Risiko hingga Evaluasi Risiko. Artinya jika penilaian risiko tidak memenuhi penilaian yang memuaskan maka perlu dilakukan penilaian kembali dimulai dari penetapan konteks hingga akhir proses penilaian risiko sampai memenuhi kondisi yang memuaskan.

Langkah awal pada proses penilaian risiko adalah penetapan konteks. Ada dua hal yang perlu ditetapkan dalam langkah ini, kriteria dasar dan batasan. Kriteria diperlukan untuk memutuskan apa saja yang akan dievaluasi, apa dampaknya dan apa penerimaan risiko pada proses penilaian risiko. Batasannya adalah memutuskan ruang lingkup proses penilaian risiko.

Ada tiga proses utama dalam penilaian risiko berdasarkan ISO 27005, yaitu:

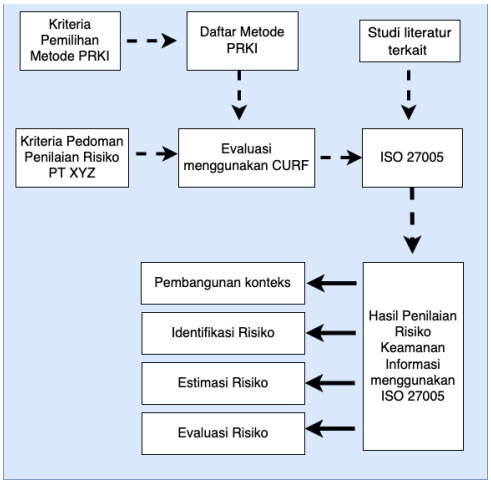
1. Identifikasi Risiko: Proses yang dijalankan untuk mengidentifikasi aset, ancaman, kontrol dan kerentanan.
2. Analisa Risiko: Adalah proses untuk menentukan kemungkinan dan dampak dari ancaman risiko keamanan informasi
3. Evaluasi Risiko: Proses evaluasi risiko untuk dipetakan dengan rangkaian penanganan risiko

D. NIST SP 800-30

NIST SP 800-30 revisi 1 digunakan untuk memberikan pedoman penilaian risiko keamanan informasi untuk organisasi dan pemerintah sebagai pelengkap pedoman NIST SP 800-39 [14]. NIST SP 800-30 dapat digunakan untuk melengkapi proses penilaian risiko pada ISO 27005. Langkah-langkah dalam penilaian risiko berdasarkan NIST SP 800-30 revisi 1 adalah, Identifikasi sumber ancaman, identifikasi kejadian ancaman, identifikasi kerentanan, penentuan kemungkinan , dan penentuan dampak.

3. Metodologi Penelitian

Kerangka teoretis untuk penelitian ini dihasilkan berdasarkan studi literatur yang mewakili alur studi teori-teori yang relevan, seperti yang ditunjukkan pada Gambar II. Proses penilaian risiko dalam ISO 27005 yang diimplementasikan dalam studi dengan kombinasi dengan NIST SP 800-30 untuk melengkapi proses evaluasi risiko.



Gambar 3.1 Kerangka Teoretis

1. Metode Pengumpulan Data

   a. Data Primer
   Data primer dikumpulkan melalui proses wawancara, *Focus Group Discussion* (FGD) dan Observasi. Wawancara dilakukan dengan narasumber *IT Security Manager*, *IT Security Team Leader*, dan *Engineering Manager*. Kegiatan FGD dilakukan dengan tim *IT Security*. Untuk pengumpulan data berupa observasi dilakukan terhadap *monitoring server* dan *reporting tools*. Data primer yang dikumpulkan terdiri dari daftar aset, ancaman, kontrol dan kerentanan berdasarkan objek penelitian.

   b. Data Sekunder
   Data sekunder adalah data yang diperoleh dari sumbernya tidak secara langsung. Data sekunder pada penelitian ini diperoleh dari studi dokumen SOP perusahaan dan studi literatur.

2. Analisis Data
   Proses analisa data primer dan data sekunder dilakukan berdasarkan proses Penilaian Risiko dari ISO 27005: 2018.

4. Hasil dan Pembahasan

Setelah semua data yang diperlukan terkumpul, penulismelakukan proses PRKI berdasarkan ISO 27005 mulai dari penetapan konteks hingga proses evaluasi risiko.

A. Pembangunan Konteks

1. Kriteria Dasar
   a. Kriteria Evaluasi Risiko: Penetapan evaluasi risiko pada penelitian ini menggunakan kriteria sebagai berikut:
      1) Proses informasi bisnis terkait dengan aplikasi OTA PT XYZ
      2) Tingkat kekritisan informasi dan aset proses bisnis yang terlibat
      3) Aset pendukung yang berhubungan dengan aplikasi OTA
      4) Kebijakan dan peraturan yang berlaku
   b. Kriteria Dampak: Kriteria probabilitas dan dampak ditentukan berdasarkan pedoman penilaian risiko perusahaan yang ditunjukkan pada tabel III dan IV. Untuk penilaian risiko ditentukan berdasarkan NIST SP 800-30 revisi 1 menggunakan pendekatan kuantitatif.
   c. Kriteria Penerimaan Risiko: ntuk kriteria penerimaan risiko pada penelitian ini berdasarkan pada pedoman perusahaan yaitu untuk risiko dengan skor maksimal 4.
2. Ruang Lingkup dan Batasan: Ruang lingkup penilaian risiko adalah untuk aplikasi OTA dan proses-proses utamanya, alat pendukung TI seperti perangkat keras dan perangkat lunak, serta semua personel TI yang terlibat.

B. Identifikasi Resiko

1. Identifikasi Aset
   Aset berdasarkan ISO 27005:2018 dibagi menjadi aset utama dan aset pendukung. Aset utama adalah aset yang memiliki dampak besar jika terkena risiko seperti kegagalan proses bisnis, gagal mematuhi aturan pemerintah, kehilangan modal, dan kehilangan kepercayaan pelanggan. Aset pendukung adalah aset-aset yang mendukung berjalannya proses bisnis Aplikasi OTA.

Tabel 4.1 Ringkasan Identifikasi Aset

Aset	Tipe	Total
Utama	Proses Bisnis(PB)	31
	Informasi (In)	18
Pendukung	Teknologi (Te)	13
	Manusia (Ma)	8
Total		70

Tabel 4.2 Ringkasan Identifikasi Ancaman

No	Tipe Ancaman	Tipe Aset	Sumber	Total
1	Kegagalan Fungsi	Bisnis Proses, Teknologi	D, A	15
2	Transaksi Palsu	Informasi	D	3
3	Serangan Eksternal	Teknologi	D	5
4	Kerahasiaan Data	Informasi	A	2
5	Integritas Data	Informasi	D, A	3
6	Ketersediaan Data	Informasi	D, A, E	2
7	Lingkungan	Teknologi, Manusia	E	1
8	Manajemen Proyek	Bisnis Proses, Teknologi, Manusia	A	3
Total				34

Tabel 4.3 Ringkasan Identifikasi Kontrol

No.	Aspek Keamanan Informasi	Total
1.	Proses Bisnis	5
2.	Informasi	6
3.	Teknologi	16
4.	Manusia	6
5.	Manajemen Proyek	1

Aset utama terdiri dari semua proses bisnis yang dijalankan pada aplikasi OTA seperti pencarian tiket, pembayaran, pengembalian dana, dan lain-lain dan informasi yang dikumpulkan dari proses bisnis tersebut seperti data pelanggan, data transaksi, dan lain-lain. Aset Pendukung adalah daftar aset yang mendukung bisnis proses seperti teknologi dan manusia. Ringkasan identifikasi aset dapat dilihat pada Tabel 4.1

2. Identifikasi Ancaman
Pada proses identifikasi ancaman, penulismengelompokkan ancaman menjadi 8 jenis yaitu: kegagalan fungsi, transaksi palsu, serangan eksternal, kerahasiaan data, integritas data, ketersediaan data, lingkungan, dan manajemen proyek. Sumber ancaman pada ISO 27005 diklasifikasikan menjadi 3, disengaja (*Deliberate*) (D), tidak disengaja (*Accident*) (A), dan lingkungan (*Environment*) (E). Daftar ancaman dibuat pada setiap aset berdasarkan jenis ancaman, sumber, dan agen ancaman. Ringkasan identifikasi aset dapat dilihat pada Tabel 4.2

3. Identifikasi Kontrol
Setelah ancaman terhadap setiap aset diidentifikasi, penulismengidentifikasi kontrol yang ada saat ini pada setiap aset berdasarkan 5 aspek, yaitu proses bisnis, informasi, teknologi, manusia, dan manajemen proyek. Penulismengidentifikasi total 29 kontrol berdasarkan aset yang diidentifikasi. Rangkuman identifikasi kontrol pada aplikasi OTA PT XYZ bisa dilihat pada Tabel 4.3

4. Identifikasi Kerentanan
   Kerentanan diidentifikasi dengan menganalisis ancaman mana yang tidak diselesaikan oleh kontrol saat ini pada setiap aset. Penulismengidentifikasi 34 kerentanan pada aplikasi OTA.

C. Estimasi Resiko

1. Tingkatan Probabilitas dan Dampak
   Tingkatan probabilitas dan dampak yang digunakan proses PRKI Aplikasi OTA pada penelitian ini berdasarkan pada dokumen Pedoman Penilaian Risiko PT XYZ. Tingkatan probabilitas yang dideskripsikan pada Tabel V diurutkan dari tingkatan terendah (tidak mungkin) sampai ke tingkat paling tinggi (hampir pasti). Tingkatan dampak yang dapat dilihat pada tabel 4.5 berdasarkan pada area dampak dari risiko. Area dampak terdiri dari:
   a. dampak pada pelanggan
   b. biaya keuangan
   c. Kesehatan dan keselamatan
   d. Kerusakan reputasi,
   e. kepatuhan hukum, kontrak dan organisasi

   Tingkatan dampak diurutkan dari tingkat terendah (dapat diabaikan) sampai tertinggi (sangat tinggi). Setelah tingkatan probabilitas dan dampak ditentukan dibuatlah sebuah matriks dari probabilitas dan dampak untuk menentukan urgensi dari risiko yang digambarkan pada Gambar 4.1. Risiko dengan urgensi rendah seperti yang ditunjukkan pada bagian hijau pada area matriks adalah risiko yang bisa diterima oleh perusahaan sedangkan risiko dengan urgensi sedang dan tinggi yang digambarkan pada warna kuning dan merah adalah risiko-risiko yang harus dimitigasi oleh sistem MRKI di PT XYZ

2. Analisa Resiko
   Analisa risiko dilakukan dengan menggunakan metode kualitatif berdasarkan metode NIST SP 800-30 setiap ancaman dianalisis berdasarkan nilai probabilitas dan dampak dari ancaman tersebut. Hasil analisa risiko menghasilkan 2 risiko dengan level tinggi, 79 risiko dengan level rendah dan 67 risiko dengan level rendah.

Tabel 4.4 Tingkat Probabilitas

Peringkat	Kemungkinan	Deskripsi
1	Tidak mungkin	Risiko belum pernah terjadi sebelumnya dan tidak pernah memikirkan seperti itu
2	Kemungkinan kecil	Ada kemungkinan risiko bisa terjadi, namun bisa juga tidak mungkin terjadi
3	Mungkin	Risiko lebih mungkin daripada tidak
4	Kemungkinan besar	Besar kemungkinan risiko akan terjadi baik berdasarkan history masa lalu atau kejadian/ keadaan saat ini
5	Hampir pasti	Risiko sudah terjadi atau diyakini risiko akan segera terjadi

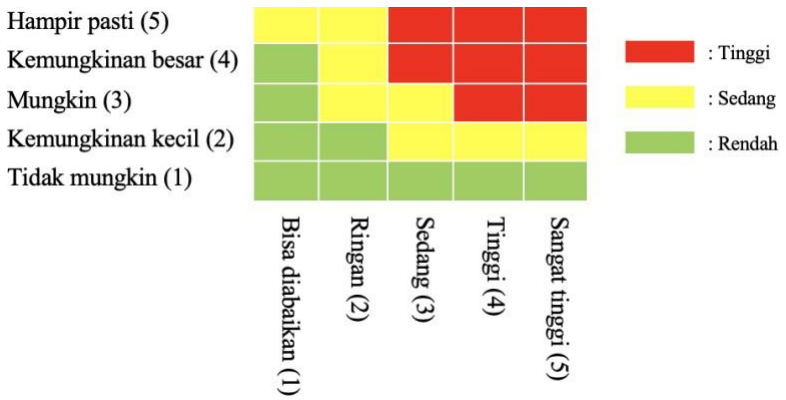
Tabel 4.5 Resiko Dampak

Peringkat	Dampak	Pada Pelanggan	Biaya Keuangan	Kerusakan Reputasi	Kepatuhan hukum, kontrak dan organisasi
1	Dapat diabaikan	Tidak Ada	Sangat sedikit atau tidak ada sama sekali	Dapat diabaikan	Tidak ada implikasi
2	Ringan	Beberapa gangguan lokal pada operasi, bisnis normal	Beberapa biaya lokal	Ringan	Risiko kecil tidak terpenuhinya kepatuhan
3	Sedang	Masi dapat memberikan produk/ layanan dengan beberapa kesulitan	Tidak dikehendaki tapi bisa ditanggung	Sedang	Pasti berisiko beroperasi secara ilegal
4	Tinggi	Bisnis Lumpuh di area utama	Efek besar pada pendapatan dan/ atau laba	Tinggi	Beroperasi secara ilegal di beberapa area
5	Sangat Tinggi	Bangkrut, tidak ada layanan pada pelanggan	Lumpuh, organisasi bangkrut	Sangat tinggi	Denda yang besar dan kemungkinan berakhir di penjara

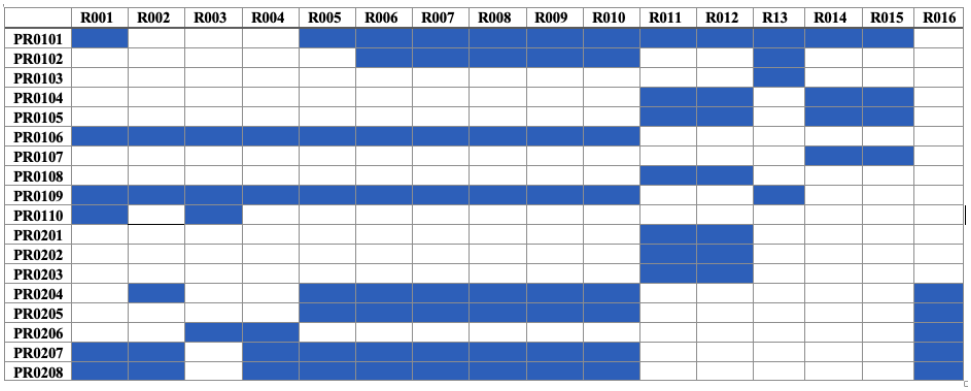
D. Evaluasi Resiko

Setelah mengurutkan risiko hasil proses analisa risiko berdasarkan skor, kemudian penulis mengelompokkan ancaman yang serupa menjadi satu risiko sehingga menghasilkan 16 risiko yang harus ditangani, yaitu 2 risiko tinggi dan 14 risiko dengan level sedang

Ada empat pilihan dalam menangani risiko dalam ISO 27005:2018, yaitu pengurangan (*reduction*), pemindahan (*transfer*), menghindari (*avoidance*), dan mempertahankan (*retention*) risiko [3]. Penulismengusulkan 18 penanganan risiko, 10 penanganan risiko pada aspek teknologi dan 8 penanganan risiko pada aspek organisasi. Hasil evaluasi risiko ditampilkan sebagai peta risiko dan penanganan risiko bisa dilihat pada Gambar 4.1 dan 4.2 berikut ini:



Gambar 4.1 Peta Resiko



Gambar 4.2 Penanganan Resiko

5. Penutup

5.1. Kesimpulan

Untuk menjaga keberlanjutan Aplikasi OTA, MRKI di PT XYZ perlu mengatasi semua potensi risiko yang dapat mengganggu aplikasi OTA menjalankan fungsinya. Pada penelitian ini, kami mencoba untuk mengatasi masalah tersebut dengan menemukan metode apa yang terbaik yang dapat digunakan untuk menilai risiko keamanan informasi untuk aplikasi OTA dan penanganan apa yang dapat diberikan untuk setiap risiko yang dievaluasi menggunakan metode PRKI yang dipilih.

Dari penelitian ini ditemukan bahwa kita dapat menggunakan kerangka evaluasi PRKI yang ada untuk mengevaluasi daftar metode PRKI yang dihasilkan dari kriteria yang dipilih. Kami memilih CURF untuk mengevaluasi metode ISRA berdasarkan kelengkapan karena juga sejalan dengan pedoman penilaian risiko perusahaan. Dengan membandingkan metode PRKI yang dipilih menggunakan CURF, kami memutuskan untuk menggunakan metode ISRA dengan skor tertinggi, ISO 27005:2018 sebagai metode ISRA yang paling sesuai untuk menjalankan proses penilaian risiko pada PT XYZ.

Untuk menguatkan keputusan penggunaan ISO 27005:2018 sebagai metode PRKI untuk PT XYZ, kami mempelajari literatur akademis terdahulu mengenai ISO 27005:2018, termasuk studi kasus di Indonesia. Dari penelitian sebelumnya kami menemukan bahwa NIST SP 800-30 banyak digunakan untuk melengkapi proses PRKI pada ISO 27005. Pedoman penilaian risiko keamanan informasi pada ISO 27005 yang berdasarkan pada ISO 27001 juga menjadi faktor pendukung untuk digunakannya ISO 27005 pada penelitian ini.

Dengan menggunakan ISO 27005:2018 untuk menjalankan PRKI pada aplikasi OTA di PT XYZ, kami menemukan ada 16 risiko yang harus ditangani. Berdasarkan penanganan risiko yang kami ajukan, dihasilkan peta penanganan risiko dengan penanganan risiko. Kami berharap hasil evaluasi risiko bisa digunakan sebagai masukan dalam perancangan MRKI di tempat studi kasus sehingga Aplikasi OTA bisa berjalan lancar sehingga proses bisnis di PT XYZ tidak terganggu.

Daftar Pustaka

[1] Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2017). Cyber risk assessment and mitigation (CRAM) framework using logit and Probit models for Cyber Insurance.

[2] Information Systems Frontiers, 21(5), 997–1018

[3] Inversini, A., & Masiero, L. (2014). Selling rooms online: The use of social media and online travel agents. International Journal of Contemporary Hospitality Management, 26(2), 272–292.

[4] Werthner, H. and Ricci, F. (2004), "E-commerce and tourism", Commun. ACM, Vol. 47 No. 12, pp. 101-105.

[5] Buhalis, D. and Law, R. (2008), "Progress in information technology and tourism management: 20 years on and 10 years after the internet – the state of etourism research", Tourism Management, Vol. 29 No. 4, pp. 609-623.

[6] Xiang, Z., Wo¨ber, K. and Fesenmaier, D.R. (2008), "Representation of the online tourism domain in search engines", Journal of Travel Research, Vol. 47 No. 2, pp. 137-150

[7] Inversini, A. and Buhalis, D. (2009), "Information convergence in the long tail: the case of tourism destination information", in Ho¨pken, W., Gretzel, U. and Law, R. (Eds), Information and Communication Technologies in Tourism 2009, Springer, Vienna, pp. 381-392

[8] Lee, H. "A., Denizci Guillet, B., & Law, R. (2012). An examination of the relationship between online travel agents and hotels. Cornell Hospitality Quarterly, 54(1), 95–107.

[9] ISO/IEC, "International Standard ISO/IEC 27005: 2018," International Organization for Standardization, London, 2018.

[10] Wangen, G., Hallstensen, C., & Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness. International Journal of Information Security J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[11] Liao, Z., Nazir, S., Khan, H. U., & Shafiq, M. (2021). Assessing security of software components for internet of things: A systematic review and Future Directions. Security and Communication Networks, 2021, 1–22..

[12] Sensuse, D. I., Syahrizal, A., Aditya, F., & Nazri, M. (2020). Information security risk management planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik. 2020 Fifth International Conference on Informatics and Computing (ICIC).

[13] Putra, I. M., & Mutijarsa, K. (2021). Designing information security risk management on Bali Regional Police Command Center based on ISO 27005. 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)

[14] Fikri, M. A., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. Procedia Computer Science, 161, 1206-1215

[15] NIST, "NIST SP 800-30 Revision 1: Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg,