Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Risk Assessment Keamanan Informasi dengan Menggunakan ISO/IEC 27001: Studi Kasus PT Dyandra Promosindo

Mahansa Putra[1], Rizal Fathoni Aji[2]
[1,2]Universitas Indonesia, Indonesia
e-mail: [1]mahansa.putra11@ui.ac.id, [2]rizal@cs.ui.ac.id

Abstract

PT Dyandra Promosindo is a company that operates in the event organizer sector, when carrying out their daily business processes they will always be in contact with important information from their clients. Therefore, it is necessary to carry out a risk assessment to avoid loss of confidentiality, integrity and availability of an information asset. The author wants to know how big the risk impact that threatens the security of information assets and provide control recommendations over these assets. The risk assessment process can be divided into three stages, namely, risk identification through interviews and document review, risk analysis using asset valuation and vulnerability and threat ratings, and finally risk evaluation using risk impact measurements. The results of this research showed that 10 critical information assets were identified and only 1 was in the Tolerable risk mitigation group where the other assets were in the Acceptable group. Recommendations for controls for PT Dyandra Promosindo information assets risk based on Annex A ISO/IEC 27001:2022 show 15 controls consisting of 4 Organizational control, 5 People control, 1 Physical control, and 5 Technological control

Keywords*: Risk Assessment, Asset Valuation, Information Security, ISO 27001*

Abstrak

PT Dyandra Promosindo merupakan perusahaan yang bergerak dibidang event organizer, dimana dalam menjalankan proses bisnisnya sehari-hari pasti akan selalu berhubungan dengan informasi penting dari klien mereka. Oleh karena itu perlu dilakukan risk assessment untuk menghindari hilangnya confidentiality, integrity dan availability dari suatu aset informasi. Penulis ingin mengetahui seberapa besar dampak risiko yang mengancam keamanan aset informasi dan memberikan rekomendasai kontrol pada aset tersebut. Proses risk assessment dapat dibagi menjadi tiga tahapan yaitu, risk identification secara interview dan peninjauan dokumen, risk analysis dengan menggunakan asset valuation dan vulnerability and threat rating, dan terakhir risk evaluation menggunakan pengukuran risk impact. Hasil dari penelitian ini didapatkan 10 aset informasi kritis yang teridentifikasi dan hanya 1 yang masuk ke kelompok mitigasi risiko Tolerable dimana aset-aset lainnya dikelompok Acceptable. Rekomendasi kontrol untuk risiko aset informasi PT Dyandra Promosindo yang berdasarkan pada Annex A ISO/IEC 27001:2022 didapatkan 15 kontrol, yang terdiri dari 4 Organizational control, 5 People control, 1 Physical control, dan 5 Technological control.

Kata kunci*: Risk Assessment, Asset Valuation, Keamanan Informasi, ISO 27001*

1. PENDAHULUAN

Seiring berkembangnya teknologi, pengguna layanan internet atau perangkat teknologi juga akan mengalami peningkatan. Yang mengakibatkan pertukaran informasi meningkat maupun itu dalam ranah perorangan atau secara besar dan luas seperi pada suatu lingkungan perkantoran. Terutama pada suatu perusahaan sangatlah diperlukan adanya suatu perencanaan terkait keamanan informasi. Salah satu langkah pertama dalam perencanaan strategis keamanan informasi adalah dilakukannya manajemen risiko dan evaluasi risiko [1]. Ancaman terhadap sistem

informasi termasuk kerusakan peralatan, gangguan alam, kesalahan manusia atau perangkat, dan serangan dengan sengaja yang biasanya canggih, disiplin, terorganisir, dan terdanai. Ketika berhasil, serangan pada sistem informasi dapat berdampak serius atau kerusakan berat pada operasi dan aset organisasi, individu, organisasi lain, dan negara [2].

PT Dyandra Promosindo merupakan perusahaan yang bergerak dibidang event organizer (EO) sejak 1994 dan telah mengorganisir lebih dari 1100 pameran di Jakarta, Surabaya, Yogyakarta, dan kota besar lainnya. Perusahaan ini menyediakan jasa EO untuk segala macam acara termasuk pameran Business to Business (B2B), pameran Business to Customer (B2C), festival musik, konferensi, dan summit [3]. Dalam pengelolaan aset informasi PT Dyandra Promosindo menggunakan beberapa aplikasi sistem informasi seperti E-Procurement, SI untuk CRM, sistem rancangan anggaran biaya project, dan aplikasi on-site. Tentunya pada setiap aplikasi tersebut yang dalam penggunaannya dapat memunculkan risiko-risiko yang dapat berdampak merugikan. Dan juga pernah ada insiden terkait kehilangan data yang diakibatkan oleh adanya salah satu staff yang dengan sengaja mengambil dan menghapus data-data penting termasuk data klien yang membuat perusahaan mengalami kerugian.

Dalam konteks sebuah perusahaan event organizer, lingkup risik untuk aset informasi sangatlah dinamis dan beragam. Mengingat sifat industri ini, yang melibatkan penanganan jumlah besar data sensitif mulai dari detail kilen hingga logistik acara, potensi dampak pelanggaran keamanan sangatlah signifikan. Keamanan informasi menjadi hal terpenting untuk menjaga kepercayaan klien, melindungi rencana acara, dan memastikan kelancaran pelaksanaan acara. Risiko termasuk akses yang tidak sah pada set informasi, kebocoran informasi klien, dan/atau gangguan pada sistem penting selama pelaksanaan acara.

Untuk mengatasi tantangan ini, perusahaan harus merumuskan kebijakan keamanan informasi yang dirancang khusus untuk mempertimbangkan risiko terkait dengan operasinya. Kebijakan ini, dapat dibuat dengan bantuan oleh standar internasional seperti ISO 27001, yang menjadi kunci utama dalam memitigasi risiko secara efektif. ISO 27001 menekankan perlunya proses penilaian risiko (Clause 6) yang disesuaikan dengan konteks organisasi. Melakukan penilaian risiko menyeluruh memungkinkan perusahaan mengidentifikasi, menganalisis, dan memprioritaskan potensi ancaman terhadap aset informasinya, memberikan landasan untuk menerapkan kontrol yang ditargetkan [4].

Maka dari itu diperlukan adanya pengelolaan sistem keamanan informasi. Untuk menerapkan keamanan informasi dan mengurangi risiko pelanggaran keamanan, organisasi perlu mengambil langkah yang tepat untuk menjaga aset informasinya dan memastikan kontinuitas bisnis [5].

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode pengolahan data secara campuran (mixed methods) atau penggabungan antara teknik pengambilan data atau proses analisis secara kualitatif dan kuantitatif dalam penelitian yang sama [6]. Pengolahan data kualitatif dilakukan pada tahapan identifikasi aset informasi dan

risiko dengan melakukan wawancara terhadap individu yang bersangkutan dengan aset informasi. Pengolahan data secara kuantitatif dilakukan pada tahap selanjutnya yaitu penilaian Asset Valuation (AV), Vulnerability (V) and Threat (T) Rating, dan Likelihood (L). Penelitian ini juga menggunakan studi secara sequential exploratory dimana penelitian diawali secara kualitatif dan dilanjutkan dengan kuantitatif [6].

Penelitian ini menggunakan teknik sampling yang disebut purposive sampling dimana teknik ini dibutuhkan pertimbangan penulis untuk memilih cases yang cocok untuk menjawab pertanyaan penelitian dan sesuai dengan tujuan. Oleh karena itu teknik ini biasa disebut judgemental sampling [6]. Teknik ini biasa digunakan ketika dilakukan pada sampel yang sedikit seperti dalam penelitian studi kasus.

2.1. Identifikasi Aset dan Risiko

Tahapan identifikasi aset informasi beserta risikonya digunakan pertanyaan secara open-ended. Contoh pertanyaan tersebut dapat dilihat pada Tabel 1.

Tabel 1. Contoh pertanyaan Open-ended

Kategori	Pertanyaan
Aset Informasi	Apa saja aset informasi yang ada pada PT Dyandra?
Ancaman terhadap Aset Informasi	Berdasarkan aset informasi yang sudah disebutkan apa saja ancaman yang mungkin terjadi dan seberapa besar dampak dari ancaman terhadap proses bisnis?

2.2. *Asset Valuation*

Pertama penulis perlu menentukan nilai dari suatu aset informasi suatu organisasi berdasarkan keamanan CIA (*confidentiality, integrity, availability*). Kemudian nilai dari aset informasi dapat digabungkan dengan bobot dari suatu aset dengan asumsi nilai suatu aset ditentukan berdasarkan seberapa sensitif data yang yang ditampung [1]. Tiap variabel dari CIA memiliki tiga tingkatan dengan nilai yaitu: 3 untuk *high* berdampak parah, 2 untuk *medium* berdampak serius, dan 1 untuk *low* berdampak kecil pada operasi, aset atau individu pada organisasi. Rating tersebut memiliki kriteria yang dapat digunakan sebagai acuan sebagai berikut.

a) *Confidentiality*: adanya kebocoran informasi /data dapat berdampak...
b) *Integrity*: adanya perubahan atau kerusakan dari informasi/data dapat berdampak...
c) *Availability*: adanya gangguan dalam pengaksesan atau penggunaan dari informasi/data atau sistem informasi dapat berdampak...

Gambar 1 merupakan matriks CIA yang digunakan sebagai petunjuk dalam menentukan nilai dari suatu aset informasi. Contoh jika suatu aset informasi

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

memiliki nilai confidentiality low, integrity medium, dan availability high maka aset tersebut memiliki nilai sebesar 6.

	Confidentiality	Low (1)			Medium (2)			High (3)		
	Integrity	L	M	H	L	M	H	L	M	H
Availability	Low (1)	3	4	5	4	5	6	5	6	7
	Medium (2)	4	5	6	5	6	7	6	7	8
	High (3)	5	6	7	6	7	8	7	8	9

Gambar 1. Matriks CIA

Kemudian setiap aset perlu juga dinilai bobotnya yang dapat ditentukan berdasarkan sensitivitas dari data yang ada didalamnya. Sebagai contoh basis data yang berisi informasi pegawai mungkin memiliki nilai yang lebih kecil dibandingkan dengan basis data yang memiliki data transaksi pelanggan [1]. Bobot dari suatu aset dibagi menjadi tiga berdasarkan tujuan bisnis, yaitu 1 low (nilai data kecil/tidak ada), 2 medium (nilai data sedang), dan 3 high (nilai data penting).

Total Asset Value								
Asset Value		3	4	5	6	7	8	9
Weight	1	3	4	5	6	7	8	9
	2	6	8	10	12	14	16	18
	3	9	12	15	18	21	24	27

Gambar 2. Matriks Bobot Total Aset

Pada Gambar 2 dapat dilihat matriks bobot total aset dimana nilai terkecil 3 dan terbesar 27. Dalam tahap ini dapat kita kategorisasikan aset kedalam tiga tingkatan berdasarkan matriks tersebut. Kategori dari aset mengindikasikan *level of concern* yang perlu diberikan pada aset tersebut. Maka dari itu, diperlukan lebih banyak implementasi keamanan, investasi atau perhatian yang diberikan kepada kategori I aset (nilai aset total antara 20 dan 27) dibanding untuk kategori II aset (antara 12 dan 18) dan untuk kategori III (kurang dari 10) aset [1].

2.3. *Vulnerability and Threat Rating*

Vulnerability dan *threat rating* berisi mengenai seberapa rentan suatu sistem terhadap eksploitasi dari kelemahan yang dimiliki (*susceptibility*), potensi paparan kerugian terhadap akses penyerang pada *flow* (*exposure*), kemampuan suatu ancaman sukses dalam menyerang aset dengan memanfaatkan kerentanan (*capability*), dan dampak dari ancaman yang dapat mengakibatkan kerugian (*impact*). *Vulnerability* dan *threat* memiliki lima tingkat rating *very low (1), low (2), medium (3), high (4),* dan *very high (5)* seperti pada Gambar 3.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Susceptibility Rating	Exposure Rating		
	1	2	3
1	1	2	3
2	2	3	4
3	3	4	5

Gambar 3. Model untuk Vulnerability Rating

Model untuk penilaian *threat rating* menggunakan *impact* dan *capability* dari *threat*, sama seperti pada model *vulnerability rating* pada Gambar 3.4. Perbedaannya adalah pada *vulnerability rating* digunakan *susceptibility* dan *exposure* [1].

2.4. *Likelihood of Risk*

Selanjutnya penilaian terhadap probabilitas atau kemungkinan (*likelihood*) terjadinya suatu ancaman pada aset informasi. Kemungkinan terjadinya suatu ancaman dapat dinyatakan dalam istilah *probability of occurance*. Terdapat lima nilai yaitu:

a) 1 = *never happened* (tidak terjadi dalam tiga tahun terakhir)
b) 2 = *rare* (terjadi setahun sekali)
c) 3 = *periodic* (terjadi sekali selama tiga bulan)
d) 4 = *regular* (terjadi sekali dalam dua minggu)
e) 5 = *frequent* (terjadi sekali dalam seminggu)

2.5. Metode Pengolahan Data

Pengolahan data dalam penelitian ini menggunakan metode kualitatif pada wawancara dan *document review* serta kuantitatif, dimana hasil dari peniliaian aset dapat dijadikan suatu bilangan yang terhitung. Tahap pengolahan data kualitatif dilakukan pada hasil wawancara dan *document review* identifikasi aset informasi dan risiko yang bersangkutan. Aset informasi dan risiko yang telah teridentifikasi kemudian dapat dilakukan penilaian pada tiap komponen yang telah disebutkan sebelumnya pada metode pengumpulan data [1].

Pada penilaian CIA didapatkan output berupa *asset value* berupa penjumlahan nilai *confidentiality (C), integrity (I),* dan *availability (A)* beserta bobotnya. Yang kemudian dapat dihitung menjadi *total asset value* dengan menggunakan persamaan sebagai berikut:

$$Asset\ Value\ (AV) = C + I + A \quad (1)$$

$$Total\ Asset\ Value\ (TAV) = AV + Weight\ of\ Asset\ (W) \quad (2)$$

Selanjutnya pada kuesioner *vulnerability* dan *threat rating* didapatkan output berupa nilai *vulnerability severity (V)* dan *threat severity (T)*. Nilai tersebut beserta dengan *TAV* dikalikan untuk mendapatkan nilai *potential risk (PR)* sebagai berikut:

$$Potential\ Risk\ (PR) = TAV * V * T \quad (3)$$

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Kemudian pada kuesioner *likelihood (L)* didapatkan output berupa nilai kemungkinan suatu risiko mungkin terjadi. Nilai ini dikalikan dengan nilai *PR* untuk mendapatkan nilai *risk impact (RI)* sebagai berikut:

$$Risk\ Impact\ (RI) = PR * Likelihood\ (L) \quad (4)$$

Nilai dari *risk impact* dapat digunakan sebagai rencana mitigasi dari risiko yang dapat dibagi menjadi *acceptable, tolerable,* dan *intolerable risk* [1]. Dengan pengelompokkan nilai *risk impact*, *acceptable* kurang dari 540, *tolerable* diantara 540 hingga 1215, dan *intolerable* lebih dari 1215.

3. HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan mengenai hasil penelitian berupa indentifikasi aset informasi, penilaian dan pembobotan aset, penilaian kerentanan dan ancaman, dan pengukuran risk impact, rekomendasi strategi mitigasi risiko dan pembahasan mengenai hasil penelitian yang telah didapatkan.

3.1. Identifikasi Aset Informasi

Mengidentifikasi aset informasi pada PT Dyandra Promosindo dapat dilakukan dengan cara mengetahui terlebih dahulu aplikasi/sistem informasi/kontainer yang digunakan dalam proses bisnis perusahaan. Kontainer merupakan tempat dimana suatu aset informasi atau data "tinggal" atau berbagai jenis aset informasi yang disimpan, dipindah, atau diproses. Dilihat dari proses bisnis sistem informasi yang digunakan dimulai dari pelelangan suatu event atau saat pembuatan konsep sebuah event hingga pada akhirnya event tersebut berjalan dan dihadiri oleh banyak pihak seperti peserta dan pengunjung event adalah sebagai berikut:

a) Sistem informasi CRM (Customer Relationship Management) menggunakan Dynamics AX, data disimpan pada cloud.
b) Sistem informasi Project Management menggunakan Dynamics AX, data disimpan pada cloud.
c) Sistem informasi E-Procurement menggunakan DyandraKu, data disimpan pada server on-premise pada perusahaan.
d) Sistem informasi SDM (Sumber Daya Manusia), data disimpan pada server on-premise pada perusahaan.

Dari sistem informasi yang telah disebutkan selanjutnya dapat diidentifikasi aset informasi apa saja yang terdapat didalamnya dan juga kepemilikan dari aset tersebut.

Tabel 2. Daftar Aset Informasi

Aset Informasi	Aplikasi/Container	Owner(s)
Business relation/ Potential customer	SI CRM (Dynamics AX)	Divisi, IT Dept
Sales quotation		Divisi, IT Dept
Sales order	SI Project Management (Dynamics AX)	Finance, IT Dept
Journal Transaction Log		Divisi, IT Dept
Rencana Anggaran Biaya (RAB)		
Project analysis/ Gross margin		

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Aset Informasi	Aplikasi/Container	Owner(s)
Project activity report		
Quality supplier	*E-Procurement* (DyandraKu)	*Procurement,* IT Dept
Profil Karyawan	SI SDM	HR, IT Dept
Absensi Karyawan		

Dapat dilihat pada Tabel 2 terdapat 10 aset informasi dan kepemilikannya yang dapat diidentifikasi berdasarkan dari sistem informasi yang sebelumnya telah disebutkan. Setiap sistem informasi dapat memiliki lebih dari satu aset informasi yang ditampung.

3.2. Perhitungan dan Pembobotan Aset Informasi

Metode perhitungan *asset value* berdasarkan oleh keamanan CIA-nya (*Confidentiality, Integrity, Availability*) dengan penilaian dari *low (1), medium (2),* dan *high (3)* berdasarkan dari seberapa besar dampak terhadap operasional organisasi, aset, atau individu jika terganggunya keamanan CIA. Dapat dilihat kembali pada Subbab 2.2 terkait *asset valuation* serta Gambar 1 untuk matriks CIA. Setelah didapatkan nilai aset berdasarkan matriks CIA, selanjutnya perlu ditentukan *weight* atau bobot dari aset tersebut berdasarkan seberapa penting data yang disimpan terhadap tujuan bisnis.

Tabel 3. Perhitungan *Asset Value*

Aset Informasi	Matriks CIA			*Weight (W)*	*Total Asset Value (TAV)* (C+I+A) x W
	C	I	A		
Business relation/ Potential customer	3	3	2	3	24
Sales quotation	3	3	2	3	24
Sales order	3	3	2	3	24
Journal Transaction Log	3	3	2	3	24
Rencana Anggaran Biaya (RAB)	3	3	1	3	21
Project analysis/ Gross margin	3	3	3	3	27
Project activity report	3	3	3	3	27
Quality supplier	2	3	2	3	21
Profil Karyawan	2	2	1	2	10
Absensi Karyawan	1	2	1	1	4

Penilaian *asset value* dan pembobotan pada Tabel 3 dilakukan dengan bantuan narasumber serta dokumen pendukung PT Dyandra Promosindo. Penilaian dapat dilakukan dengan mengingat inti dari setiap poin *confidentiality, integrity* dan *availability*.

Tabel 4. Kategorisasi *Level of Concern* Aset Informasi

Level of Concern	Aset Informasi
Kategori I (nilai TAV 20-27)	*Business relation/Potential customer, Sales quotation, Sales order, Journal transaction log,* RAB, *Project analysis/Gross margin, Project activity report, Quality*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Level of Concern	**Aset Informasi**
	supplier
Kategori II (nilai TAV 12-18)	-
Kategori III (nilai TAV kurang dari 10)	Profil karyawan, Absensi karyawan

Berdasarkan nilai TAV yang didapatkan, maka aset dapat dikategorikan kedalam tiga *level of concern* seperti pada Gambar 2. Tabel 4 menunjukkan aset apa saja yang masuk kedalam kategori yang telah ditetapkan. Tujuan dari pengkategorian ini adalah untuk mengetahui aset mana saja yang memerlukan implementasi keamanan, *investment*, atau perhatian yang lebih.

3.3. Perhitungan Nilai *Vulnerability* dan *Threat Rating*

Dalam melakukan perhitungan nilai *vulnerability* menggunakan dua komponen penilaian yaitu *susceptibility* atau seberapa besar upaya yang diperlukan untuk dapat mengeksploitasi kelemahan dan *exposure* atau akses dari ancaman terhadap flow proses. Sedangkan untuk menghitung nilai *threat* menggunakan *capability* atau kemampuan dari *threat agent* beserta tingkat *effort* yang dibutuhkan untuk berhasil menyerang aset dan *impact* atau dampak/konsekuensi atau efek kuat dari ancaman terhadap proses bisnis/aset.

Tabel 5. Daftar Risiko

No.	***Risk***
1	*Human error,* seperti kesalahan menginput data
2	Penyebaran hak akses (*password*) aplikasi sistem informasi PT Dyandra Promosindo oleh staff yang memiliki hak akses
3	*Bug/error* yang muncul ketika staff IT melakukan *maintenance*
4	Eksploitasi celah keamanan pada aplikasi sistem informasi
5	Penyebaran/pencurian data *confidential* perusahaan oleh staff
6	*Malware* atau ransomware yang mempengaruhi sistem informasi
7	*Social engineer,* seperti *phishing*
8	Bencana alam dan lingkungan, seperti gempa bumi, kebakaran,

Demi memudahkan penilaian dapat terlebih dahulu menuliskan apa saja *risk* yang mengancam aset informasi secara *general*. Dengan mengetahui *risk* penilaian *vulnerability* dan *threat rating* dapat lebih akurat dan mudah karena bisa mengacu pada Tabel 5. Alasan risiko yang teridentifikasi tidak dinilai satu persatu karena untuk setiap aset informasi dapat terpengaruhi oleh seluruh risiko tersebut.

Tabel 6. *Vulnerability Rating*

Aset Informasi	***Susceptibility (S)***	***Exposure (E)***	***Vulnerability (V)***
Business relation/ Potential customer	2	3	4
Sales quotation	2	3	4
Sales order	2	2	3
Journal Transaction Log	2	2	3
Rencana Anggaran Biaya (RAB)	2	2	3

Aset Informasi	*Susceptibility (S)*	*Exposure (E)*	*Vulnerability (V)*
Project analysis/ Gross margin	2	2	3
Project activity report	2	2	3
Quality supplier	2	2	3
Profil Karyawan	1	1	1
Absensi Karyawan	1	1	1

Nilai *vulnerability* pada Tabel 6 didapatkan berdasarkan dari Gambar 3 model untuk *vulnerability rating.* Didapatkan nilai *vulnerability* paling besar yaitu 4 dan terendah 1. Selanjutnya untuk menghitung *threat rating* mirip seperti menghitung *vulnerability,* namun perbedaannya adalah *threat* menggunakan *impact* dan *capability* untuk menggantikan *susceptibility* dan *exposure*.

Tabel 7. *Threat Rating*

Aset Informasi	*Capability (C)*	*Impact (I)*	*Threat (T)*
Business relation/ Potential customer	2	3	4
Sales quotation	1	1	1
Sales order	2	3	4
Journal Transaction Log	2	2	3
Rencana Anggaran Biaya (RAB)	2	3	4
Project analysis/ Gross margin	2	3	4
Project activity report	2	3	4
Quality supplier	1	2	2
Profil Karyawan	1	1	1
Absensi Karyawan	2	1	2

Selanjutnya menilai *threat rating*, hasil dapat dilihat pada Tabel 4.6. Untuk mendapatkan nilai *threat* sama seperti penilaian *vulnerability* yaitu menggunakan model pada Gambar 3.

3.4. *Probability* atau *Likelihood* dari Risiko

Dalam menentukan nilai *probability* dilihat dari estimasi frekuensi munculnya *threat*. Nilai *probability* memiliki skala dari 1 – 5, dimana 1 mendeskripsikan *threat* tidak pernah terjadi selama tiga tahun terakhir, hingga 5 mendeskripsikan *threat* terjadi satu minggu sekali.

Tabel 8. *Probability Value*

Aset Informasi	*Probability (P)*
Business relation/ Potential customer	2
Sales quotation	1
Sales order	1
Journal Transaction Log	1
Rencana Anggaran Biaya (RAB)	1
Project analysis/ Gross margin	1
Project activity report	1
Quality supplier	1

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Aset Informasi	*Probability (P)*
Profil Karyawan	1
Absensi Karyawan	1

Berdasarkan nilai *probability* yang didapat, hanya aset *business relation/potential customer* yang bernilai 2, hal ini disebabkan oleh insiden yang pernah terjadi terkait hilangnya *integrity* aset informasi oleh staf yang sudah *resign* namun masih memiliki akses ke sistem perusahaan. Aset informasi lainnya hanya bernilai 1 dikarenakan aset-aset tersebut belum pernah terjadi insiden sepengetahuan narasumber.

3.5. Perhitungan *Risk Impact*

Perhitungan *risk impact* membutuhkan dua komponen yaitu *potential risk* dan *probability*. *Potential risk* didapatkan dari perhitungan yang sudah dilakukan sebelumnya yaitu *total asset value, vulnerability,* dan *threat*. Kemudian nilai tersebut dikalikan dengan nilai probabilitas untuk mendapatkan hasil berupa nilai *risk impact*.

Tabel 9. *Risk Impact Value*

Aset Informasi	*Total Asset Value*	*Vulnerability*	*Threat*	*Potential Risk*	*Probability*	*Risk Impact Value*
Business relation/ Potential customer	24	4	4	384	2	768
Sales quotation	24	4	1	96	1	96
Sales order	24	3	4	288	1	288
Journal Transaction Log	24	3	3	216	1	216
Rencana Anggaran Biaya (RAB)	21	3	4	252	1	252
Project analysis/ Gross margin	27	3	4	324	1	324
Project activity report	27	3	4	324	1	324
Quality supplier	21	3	2	126	1	126
Profil Karyawan	10	1	1	10	1	10
Absensi Karyawan	4	1	2	8	1	8

Berdasarkan hasil pada Tabel 9 nilai *risk impact* kemudian dapat dikelompokkan untuk menentukan perlakuan mitigasi risiko setiap aset informasi. Terdapat tiga perlakuan mitigasi risiko yaitu *acceptable, tolerable,* dan *intolerable*.

3.6. Implementasi Kontrol

Hasil dari perhitungan *risk impact* dan pengelompokkan opsi *risk mitigation* selanjutnya risiko aset informasi akan direkomendasikan respons terhadap risiko dan diimplementasikan *control* yang digunakan untuk mengendalikan, mengatur, atau mengurangi ancaman terhadap aset, yang mana *control* tersebut dapat bersifat *corrective* (memperbaiki), *detective* (mendeteksi), atau *preventive* (mencegah).

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 8 Nomor 1, Maret 2024, pp. 159-170
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Tabel 10. Implementasi *Control*

Risk	***Risk Response***	***Controls (Annex A)***
Human error, seperti kesalahan menginput data	○ Membuat pengecekan otomatis validasi data ○ Membuat SOP terkait proses penginputan data kritis dan sensitif. ○ Menerapkan verifikasi dua orang untuk melakukan *cross-check* keakuratan pada informasi yang diinput	○ *5.1 Policies for information security* ○ *5.4 Management responsibilities*
Penyebaran hak akses (*password*) aplikasi sistem informasi PT Dyandra Promosindo oleh staff yang memiliki hak akses	○ Mengadakan *security awareness training* sebagai edukasi karyawan pentingnya menjaga *access credentials* ○ Mengimplementasi autentikasi *multi-factor*	○ *5.15 Access control* ○ *5.18 Access rights* ○ *6.3 Information security awareness, education, and training* ○ *8.5 Secure authentication*
Bug/error yang muncul ketika staff IT melakukan *maintenance*	○ Memprioritaskan *testing* dan *quality assurance* sebelum mengimplementasikan perubahan. ○ Memiliki *rollback plan* jika terjadi isu kritis	○ *8.13 Information backup* ○ *8.29 Security testing in development acceptance*
Eksploitasi celah keamanan pada aplikasi sistem informasi	○ Kerjasama dengan vendor atau penyedia jasa untuk selalu mengupdate dan menginfokan terkait kerentanan ○ Melakukan *vulnerability scanning* dan *penetration test*	○ *8.9 Configuration Management* ○ *8.29 Security testing in development acceptance* ○ *8.34 Protection of information systems during audit testing*
Penyebaran/pencurian data *confidential* perusahaan oleh staff	○ Mengecek riwayat pegawai sebelum dipekerjakan ○ Membuat *exit procedures* ○ Mengkomunikasikan konsekuensi secara *legal*	○ *6.1 Screening* ○ *6.2 Terms and conditions of employment* ○ *6.4 Disciplinary process* ○ *6.5 Responsibilities after termination or change of employment*
Malware atau ransomware yang mempengaruhi sistem informasi	○ Secara berkala memperbarui perangkat dan *patch keamanan* ○ Melakukan penetration testing	○ *8.9 Configuration management* ○ *8.29 Security testing in development acceptance* ○ *8.34 Protection of information systems during audit testing*
Social engineer, seperti *phishing*	○ Mengadakan training awareness terhadap *social engineering, phishing scam,* dan verifikasi kepada individu yang tidak diketahui	○ *6.3 Information security awareness, education, and training*
Bencana alam dan lingkungan, seperti gempa bumi,	○ Membuat dan memperbarui secara berkala emergency response plan	○ *7.5 Protecting against physical and environmental threats*

Risk	*Risk Response*	*Controls (Annex A)*
kebakaran,	○ Membuat contingency plan untuk alternatif venue event	

4. SIMPULAN

Berdasarkan hasil yang diperoleh, teridentifikasi aset informasi kritis berjumlah 10 aset yaitu *Business relation/Potential customer, Sales quotation, Sales order, Transaction Log/Journal,* Rancangan Anggaran Biaya (RAB), *Project Gross margin, Project Activity report, Quality supplier*, Profil Karyawan, dan Absensi karyawan. Aset-aset informasi tersebut berada didalam kontainer sistem informasi CRM (Dynamics AX), *Projcet Management (Dynamics AX)*, *Procurement (DyandraKu),* dan SDM. Aset informasi tersebut kemudian dihitung nilai *Total Asset Value* dan *Probability of Occurance*-nya untuk mendapatkan nilai *Risk Impact* dari setiap aset informasi. Nilai TAV untuk mayoritas aset informasi selain Profil dan Absensi karyawan termasuk besar dikarenakan jika risiko terjadi pada aset tersebut akan berdampak cukup besar pada proses bisnis serta reputasi dan kepercayaan mitra, *supplier,* relasi bisnis dan *customer*. Namun *Probability of Occurance* untuk setiap aset hanya 1 dan paling besar yaitu pada aset *Business relatian* yaitu 2, dalam skala 1-5 yang mengakibatkan nilai *Risk Impact* menjadi kecil. Pada rekomendasi kontrol didapatkan 15 kontrol yang dapat dilihat pada Tabel 5.10 dan 5.11, yang terdiri dari 4 *Organizational control*, 5 *People control, 1 Physical control,* dan 5 *Technological control.* Kontrol tersebut dijadikan rekomendasi berdasarkan dari *risk response* untuk setiap risiko.

DAFTAR PUSTAKA

[1] S. G. Kassa, "IT Asset Valuation, Risk Assessment and Control Implementation Model," *ISACA J.*, vol. 3, pp. 1–9, 2017.
[2] NIST, "NIST Special Publication 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations," pp. 229–270, 2017.
[3] Dyandra & Co, "https://www.dyandra.com/about." .
[4] the International Organization for Standardization, "ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements," 2022.
[5] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis," *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 87–100, 2021.
[6] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, vol. 195, no. 5. 2018.