SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK IV - Surabaya, 27 April 2024
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2024.5835

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Penilaian Risiko Keamanan Informasi Menggunakan Standar NIST SP 800-30 pada PT.XYZ

Aminatuz Zuhriyah, Adib Pakarbudi

Sistem Informasi, Institut Teknologi Adhi Tama Surabaya
e-mail: aminatuzuhriyah.edu@gmail.com

ABSTRACT

Information systems are things that need to be managed well by companies because companies can run optimally if they implement an information security system to maintain the business they run. PT. XYZ is a company that implements information systems in its business processes. This research aims to analyze, identify and mitigate risks that occur in each company asset, especially in raw material production planning system assets at PT. PT. After conducting an analysis using the NIST SP 800-30 standard, it was found that the raw material production planning system assets at PT. Therefore, mitigation needs to be carried out in the form of implementing system security and software security updates that are updated regularly with the latest security patches to overcome risk vulnerabilities as well as using intrusion detection tools to monitor suspicious activity in the network and system.

Keywords: *Information Systems, Information Security, Risk Assessment, NIST SP 800-30, Risk Mitigation.*

ABSTRAK

Sistem informasi merupakan hal yang perlu dikelola dengan baik oleh perusahaan dikarenakan perusahaan dapat berjalan secara optimal jika menerapkan sistem keamanan informasi guna mempertahankan bisnis yang dijalankan. PT. XYZ merupakan perusahaan yang menerapkan sistem informasi dalam proses bisnisnya. Penelitian ini bertujuan untuk menganalisis, mengidentifikasi dan memitigasi risiko yang terjadi pada tiap aset perusahaan terlebih khusus pada aset sistem perencanaan produksi bahan baku di PT.XYZ menggunakan standar NIST SP 800-30. PT.XYZ mengalami kebobolan data berupa terjadinya risiko web spoofing sehingga perusahaan kehilangan data perencanaan produksi bahan baku. Setelah dilakukan analisa dengan penerapan standar NIST SP 800-30 didapat hasil bahwa aset sistem perencanaan produksi bahan baku di PT.XYZ memiliki kemungkinan sangat jarang dengan nilai likelihood sebesar 0,015 namun didapati

dampak yang sangat besar sehingga tergolong kedalam risiko level tinggi. Oleh karena itu, perlu dilakukan mitigasi berupa penerapan pengamanan sistem dan pembaruan keamanan perangkat lunak yang diupdate secara berkala dengan patch keamanan terbaru untuk mengatasi kerentanan risiko serta penggunaan alat deteksi intrusi untuk memantau aktivitas mencurigakan dalam jaringan dan sistem.

Kata kunci: Sistem Informasi, Keamanan Informasi, Penilaian Risiko, NIST SP 800-30, Mitigasi Risiko.

PENDAHULUAN

Penerapan teknologi informasi semakin berkembang seiring kemajuan era globalisasi yang mana telah mengambil peran penting terkhusus dalam dunia bisnis. Hal ini tentunya menjadi peluang bagi perusahaan dalam meningkatkan kualitas bisnisnya. Teknologi informasi merupakan hal yang harus diperhatikan dan dikelola dengan baik oleh perusahaan guna mempertahankan bisnis yang dijalankan [1]. Namun seiring perkembangan teknologi yang semakin pesat dan juga kompleks banyak terjadi peluang kejahatan di dalam ranah bisnis. Oleh karena itu perlu diterapkannya keamanan informasi untuk memastikan keamanan yang spesifik agar dapat terpenuhi tujuan dari suatu perusahaan.

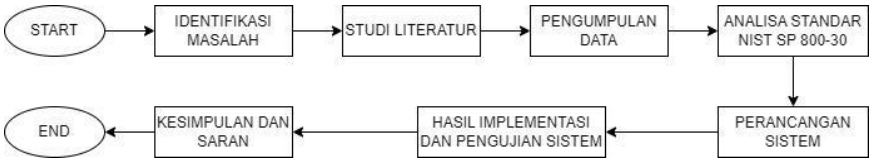
Perusahaan dapat berjalan secara optimal dengan menerapkan sistem keamanan informasi. Keamanan informasi merupakan upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Secara tidak langsung keamanan informasi menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, dan mengoptimalkan pengembalian investasi [2]. Manajemen risiko merupakan suatu kegiatan praktik dalam melakukan identifikasi, penilaian, kontrol serta menanggulangi risiko terhadap aset yang ada. Untuk mengatur proses bisnis sehingga dapat berjalan secara efektif dan memberi keuntungan bagi organisasi serta meminimalisir dampak yang disebabkan risiko TI maka diperlukan manajemen penilaian risiko [3]. Penilaian risiko adalah suatu kinerja terstruktur untuk mengidentifikasi kemungkinan bahaya atau ancaman, menganalisis penyebab dan akibat serta menjelaskan risiko secara kualitatif maupun kuantitatif dan dengan representasi yang tepat [4].

Pada PT.XYZ ini terdapat risiko yang timbul dalam penggunaan sistem informasi perencanaan produksi bahan baku dikarenakan dalam segi keamanan yang masih lemah. Hal ini sangat selaras dengan wawancara yang dilakukan bersama informan selaku staff IT PT.XYZ pada 10 April 2023 bahwa pada pertengahan tahun 2022 sistem informasi perencanaan produksi mengalami kebobolan data perencanaan produksi bahan baku berupa terserangnya virus *website spoofing* dikarenakan kurangnya keamanan juga kurangnya perhatian pada sistem yang harusnya dapat dilakukan oleh departemen IT perusahaan. Akibat dari kebobolan tersebut perusahaan mengalami kerugian yang cukup besar, tidak hanya kerugian berupa materi, kegiatan bekerja yang seharusnya dapat berjalan normal menjadi terhambat karena adanya perbaikan pada sistem[5].

Apabila kondisi tersebut terus menerus diabaikan oleh perusahaan maka tidak menutup kemungkinan ancaman yang lebih besar akan terjadi[6]. Dari wawancara tersebut penulis dapat menyimpulkan bahwa perusahaan belum atau tidak melakukan penilaian risiko pada aset-aset yang dimiliki oleh perusahaan, sehingga perusahaan tidak mengetahui risiko dan dampak apa saja yang akan terjadi dalam jangka panjang. Adapun kepentingan dan keuntungan dalam menerapkan penilaian risiko pada PT.XYZ yaitu dapat mengurangi dampak bahaya dengan berinvestasi dalam mitigasi, selain itu juga dapat menjaga aset yang berisiko di dalam perusahaan seperti teknologi informasi, sistem utilitas, mesin dan bahan mentah hingga barang jadi siap dipasarkan [7]. Dari masalah yang telah dipaparkan tersebut perlu dilakukan penelitian terkait penilaian risiko menggunakan standar NIST (National Institute of Standards and Technology) SP (Special Publication) 800-30. Standar NIST SP 800-30 ini memiliki keunggulan di mana salah satunya yaitu melakukan detail pelaksanaan assessment dan memberikan rekomendasi kontrol yang baik dan luas dibandingkan dengan metode lainnya [8].

METODE

Keamanan informasi digunakan untuk mendeskripsikan perlindungan pada *hardware*, data, *software*, informasi, dan infrastruktur agar tidak disalah gunakan oleh pihak yang tidak berwenang. Keamanan sistem informasi bertujuan untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat segala kerusakan sistem[9]. Manajemen risiko pada dasarnya dilakukan melalui proses- proses identifikasi risiko, evaluasi dan pengukuran risiko serta pengelolaan risiko[10]. Pada tahapan penelitian ini menggambarkan alur dari proses penelitian dalam pembuatan sistem yang sesuai dengan standar NIST SP 800-30. Dalam melakukan penilaian risiko pada PT. XYZ ini dimulai dengan tahap identifikasi masalah di mana berisi masalah yang sesuai dengan kondisi yang terjadi pada PT. XYZ[11]. Untuk memastikan kelangsungan proses bisnis dan mengurangi risiko bisnis, Tujuan dari adanya keamanan suatu informasi adalah memberikan perlindungan terhadap informasi tersebut agar aman dari berbagai macam jenis bahaya[12]. Berikut merupakan alur penelitian yang dapat dilihat pada Gambar 1:



Gambar 1. Alur Penelitian

Tahap penelitian ini meliputi beberapa tahapan penelitian dari awal hingga akhir. Penelitian ini dilakukan dengan menggunakan Standar NIST (National Institute of Standards and Technology) SP (Special Publication) 800-30 [8].

Analisa Standar NIST SP 800-30

Salah satu tahapan yang harus dilakukan sebelum melakukan manajemen keamanan aset informasi adalah dengan melakukan manajemen risiko terhadap aset informasi yang dimiliki. Manajemen risiko aset informasi merupakan sebuah praktik mengidentifikasi, menilai, mengendalikan, dan memitigasi risiko dari aset informasi yang meliputi sistem informasi dan teknologi informasi[13]. Secara garis besar sesuai dengan standar NIST SP 800-30, terdapat sembilan tahapan dalam melakukan penilaian risiko [14]. Adapun alur tahap analisa menggunakan Standar NIST SP 800-30 dapat dilihat pada Gambar 2 berikut:

Gambar 2. Alur Penerapan Standar NIST SP 800-30

NIST SP 800-30 digunakan oleh peneliti karena mempunyai tahapan yang lebih detail, yang memungkinkan pengumpulan data yang lebih detail serta fokus kepada aset-aset perusahaan[12]. Pada standar NIST SP 800-30 ini terdapat sembilan tahapan yang dimulai dengan tahapan sebagai berikut:

1. System Characterization atau karakteristik sistem atau menentukan ruang lingkup atau scope dari aset.

2. Threat Identification atau identifikasi ancaman, potensi ancaman bisa berasal dari luar maupun dari dalam perusahaan sehingga harus diidentifikasi. Sumber ancaman bisa berupa tindakan atau kejadian, intinya semua yang bisa memberikan atau menyebabkan kerusakan pada sistem informasi.
3. Vulnerability Identification atau identifikasi kerentanan TI secara teknis maupun non teknis yang disebabkan atau dipicu oleh sumber-sumber ancaman. Untuk mengidentifikasi ancaman perlu dilakukan penentuan aset yang bersangkutan dengan sistem informasi.
4. Control Analysis atau analisis pengendalian, tahap ini dilakukan dengan cara mendokumentasikan dan menilai efektivitas pengendalian teknis dan non-teknis yang telah atau akan dilaksanakan oleh suatu perusahaan agar meminimalkan atau mengurangi suatu sumber ancaman untuk sebuah sistem informasi.
5. Likelihood atau penentuan kemungkinan untuk menentukan nilai keseluruhan yang menunjukkan bahwa kerentanan dapat dimanfaatkan oleh sumber ancaman yang diberikan kontrol keamanan. Pada tahap ini perlu dilakukan perhitungan nilai kemungkinan/*likelihood* dengan rumus *Rerata Probabilitas* = $\frac{Jumlah\ Kejadian}{Periode\ Kejadian}$ setelah didapat nilai rerata probabilitas maka langkah selanjutnya mencari nilai kemungkinan dengan rumus *Nilai Kemungkinan / Likelihood* = $\frac{Jumlah\ Rerata\ Probabilitas}{Total\ Kejadian}$ setelah mendapatkan nilai kemungkinan kemudian memberikan rating sesuai ketentuan pada Tabel 1 berikut:

Tabel 1. Definisi Besarnya Kemungkinan

Nilai	Tingkatan	Definisi
0,8-1,0	Sangat sering	Hampir selalu terjadi
0,6-0,8	Sering	Kemungkinan besar terjadi
0,4-0,6	Mungkin	Mungkin saja terjadi tetapi jarang
0,2-0,4	Jarang	Kemungkinan terjadi tapi kecil
0 -0,2	Sangat jarang	Hampir tidak pernah terjadi

6. Impact Analysis atau analisa dampak yang bertujuan menentukan tingkat dampak negatif yang akan dihasilkan dari ancaman sehingga menghasilkan kerentanan [8]. Adapun tingkatan besarnya dampak dapat dilihat pada Tabel 2 berikut.

7.

Tabel 2. Definisi Besarnya Dampak

Nilai	Tingkatan	Definisi
1	Sangat Kecil	Dampak kecil yang dapat diabaikan
2	Kecil	Kerusakan kecil yang mudah diperbaiki kembali
3	Sedang	Memengaruhi pencapaian beberapa sasaran
4	Besar	Sasaran-sasaran penting tidak dapat tercapai
5	Sangat Besar	Semua sasaran tidak dapat tercapai

8. Risk Determination yaitu perhitungan penentuan risiko dengan cara mengalikan peringkat dari penentuan kemungkinan dan analisis dampak pada tingkat risiko yang sudah ditentukan sebelumnya dengan rumus Penilaian Risiko = Kemungkinan x Dampak.

Tabel 3. Tingkat Penentuan Risiko

Matriks Analisis Risiko			Dampak/Impact				
			1	2	3	4	5
			Sangat Kecil	Kecil	Sedang	Besar	Sangat Besar
P	5	Sangat Sering	Sedang	Tinggi	Tinggi	Ekstrim	Ekstrim
	4	Sering	Sedang	Sedang	Tinggi	Tinggi	Ekstrim
	3	Mungkin	Rendah	Sedang	Sedang	Tinggi	Ekstrim
	2	Jarang	Rendah	Sedang	Sedang	Tinggi	Tinggi
	1	Sangat Jarang	Rendah	Rendah	Sedang	Sedang	Tinggi

9. Control Recommendation yang bertujuan untuk memberi kontrol dan mengurangi tingkat risiko terhadap sistem dan data ke tingkat yang dapat diterima.
10. Results Documentation atau Dokumentasi Hasil Kegiatan yang bertujuan melakukan dokumentasi dari hasil kegiatan penilaian risiko yang kemudian diimplementasikan dalam bentuk laporan lalu diberikan kepada pihak perusahaan.

HASIL DAN PEMBAHASAN

Dalam menyelesaikan penelitian ini dilakukan proses analisis sistem yang memiliki sejumlah teknik untuk membantu memahami konteks penggunaan. Seperti survei, observasi, analisis tugas, dan wawancara [15].

Karakteristik Sistem

Pada tahap pertama dalam melakukan analisis penilaian risiko yaitu karakteristik sistem dengan mengkategorikan aset yang ada di dalam perusahaan. Adapun hasil wawancara yang telah dilakukan bersama informan selaku staff IT pada PT.XYZ terdapat beberapa aset perusahaan yang terbagi ke dalam lima kategori aset seperti pada Tabel 4.

Tabel 4. Karakteristik Sistem

No	ID Aset	Nama Aset	Proses Bisnis	Kategori Aset
1	HW_1	Server Komputer	Menyediakan beragam *resources* yang dapat digunakan komputer *client* terhubung jaringan di mana server dapat melayani permintaan data dari komputer *client.*	*Hardware*
2	SO_1	*Windows*	Sistem operasi yang digunakan perusahaan dalam menunjang sistem perencanaan produksi bahan baku di mana perusahaan membeli domain sehingga dapat mengakses web aplikasi secara online.	Sistem Operasi

3	NET_1	Jaringan LAN	Perangkat jaringan yang digunakan yaitu LAN dengan jenis topologi *star* dikarenakan dapat memungkinkan pengiriman data dan informasi antar perangkat menjadi lebih cepat dan efisien.	*Network*
4	SW_1	Sistem Perencanaan Produksi Bahan Baku	Aplikasi yang berisikan perencanaan dan realisasi produksi hingga barang siap dipasarkan. Sistem ini digunakan untuk melakukan pendataan produksi bahan baku, mengontrol data produksi, serta finishing produksi.	*Software*
5	DT_1	Data Produksi	Data yang melibatkan pemantauan dan pencatatan jumlah produksi, waktu produksi, kualitas produk efisiensi operasional serta mengidentifikasi target produksi.	Data
6	DT_2	Data *Accounting*	Data yang menyediakan informasi laporan keuangan perusahaan laba bersih, total aset, pendapatan penjualan, kas, dan piutang usaha hingga data produksi.	
7	SDM_1	Departemen Produksi	Departemen produksi bertugas melakukan pengadaan dan pendataan barang produksi hingga barang siap dipasarkan juga bertanggung jawab atas pengendalian bahan baku serta berwenang dalam pembuatan perencanaan produksi.	Sumber Daya Manusia

Identifikasi Ancaman

Pada tahap identifikasi ancaman ini dilakukan guna mengetahui kelemahan pada aset perusahaan serta ancaman apa saja yang dapat mengancam aset perusahaan yang dapat dilihat pada Tabel 5 berikut.

Tabel 5. Identifikasi Kelemahan dan Ancaman pada PT. XYZ

No	Kode	Jenis Kejadian	Keterangan	Aset
1	W1	Sistem keamanan yang lemah	Kurangnya perlindungan keamanan sistem karena tidak adanya penerapan *user access controls.*	Sistem Perencanaan Produksi Bahan Baku
2	W2	Server komputer mudah mengalami *overheat*	Penggunaan server yang intensif dan pendinginan ruang yang tidak efektif.	Server Komputer
3	W6	*Maintenance* yang tidak terjadwal	Tidak dilakukan perawatan secara berkala sehingga berakibat terjadinya gangguan layanan.	Server Komputer, Jaringan LAN

4	W8	Kondisi perangkat lunak yang telah usang (sistem operasi dan aplikasi perkantoran)	Perangkat lunak yang tidak diperbarui secara teratur dapat memiliki kerentanan yang menyebabkan usangnya perangkat penunjang perusahaan.	*Windows,* Sistem Perencanaan Produksi Bahan Baku
5	W11	Kurangnya pengarsipan data	Perusahaan tidak melakukan penyimpanan dan pengarsipan secara berkala sehingga berisiko terjadinya kehilangan data.	Data Produksi, Data *Accounting*, Dept. Produksi
6	T1	Terjadi peretasan komputer	Peretasan komputer (*computer hacking*) yang merusak operasi sistem sehingga terjadinya pembobolan data.	Server Komputer, Sistem Perencanaan Produksi Bahan Baku,Data Produksi, Data *Accounting*
7	T2	Serangan virus, *website spoofing* dan sejenisnya	Penyerang menyebarkan virus seperti *website spoofing* dan *phising* untuk mencuri data pada sistem atau jaringan terinfeksi, setelah itu penyerang menuntut tebusan kepada perusahaan agar dapat mengembalikan data ke kondisi semula.	Server Komputer, *Windows*, Jaringan LAN, Sistem Perencanaan Produksi Bahan Baku, Data Produksi, Data *Accounting*
8	T4	Gangguan perangkat dan keamanan jaringan	Terjadinya kegagalan perangkat jaringan dikarenakan sistem keamanan yang kurang dapat menimbulkan ancaman berupa serangan virus.	Komputer, Jaringan LAN, Sistem Perencanaan Produksi Bahan Baku
9	T5	Kesalahan fungsional sistem	Terjadi kesalahan dan kegagalan yang terkait dengan fungsi atau kinerja sistem komputer.	*Windows*, Sistem PerencanaanProduksi Bahan Baku
10	T6	Kerusakan dan kehilangan data	Terjadinya kegagalan perangkat keras maupun perangkat lunak dapat menyebabkan kerusakan data.	Data Produksi, Data *Accounting*

**Keterangan: Kode W (Weakness) Kelemahan || Kode T (Threat) Ancaman*

Identifikasi Kerentanan *(Vulnerability Identification)*

Identifikasi kerentanan dilakukan untuk mengetahui potensi kejadian pada tiap aset perusahaan. Identifikasi kerentanan merupakan langkah penting dalam melakukan analisa risiko untuk mengembangkan strategi pengamanan yang efektif. Data kerentanan ini didapat dari identifikasi kelemahan dan ancaman yang disesuaikan dengan kondisi pada PT. XYZ kemudian dikembangkan dari penelitian terdahulu. Berikut merupakan tabel identifikasi kerentanan yang dapat dilihat pada Tabel 6.

Tabel 6. Identifikasi Kerentanan

ID Aset	Nama Aset	Kerentanan
HW_1	Server Komputer	Penyebaran virus, kehilangan data, gangguang pelayanan, *overheat,* akses tidak sah, serangan keamanan dan kapasitas penyimpanan overload
SO_1	*Windows*	Kegagalan operasional, kerugian perbaikan perangkat, sistem *error, pencurian data, sistem tidak dapat diakses.*
NET_1	Jaringan LAN	Jaringan down, terhambatnya akses ke layanan, rusaknya perangkat jaringan karena terbengkalai, lupa password jaringan, akses tidak sah.
SW_1	Sistem Perencanaan Produksi Bahan Baku	Serangan virus *website spoofing,* pencurian data, sistem tidak dapat diakses, kegagalan operasional, sistem error.
DT_1	Data Produksi	Kehilangan data, manipulasi data, pencurian informasi data, akses tidak sah, kegagalan keamanan dan privasi.
DT_2	Data *Accounting*	Kehilangan data, manipulasi data, pencurian informasi data, akses tidak sah, kegagalan keamanan dan privasi.
SDM_1	Departemen Produksi	Kesalahan input data, peningkatan risiko kecurangan, penurunan produktivitas, pemalsuan data.

Analisa Pengendalian

Setelah melakukan identifikasi kerentanan selanjutnya dilakukan proses analisa pengendalian untuk menentukan langkah-langkah perbaikan yang diperlukan serta mengurangi juga mengelola risiko yang terjadi pada perusahaan. Data analisis pengendalian ini dilakukan berdasarkan kondisi yang sesuai dengan keadaan pada PT.XYZ dan dikembangkan dari penelitian sebelumnya. Berikut merupakan daftar analisa pengendalian yang dapat dilihat pada Tabel 7.

Tabel 7. Analisa Pengendalian

ID Aset	Nama Aset	Kerentanan	Pengendalian
HW_1	Server Komputer	Penyebaran virus, kehilangan data, gangguan pelayanan, *overheat,* akses tidak sah, serangan keamanan dan kapasitas penyimpanan overload	Penerapan solusi anti-DDoS/CDN, pencadangan data, regulasi pemantauan suhu dan kelembaban, menambah kapasitas memori.
SO_1	*Windows*	Kegagalan operasional, kerugian perbaikan perangkat, sistem *error,* pencurian data, sistem tidak dapat diakses.	Menjalankan prosedur pemeliharaan rutin, regulasi audit perangkat, verifikasi identitas,tingkat keamanan.
NET_1	Jaringan LAN	Jaringan down, terhambatnya akses ke layanan, rusaknya perangkat jaringan karena	Penerapan prosedur pemantauan jaringan, pencadangandan

		terbengkalai, lupa password jaringan, akses tidak sah.	pemulihan jaringan,pengelolaan identitas akses.
SW_1	Sistem Perencanaan Produksi Bahan Baku	Serangan virus *website spoofing,* pencurian data, sistem tidak dapat diakses, kegagalan operasional, sistem error.	Meningkatkan keamanan browser, prosedur pengoperasian sistem, pengelolaan identitas akses, pemeliharaan rutin.
DT_1	Data Produksi	Kehilangan data, manipulasi data, pencurian informasi data, akses tidak sah, kegagalan keamanan dan privasi.	Penerapan pencadangan data, regulasi validasi data, pencadangan data, pengelolaan identitas akses.
DT_2	Data *Accounting*	Kehilangan data, manipulasi data, pencurian informasi data, akses tidak sah, kegagalan keamanan dan privasi.	Penerapan pencadangan data, regulasi validasi data, pencadangan data, pengelolaan identitas akses.
SDM_1	Departemen Produksi	Kesalahan input data, peningkatan risiko kecurangan, penurunan produktivitas, pemalsuan data.	Menerapkan prosedur pengoperasian sistem (input dan pengecekan data), regulasi pelatihan karyawan.

Penentuan Kemungkinan

Pada tahap penentuan kemungkinan (*likelihood*) ini dilakukan perhitungan nilai kemungkinan (*likelihood*) pada tiap aset yang bertujuan untuk mengetahui besarnya kondisi ancaman yang terjadi pada aset perusahaan. Adapun hasil dari perhitungan nilai kemungkinan (*likelihood*) pada aset dapat dilihat pada Tabel 8 berikut.

Tabel 8. Penentuan Nilai Kemungkinan Beserta Tingkatannya

ID Aset	Nama Aset	Nilai *Likelihood*	Tingkat Kemungkinan
HW_1	Server Komputer	0,028	Sangat Jarang
SO_1	*Windows*	0,025	Sangat Jarang
NET_1	Jaringan LAN	0,025	Sangat Jarang
SW_1	Sistem Perencanaan Produksi Bahan Baku	0,015	Sangat Jarang
DT_1	Data Produksi	0,034	Sangat Jarang
DT_2	Data *Accounting*	0,013	Sangat Jarang

SDM_1	Departemen Produksi	0,045	Sangat Jarang

Analisa Dampak

Pada tahapan analisa dampak ini dilakukan pendataan dampak yang pernah terjadi di perusahaan, tujuan utama dari dilakukannya analisa dampak ini untuk mengetahui potensi kerugian bagi perusahaan akibat terjadinya risiko pada tiap aset yang dapat dilihat pada Tabel 9.

Tabel 9. Analisa Dampak

ID Aset	Nama Aset	Dampak	Nilai	Tingkatan Dampak
HW_1	Server Komputer	Kerusakan pada server yang berakibat kerugian finansial.	5	Sangat Besar
SO_1	*Windows*	Terjadi kegagalan operasional yang tidak dapat berjalan sebagaimana mestinya.	3	Sedang
NET_1	Jaringan LAN	Akses internet tidak dapat terhubung sehingga terhambatnya proses penginputan data perusahaan.	4	Besar
SW_1	Sistem Perencanaan Produksi Bahan Baku	Terjadinya pembobolan data yang mengakibatkan perusahaan mengalami kerusakan data.	5	Sangat Besar
DT_1	Data Produksi	Aktivitas perusahaan terhambat selama proses pemulihan data.	5	Sangat Besar
DT_2	Data *Accounting*	Aktivitas perusahaan terhambat selama proses pemulihan data.	2	Kecil
SDM_1	Departemen Produksi	Terjadinya peningkatan risiko potensial hingga kegagalan operasional.	3	Sedang

Penentuan Kemungkinan

Setelah dilakukan analisa melalui beberapa tahapan diatas, telah ditemukan hasil dari nilai kemungkinan dan nilai dampak dimana keduanya merupakan syarat penentuan level risiko dengan perhitungan Probabilitas X Dampak yang dapat dilihat pada Tabel 10.

Tabel 10. Penentuan Risiko

ID Aset	Nama Aset	Kemungkinan	Dampak	Level
HW_1	Server Komputer	Sangat Jarang	Sangat Besar	Tinggi
SO_1	*Windows*	Sangat Jarang	Sedang	Sedang
NET_1	Jaringan LAN	Sangat Jarang	Besar	Sedang
SW_1	Sistem Perencanaan Produksi Bahan Baku	Sangat Jarang	Sangat Besar	Tinggi
DT_1	Data Produksi	Sangat Jarang	Sangat Besar	Tinggi
DT_2	Data *Accounting*	Sangat Jarang	Kecil	Rendah
SDM_1	Departemen Produksi	Sangat Jarang	Sedang	Sedang

Rekomendasi Kontrol

Berdasarkan hasil dari analisis pada tahapan sebelumnya telah diketahui risiko beserta tingkatan risiko yang terjadi pada PT.XYZ maka langkah selanjutnya yaitu melakukan rekomendasi kontrol penanganan terhadap risiko yang terjadi. Tujuan dilakukannya rekomendasi kontrol ini agar perusahaan dapat melakukan pengelolaan risiko dengan harapan mengurangi risiko-risiko yang berdampak merugikan dan lebih parah kedepannya. Rekomendasi kontrol atas risiko yang terjadi dapat dilihat pada Tabel 11.

Tabel 11. Rekomendasi Kontrol

ID Aset	Nama Aset	Risiko	Rekomendasi
HW_1	Server Komputer	Kurangnya sistem keamanan pada ruang server sehingga akses keluar masuk ruang server tidak terkontrol	Perlu dilakukan penerapan sistem cloud dan peningkatan keamanan kartu akses yang hanya dimiliki oleh pihak sah.
SO_1	*Windows*	Keterlambatan dalam pembaruan keamanan sistem yang menyebabkan terhambatnya proses penginputan data.	Perlu diterapkan penjadwalan *maintenance* SO dan mengaktifkan pembaruan otomatis.
NET_1	Jaringan LAN	Penggunaan kata sandi yang lemah.	Perlu dilakukan peningkatan kebijakan kata sandi yang kuat.
SW_1	Sistem Perencanaan Produksi Bahan Baku	Pembobolan data yang diakibatkan oleh kurangnya keamanan sistem sehingga sistem tidak dapat diakses dan operasional pendataan produksi terhambat.	Perlu dilakukan penerapan pengamanan sistem dan pembaruan keamanan perangkat lunak yang diupdate secara berkala dengan patch keamanan terbaru.
DT_1	Data Produksi	Data dan informasi diakses oleh pihak yang tidak	Perlu dilakukan penerapan pengelolaan identitas yang kuat untuk mengontrol dan memantau

		berwenang sehingga terjadi kehilangan data.	akses serta enkripsi data dan jaringan.
DT_2	Data *Accounting*	Pengarsipan data yang tidak terjadwal menyebabkan terjadinya kecurangan data.	Perlu dilakukan backup arsip data yang disimpan di lokasi aman batasi akses hanya ke pihak yang sah.
SDM_1	Departemen Produksi	Kurangnya pemahaman prosedur penggunaan IT menyebabkan terjadinya kesalahan dan kelalaian.	Perlu dilakukan pelatihan pemanduan sistem IT guna mengendalikan risiko operasional.

Dokumentasi Hasil

Setelah dilakukannya analisis penilaian risiko pada PT. XYZ melalui beberapa tahapan diatas terdapat aset perusahaan yang perlu menjadi perhatian khusus. Adapun hasil tingkatan risiko dari aset tersebut sebagai berikut:

1. Aset dengan risiko level tinggi: Server Komputer, Sistem Perencanaan Produksi Bahan Baku dan Data Produksi.
2. Aset dengan risiko level sedang: Sistem Operasi *Windows*, Perangkat Jaringan LAN dan Departemen Produksi.
3. Aset dengan risiko level rendah: Data *Accounting*

Apabila sudah mendapatkan tingkat risiko, maka rekomendasi yang telah diberikan sebelumnya dilaksanakan oleh perusahaan. Rekomendasi diperoleh dari probabilitas ancaman,. Rekomendasi untuk setiap aset dapat dilihat pada Tabel 11.

KESIMPULAN

Bersumber dari hasil penelitian yang telah dilakukan tentang penilaian risiko keamanan sistem informasi terhadap aset yang mendukung Sistem Perencanaan Produksi Bahan Baku, maka dapat ditarik kesimpulan bahwa penilaian yang dilakukan terhadap Sistem Perencanaan Produksi Bahan Baku dengan metode NIST SP 800-30 didapatkan satu aset yang mempunyai level risiko yang rendah yaitu Data *Accounting*; tiga aset dengan level risiko sedang yaitu Sistem Operasi *Windows*, Perangkat Jaringan LAN dan Departemen Produksi; tiga asset dengan risiko level tertinggi yaitu Server Komputer, Sistem Perencanaan Produksi Bahan Baku dan Data Produksi.

DAFTAR PUSTAKA

[1] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 (STUDI KASUS: PT GLOBAL INFOTECH)," *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, Feb. 2020, doi: 10.33557/binakomputer.v2i1.799.

[2] A. Ramadhani, "KEAMANAN INFORMASI," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, p. 39, Jun. 2018, doi: 10.30999/n-jils.v1i1.249.

[3] M. S. Hardani and K. Ramli, "Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30," *JURIKOM J. Ris. Komput.*, vol. 9, no. 3, p. 591, Jun. 2022, doi: 10.30865/jurikom.v9i3.4181.

[4] E. Zio, "The future of risk assessment," *Reliab. Eng. Syst. Saf.*, vol. 177, pp. 176–190, Sep. 2018, doi: 10.1016/j.ress.2018.04.020.

[5] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "ANALISIS RISIKO TEKNOLOGI INFORMASI PADA APLIKASI SAP DI PT SERASI AUTORAYA MENGGUNAKAN ISO 31000," *Sebatik*, vol. 23, no. 1, pp. 36–43, Jun. 2019, doi: 10.46984/sebatik.v23i1.441.

[6] A. Mukhlishin, "ANALISIS MANAJEMEN RISIKO (KAJIAN KRITIS TERHADAP PERBANKAN SYARIAH DI ERA KONTEMPORER)," vol. 05, 2018.

[7] R. Puspita, "ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI DAN PEMETAAN MATURITY LEVEL PADA PT. XYZ MENGGUNAKAN FRAMEWORK COBIT 4.1," *J. Manaj. Inform. JAMIKA*, vol. 7, no. 2, Oct. 2017, doi: 10.34010/jamika.v7i2.530.

[8] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.

[9] M. P. Mokodompit and N. Nurlaela, "Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X)," *J. Sist. Inf. Bisnis*, vol. 6, no. 2, pp. 97–104, Jan. 2017.

[10] D. M. M. Hanafi, "Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management".

[11] A. Rizky, A. Setyawan, and M. R. A. Pramudya, "Penilaian Risiko Teknologi Informasi dan Keamanan Informasi Menggunakan Framework NIST SP 800-30 (Studi Kasus : E-Learning Universitas Pembangunan Nasional Veteran Jakarta)," 2021.

[12] "Information System Security Risk Assessment NIST SP 800-30 Framework Selector Data | JATISI (Jurnal Teknik Informatika dan Sistem Informasi)," Jun. 2023, Accessed: Mar. 14, 2024. [Online]. Available: https://jurnal.mdp.ac.id/index.php/jatisi/article/view/3843

[13] A. Pakarbudi, D. T. Piay, D. Nurmadewi, and A. Rachman, "Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi," *JURIKOM J. Ris. Komput.*, vol. 10, no. 2, Art. no. 2, Apr. 2023, doi: 10.30865/jurikom.v10i2.5950.

[14] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems : recommendations of the National Institute of Standards and Technology," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30, 2002. doi: 10.6028/NIST.SP.800-30.

[15] R. R. Putri, A. Sodik, and A. Pakarbudi, "Perancangan User Experience Aplikasi Pendaftaran Mahasiswa Baru Menggunakan Metode Human-Centered Design," 2020.