Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

AUDIT KEAMANAN TEKNOLOGI INFORMASI DENGAN NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY (NIST) 800-30 PADA PD INDAH PERMAI GROUP

Muhamad Wisnu Alfiansyah[1], Christopher Michael Lauw[2], Husain[3],Rauhil Fahmi[4]

[123]Program Studi Teknologi Informasi, Universitas Bumigora, [4,]Program Studi Ilmu Komputer, Universitas Bumigora

Jln. Basuki Rahmat No.105 Praya Lombok Tengah 83511
[1] wisnu@universitasbumigora.ac.id, [2] 2001020015@universitasbumigora.ac.id,
[3]husain@universitasbumigora.ac.id, [3]rauhil@universitasbumigora.ac.id

Abstract

In the era of Industry 4.0, the utilization of Information Technology within a company serves to facilitate data exchange and storage for smooth business processes. As time progresses, companies experience growth, resulting in an increasing volume of data and information that need to be accommodated and safeguarded for confidentiality. PD Indah Permai Group (IPG) is a company engaged in the distribution of essential commodities heavily reliant on Information Technology in its business operations. The issue faced by the company is the absence of information security risk management, leading to occasional data loss, damage, and vulnerability to information theft on the server. Information Technology security audits are conducted using the National Institute of Standard and Technology 800-30 framework. The outcome of this research consists of proposed security audit. Some of the recommendations given include the transaction process, products and sales, servers, PCs, and employees will be risk transferred (transferred to a third party to handle). Then for the network, UPS, and IIS Permai information system, risk reduction will be carried out (will be followed up by internal parties).

Keywords : *Audit, Information Security, NIST 800-30, Risk Management, Security Standard*

Abstrak

Pada era industri 4.0. Pemanfaatan Teknolog Informasi dalam suatu perusahaan yaitu untuk bertukar data, menampung data untuk kelancaran proses bisnis. Seiring berjalannya waktu, perusahaan semakin berkembang dan semakin banyak pula data dan informasi yang harus ditampung dan dijaga kerahasiaannya. PD. Indah Permai Group (IPG) merupakan perusahaan yang bergerak dalam bidang distributor sembako yang sangat bergantung pada Teknologi Informasi pada proses bisnisnya. Permasalahan yang terdapat pada perusahaan tersebut yaitu, tidak adanya manajemen risiko keamanan informasi sehingga terkadang data dan inforamsi yang ada pada server sering hilang, rusak, bahkan rentan terhadap pencurian informasi. Audit keamanan Teknologi Informasi dilakukan menggunakan framework National Institute of Standard and Technology 800-30. Hasil dari penelitian ini berupa usulan hasil audit keamanan untuk diterapkan pada perusahaan *30* untuk mengidentifikasi risiko dan memberikan rekomendasi mitigasi. Beberapa rekomendasi yang diberikan diantaranya proses transaksi, produk dan penjualan, server, PC, dan karyawan akan dilakukan risk transfer(dialihkan ke pihak ketiga untuk menangani). Kemudian untuk jaringan, UPS, dan sistem informasi IIS Permai akan dilakukan risk reduction (akan ditindak lanjuti oleh pihak internal).

Kata kunci : *Audit, Keamanan Informasi, Manajemen Resiko, NIST 800-30, Standar Keamanan*

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

1. PENDAHULUAN

Perkembangan dunia maya di era industri 4.0 sangatlah pesat[1]. Dimana industri dalam era 4.0 harus terhubung ke dunia *cyber* agar dapat berkomunikasi dan bertukar data secara cepat. Internet digunakan untuk berkomunikasi maupun bertukar data antara personal hingga perusahaan berskala *enterprise*[2][3]. Perusahaan yang telah menggunakan sistem informasi dan komputasi untuk mendukung proses bisnis harus memiliki manajemen yang sangat baik terkait dengan keamanan dan kerahasiaan data dalam ruang lingkup teknologi informasi tersebut[4]. Seiring dengan berjalannya waktu, dewasa ini, hampir seluruh perusahaan sudah menggunakan teknologi informasi[5]. Adapun permasalahan dan tantangan yang dihadapi oleh perusahaan yaitu terjadinya kehilangan, pencurian, dan kerusakan data yang disebabkan oleh virus ataupun pihak yang tidak bertangung jawab[6]. Permasalahan tersebut diakibatkan oleh tidak adanya manajemen resiko yang baik terkait dengan keamanan informasi[7]. Permasalahan kedua yaitu kebocoran informasi penting terkait dengan transaksi ataupun kerahasiaan peruasahaan yang disalurkan dengan menggunakan sistem informasi[8].

Dari permasalahan diatas, maka terdapat solusi bagi perusahaan untuk melakukan standarisasi keamanan informasi. Terdapat beberapa standar keamanan teknologi informasi yang telah diakui, seperti COBIT, ISO 270001, dan NIST 800-30[9]. Framework NIST 800-30, penulis menggunakan NIST 800-30 dikarenakan standar panduan tersebut sangat cocok untuk menganalisa resiko yang akan terjadi[10]. NIST 800-30 adalah sebuah panduan yang diterbitkan oleh National Institute of Standards and Technology (NIST) di Amerika Serikat[11]. Dokumen ini berjudul "*Guide for Conducting Risk Assessments*" dan bertujuan untuk membantu organisasi dalam melakukan penilaian risiko terkait keamanan informasi[12]. *Risk assessment* atau penilaian risiko adalah proses yang digunakan untuk mengidentifikasi, mengevaluasi, dan mengelola risiko yang mungkin dihadapi oleh suatu organisasi terkait dengan keamanan informasi[13]. Melalui *risk assessment*, organisasi dapat memahami potensi ancaman, kerentanan, dan dampak dari kejadian yang dapat mengganggu kerja operasional serta kerahasiaan, integritas, dan ketersediaan informasi[14]. Pentingnya perusahaan untuk melakukan penilaian terhadap resiko yaitu agar dapat mengevaluasi tingkat keamanan yang dimiliki[15]. PT Indah Permai Group merupakan salah satu perusahaan yang bergerak di bidang retail dan distributor di daerah NTB. Dalam rangka mencapai target, tentu terdapat banyak sekali resiko yang dapat terjadi yang akan menghambat tujuan perusahaan. Tujuan dari hasil evaluasi tersebut untuk mengambil keputusan ataupun berupa rekomendasi pengembangan sistem agar dapat meminimalisir risiko yang terjadi. Penelitian ini diharapkan dapat memberikan rekomendasi untuk mengatur dan memanajemen ketika terjadi permasalahan.

2. TINJAUAN PUSTAKA

2.1. Audit Teknologi Informasi

Audit keamanan teknologi informasi adalah proses evaluasi sistem, jaringan, perangkat lunak, dan infrastruktur teknologi informasi suatu organisasi untuk mengidentifikasi potensi kerentanan, ancaman, dan risiko keamanan yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan data[16]. Tujuan dari audit keamanan TI adalah untuk memastikan bahwa sistem dan data yang digunakan oleh organisasi tersebut terlindungi dengan baik dari serangan dan pelanggaran keamanan yang dapat menyebabkan kerugian finansial, reputasi buruk, atau gangguan operasional[17].

2.2. Keamanan Teknologi Informasi

Keamanan teknologi informasi (TI) adalah upaya untuk melindungi informasi digital yang dimiliki dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data[14]. Sekarang ini, kebutuhan akan sistem keamanan TI semakin meningkat seiring dengan meningkatnya risiko serangan siber, malware, pencurian data, dan kerentanan sistem, serta adanya potensi serangan sosial(*social engineering*)[18]. Keamanan TI terdiri dari beberapa aspek, seperti pengamanan perangkat lunak, perlindungan jaringan, pengelolaan akses, serta edukasi pengguna tentang ancaman dan praktik terbaik dalam keamanan. Perkembangan teknologi yang pesat juga membawa tantangan baru dalam dunia keamanan TI. Misalnya, munculnya teknologi berbasis cloud, Internet of

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

Things (IoT), dan kecerdasan buatan (AI) telah meningkatkan kompleksitas dalam melindungi data dan infrastruktur. Hal ini menuntut organisasi untuk tidak hanya mengadopsi teknologi terbaru tetapi juga memastikan bahwa langkah-langkah keamanan yang diterapkan mampu mengimbangi risiko yang ada[19]. Terdapat beberapa framework yang dapat diterapkan untuk strategi keamanan teknologi informasi, seperti ISO/EIC 270001:2013, ITIL Security Management, COBIT 5, serta National Institute Standards and Technology (NIST) 800-30[20].

2.3. National Institute of Standards and Technology (NIST) 800-30

Standar NIST (*National Institute of Standards and Technology*) Special Publication 800-30 adalah panduan yang membahas tentang manajemen risiko keamanan informasi[21]. Dokumen ini secara khusus menguraikan proses identifikasi, penilaian, dan pengelolaan risiko keamanan informasi dalam suatu organisasi[22]. NIST 800-30 adalah bagian dari rangkaian panduan NIST yang dikeluarkan untuk membantu organisasi dalam mengembangkan dan mematuhi kebijakan keamanan informasi yang efektif[23]. Tujuan utama NIST 800-30 yaitu untuk membantu organisasi dalam mengidentifikasi, menilai, dan mengelola risiko keamanan informasi dengan pendekatan yang terstruktur dan metodologis[24]. Dokumen ini memberikan kerangka kerja untuk mengidentifikasi ancaman dan kerentanan yang mungkin mempengaruhi keamanan informasi suatu organisasi, serta untuk merumuskan rencana mitigasi dan tindakan perbaikan yang sesuai [25].

Ruang Lingkup: NIST 800-30 mencakup langkah-langkah yang harus diambil oleh organisasi untuk melakukan penilaian risiko keamanan informasi, termasuk perencanaan, analisis risiko, penilaian risiko, dan pengelolaan risiko. Dokumen ini berlaku untuk semua jenis organisasi, baik sektor publik maupun swasta, serta dapat diterapkan pada berbagai jenis sistem dan infrastruktur teknologi informasi[26]. Manfaat dari framework NIST 800-30 yaitu Memahami potensi risiko keamanan informasi yang mereka hadapi.Mengambil tindakan preventif dan perbaikan yang sesuai untuk mengurangi risiko. Mengalokasikan sumber daya dengan efektif untuk mengelola risiko. Memenuhi persyaratan peraturan dan standar keamanan informasi.

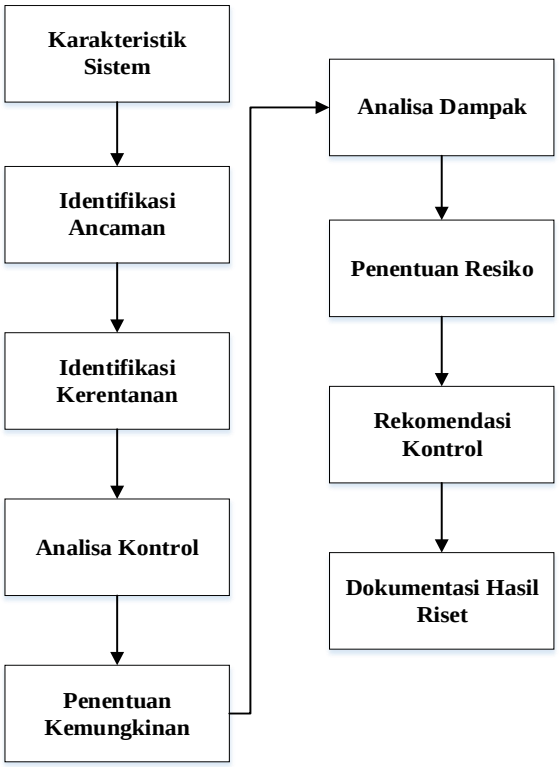
Beberapa penelitian terkait penerapan NIST 800-30 untuk menangani manajemen resiko teknologi informasi yaitu penelitian yang dilakukan oleh (Dewi,2021) [27], penulis menerapkan framework NIST 800-30 untuk melakukan manajemen resiko di UIN SUSKA Riau, Pada proses pengolahan data dihasilkan ancaman-ancaman yang sudah teridentifikasi yaitu kebakaran, human error, virus, hacking dan kegagalan jaringan. Hasil akhir penelitian yaitu memberikan rekomendasi kontrol yang didasarkan pada analisis ancaman resiko yang terjadi. Salmon dan Ramli (2022) [10], melakukan penelitian manajemen resiko keamanan Sistem Informasi Manajemen Sumber Daya Manusia (SIMS)menggunakan NIST 800-30. Dari penelitian yang dilakukan, didapatkan a manajemen risiko SIMS memiliki 1 tingkat risiko rendah, 13 tingkat risiko sedang dan 6 tingkat risiko tinggi. Untuk selanjutnya dapat dilakukan tindakan pengendalian risiko dan mitigasi risiko. Untuk nilai risiko rendah dan sedang maka berdasarkan pedoman metodologi risk assessment dari organisasi dapat diterima. Sedangkan untuk kategori nilai risiko tinggi maka perlu dilakukan pengendalian risiko dengan cara risk avoidance (menghindari risiko), risk transfer (mentransfer risiko), maupun risk reduction (mengurangi risiko).

Penerapan *framework* NIST 800-30 pada instansi PT Indah Permai Group diharapkan dapat mengevaluasi resiko secara keseluruhan yang dapat terjadi pada perusahaan. Harapannya agar visi, misi dan tujuan perusahaan dapat tercapai.

3. METODOLOGI PENELITIAN

Tahapan dari NIST 800-30 dapat terlihat pada Gambar 1.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi



Gambar 1 Alur *framework* NIST 800-30

3.1. Karakteristik Sistem

Pada tahap pertama, peneliti melakukan identifikasi terhadap batas-batas sistem teknologi informasi, termasuk sumber daya dan informasi yang berjalan di PT Indah Permai Group. Selain itu akan digambarkan Batasan sistem dan hubungan antar sistem yang ada. Adapun *output* dari tahapan ini yaitu dokumen inventaris asset dan gambaran sistem secara menyeluruh.

3.2. Identifikasi Ancaman

Pada tahap kedua, peneliti melakukan identifikasi ancaman yang dapat terjadi pada sistem dan teknologi informasi milik PT Indah Permai Group, seperti sumber, potensi, dan kerawanan serta kontrol. Setelah diidentifikasi, akan dilakukan pengelompokan ancaman berdasarkan kategori yang telah ditentukan (lingkungan, teknis, fisik, dan lain-lain). Hasil dari tahapan ini yaitu daftar ancaman potensial yang relevan dengan teknologi informasi yang dimiliki.

3.3. Identifikasi Kerentanan

Pada tahap ini, akan dilakukan identifikasi terkait kerentanan sistem dan teknologi informasi yang terdapat pada PT Indah Permai Group. Hasil identifikasi selanjutnya akan digunakan untuk daftar kerentanan sistem selanjutnya. Hasil dari tahapan ini yaitu daftar kerentanan yang ada pada teknologi informasi yang dimiliki PT. Indah Permai Group.

3.4. Analisa Kontrol

Pada tahap ini, akan dilakukan Analisa kontrol (teknis, administratif, dan fisik) yang selama ini dilakukan oleh PT Indah Permai Group. Tujuannya yaitu untuk meminimalisir kemungkinan pengembangan dari ancaman yang ada. Hasil dari tahapan ini yaitu dokumentasi kontrol yang ada, beserta efektivitasnya.

3.5. Penentuan Kemungkinan

Pada tahap ini, dilakukan perankingan terhadap potensi dari kerentanan yang berasal dari lingkungan kerawanan yang ada. Perankingan yang dilakukan berdasarkan pada gabungan informasi dari ancaman, kerentanan, dan control yang telah ada di tahapan sebelumnya. Kemudian memberikan penilaian berdasarkan skala (misalnya: **low,medium, high**). Hasil dari tahapan ini yaitu penilaian tingkat kemungkinan ancamanyang terjadi di PT. Indah Permai Group.

3.6. Analisa Dampak

Pada tahap ini, dilakukan Analisa dampak kerentanan yang telah dianalisis. Tujuannya yaitu untuk menentukan dampak negatif yang dihasilkan dari keberhasilan penerapan kerawanan. Hasil dari analisa dampak yaitu estimasi dampak yang terjadi berdasarkan skala, misalnya **low, medium, high**.

3.7. Penentuan Resiko

Pada tahap ini dilakukan penilaian tingkat resiko yang terjadi pada system TI. Penentuan tingkat resiko menggunakan matriks resiko untuk memetakan resiko ke dalam kategori (**low, medium, high**). Setelah dinilai, kemudian akan diidentifikasi prioritas resiko berdasarkan tingkat resiko yang ada.

3.8. Rekomendasi Kontrol

Pada tahap ini, akan dilakukan penilaian kontrol yang mana dapat mengurangi atau bahkan menghilangkan resiko. Kemudian mempertimbangkan langkah mitigasi yang harus dilakukan untuk perbaikan penerapan manajemen resiko teknologi informasi di PT. Indah Permai Group.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

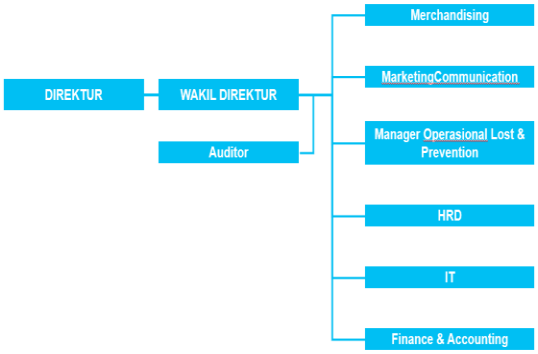
3.9. Dokumentasi Hasil Riset

Pada tahap akhir, dilakukan pengembangan laporan hasil penilaian resiko (sumber ancaman, kerawanan, resiko yang dinilai dan kontrol yang direkomendasikan).

4. HASIL DAN PEMBAHASAN

Adapun hasil dan pembahasan setelah penulis melakukan penelitian pada PD. IPG yaitu dimulai dari visi dan misi perusahaan. Visi dari PD. Indah Permai group yaitu memberi manfaat untuk orang lain, serta misi dari PD. IPG yaitu Bersama kita Berusaha untuk menjadi: Pemimpin Perusahaan Distribusi di Wilayah NTB,Perusahaan yang paling disegani di NTB, Sebagai Tempat pilihan untuk Bekerja. Dari visi misi tersebut maka dapat di ketahui pemanfaatan TI sangat berperan pentin bagi sistem perusahaan. Setlah memahami visi misi, selanjutnya yaitu memahami struktur organisasi perusahaan.

Adapun struktur organisasi yang dapat dilihat dari gambar dibawah ini. Tugas dari masing-masing divisi yaitu, yang pertama adalah direktur, yang bertugas untuk memimpin perusahaan, kemudian wakul direktur sebagai wakil dari direktur. Auditor bertugas untuk mengaudit sistem perekonomian, termasuk stock barang, barang yang banyak terjual, dan strategi pemasaran. Merchandising yaitu divisi yang bertugas untuk memberi *souvenir* kepada pelanggan yang loyal. Kemudian marketing communication yang bertugas untuk memasarkan produk. Manager operasional bertugas untuk mengawasi operasional perusahaan. HRD bertugas untuk memanajemen karyawan yang bekerja. Divisi IT bertugas untuk mengatasi permasalahan TI pada perusahaam , dan finance accounting, bertugas untuk memanajemen keuangan perusahaan.



Gambar 2 Struktur Organisasi PD. IPG

4.1. Karakteristik Sistem

Karakteristik sistem yang terdapat pada perushaan yaitu dapat dilihat pada tabel 1 dibawah ini. Tabel 1 menjelaskan bahwa setiap asset dikelompokan dengan diberikan ID sehingga memudahkan ketika proses pemetaan.

Tabel 1. Identifikasi Karakteristik Sistem

No	Kelompok	ID	Asset	Proses Bisnis
1.	Informasi	IN-001	informasi data produk meliputi penjualan, transaksi. Dsb.	Admin login ke sistem informasi IIS Permai untuk menginput data produk, admin bisa mengolah data produk, sedangkan kasir hanya bisa melihat produk yang meliputi seluruh atribut.
2.	Perangkat keras	HR-01	Server	Melayani permintaan komputer *client* dan menyediakan sumberdaya untuk digunakan bersama, baik untuk perangkat keras atau aplikasi
		HR-02	Komputer	Admin dan kasir menggunakan kompuer untuk keperluan proses bisnis dan interaksi kepada *customers.*
		HR-03	Jaringan	Topologi pada IPG menggunakan jenis topologi Mesh.
		HR-	UPS	Digunakan

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

		04		untuk menjadi *bakckup power* pada saat listrik padam.
3.	Sistem informasi	SIS-01	Sistem Informasi IIS Permai	IIS Permai digunakan untuk seluruh proses bisnis dalam IPG, yang menggunakan aplikasi ini adalah kasir dan admin.
4.	SDM	SM-01	Karyawan	Karyawan adalah orang yang melakukan tugasnya pada bidang masing-masing.

4.2. Identifikasi Ancaman dan Kemungkinan Kelemahan Sistem

Identifikasi ancaman sistem terdapat pada Tabel 2. Tabel 2 menjelaskan bahwa setiap ancaman dikelompokan dengan dengan diberikan kode. Sehingga memudahkan ketika proses pemetaan.

Tabel 2. Identifikasi Ancaman

No	Nama Kejadian	Keterangan	Kode
1.	Akses illegal	Akses tidak sah dari seseorang yang tidak memiliki kepentingan	T1
2.	serangan malware, ransomware, trojan horse	Pengrusakan fungsional dan kinerja pada perangkat lunak maupun traffic jaringan.	T2
3.	Hacker	Akses tidak sah dari pihak yang tidak bertangungjawab melalui jaringan komputer	T3
4.	Pencurian asset	Pemindahan tampa izin dari pihar luar instansi	T4
5.	Bencana Alam	Fenomena Alam yang membuat resiko semakin tinggi yaitu banjir, gempa bumi, petir, angin kencang.	T5
6.	Kebakaran	Pembakaran yang diakibatkan oleh konsletina arus litrik, atau individu yang mengancam keberadaan asset.	T6
7.	Sabotase	Kemungkinan sabotase sistem dari pemegang sistem dalam perusahaan	T7

Identifikasi kemungkinan kelemahan sistem yang terdapat pada perusahaan yaitu dapat dilihat pada Tabel 3. Tabel 3 menjelaskan bahwa setiap kemungkinan dan kejadian dikelompokan dengan dengan diberikan kode. Sehingga memudahkan ketika proses pemetaan.

Tabel 3. Identifikasi Kemungkinan Kelemahan Sistem

No.	Nama kejadian	Keterangan	Kode
1.	Kerusakan Data	Kerusakan terhadap data akibat tidak adanya pemeliharaan terhadap media penyimpanan data atau hal lainnya.	V1
2.	*Human Error*	Kesalahan entry data, kesalahan pengoperasian asset, kelalaian saat bertugas	V2
3.	Gangguan perangkat keras	*Hardware* tidak beroperasi atau asset perangkat keras sebagai mana fungsinya.	V3
4.	Gangguan Sumber daya listrik	Tidak ada supply energi listrik untuk mengoperasikan	V4

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

		perangkat kers, yaitu ketika listrik padam UPS tidak bekerja secara maksimal dan harus menunggu genset dinyalakan	
5.	Kesalahan pengiriman data	Kesalahan pengiriman data yang mengakibatkan data tidak sampai pada tujuan.	V5
6.	Perangkat lunak mengalami *BUG*	Fungsional sistem tidak berjalan sebagaimana mesitnya	V6
7.	Pembaruan aplikasi	tidak ada kontrol terhadap pembaruan sistem informasi.	V7

4.3. Pemetaan Daftar Aset dan Gangguan Keamanan Sistem

Pada tahap ini akan dilakukan daftar asset dan gangguan keamanan yang dapat terjadi berdasarkan asset yang dimiliki. Tabel 4 memperlihatkan pemetaan daftar asset dan gangguan keamanan sistem yang mungkin terjadi di PT. Indah Permai Group.

Tabel 4. Pemetaan Daftar Aset dan Gangguan Keamanan Sistem

Kode Aset	Kemungkinan Ancaman							Kemungkinan Kelemahan						
	T1	T2	T3	T4	T5	T6	T7	V1	V2	V3	V4	V5	V6	V7
IN-001	■		■			■		■						
HR-001	■			■		■				■				
HR-002	■			■		■				■	■			
HR-003	■					■				■	■			
HR-004				■		■				■				
SIS-01		■	■						■			■	■	■
SM-01	■		■				■					■		

4.4. Identifikasi Ancaman

Identifikasi ancaman yang terjadi pada PT Indah Permai Group dapat dilihat pada Tabel 5. Tabel 5 memperlihatkan daftar ancaman yang dapat terjadi pada tiap asset yang dimiliki oleh PT. Indah Permai Group.

Tabel 5. Identifikasi Ancaman

Asset	Ancaman
Informasi: Seluruh proses transaksi, produk yang dijual dan pendapatan	Kesalahan dalam pengimputan dan penghapusan data
	Tidak adanya penjadwalan *backup* data.
	Pencurian informasi
	Terkena virus
	Kehilangan atau kerusakan data.
Hardware :	
Server	Kurang pengamanan dalami infrastruktur ruangan
	Maintenance yang tidak teratur
	Kerusakan fisik pada PC server
	Konsleting arus listrik
	Suhu PC server diatas ambang batas yang ditentukan
	Server down
	Kapasitas spesifikasi server yang sudah tidak memadai
Komputer (PC)	Maintenance tidak teratur
	Spesifikasi yang mempengaruhi penggunaan yang lambat
	Terserang virus
	Penyalahgunaan *resource*
UPS	Konsleting listrik
	Baterai AKI UPS tidak kuat untuk mensuplay energi listrik ketika listrik padam
	Kerusakan perangkat
Jaringan	Lemah keamanan pada sistem internal TI
	Kurang mekanisme monitoring terhadap jaringan

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

	Gangguan jaringan sehingga mempengaruhi komunikasi dan pertukaran data	
	Kerusakan pada infrastruktur jaringan	
	Kesalahan konfigurasi	
Karyawan	Kurang sosialisasi terkait regulasi sanksi ketika terjadi *human error*	
	Kurang teliti dalam input dan pengolahan data	
Sistem Informasi IIS Permai	Sistem tidak dapat diakses	
	Kesalahan kode program	

4.5. Analisa Kontrol

Analisa kontrol yang dilakukan berdasarkan pada hasil analisis potensi ancaman yang telah dilakukan pada tahapan sebelumnya. Tiap potensi ancaman yang ada akan diberikan rekomendasi penanganan yang sesuai. Tabel 6 memperlihat analisa kontrol dan penanganannya.

Tabel 6. Analisa Kontrol dan Penanganan

Asset	Potensi Ancaman	Penanganan
Informasi: Seluruh proses transaksi, produk yang dijual dan pendapatan	Kesalahan dalam penginputan dan penghapusan data	Dilakukan verifikasi ulang
	Organisasi tidak melakukan prosedur backup	Menjadwalkan backup data secara teratur
	Salah input dan menghapus data	Dilakukan verifikasi ulang
	Terserang virus	Menggunakan antivirus dan menghapus file-file mencurigakan
Hardware :		
Server	Kurang pengamanan informasi	Meningkatkan keamanan
	Maintenance yang tidak teratur	Malakukan *maintenance* terjadwal
	Kerusakan fisik pada server	*Maintanance*
	Konsleting listrik	*Maintenance* pada kabel dan gardu listrik
	Server overheat	Membersihkan atau menambahkan sistem pendingin
Komputer	Maintenance tidak teratur	Melakukan *maintenance* secara teratur
	Spesifikasi yang mempengaruhi penggunaan yang lambat	Menupgrade perangkat keras
	Terserang virus	Melakukan scanning file secara terjadwal
	Penyalahgunaan resource	Adanya prosedur jika ingin menggunakan resource
UPS	Konsleting listrik	*Maintenance*
	Baterai AKI UPS tidak kuat untuk mensuplay energi listrik ketika listrik padam	*Maintenance*
	Kerusakan perangkat	*Maintenance*
Karyawan	Kurang sosialisasi terkait regulasi sanksi ketika terjadi *human error*	Melakukan sosialisasi
	Kurang teliti dalam input dan pengolahan data	Melakukan verifikasi ulang

4.6. Penentuan Kemungkinan

Pada tahap ini akan dilakukan analisis frekuensi kemungkinan ancaman terjadi pada setiap asset. Tabel 7 memperlihatkan pemetaan terkait aset dan peluang terjadinya ancaman.

Tabel 7. Penentuan Kemungkinan

Kategori Aset	Nama Aset	Kode Aset	Kemungkinan	Sebutan

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

Informasi	Seluruh proses transaksi, produk yang dijual dan pendapatan	IN-001	0.04	Sangat Jarang
Perangkat keras	Server	HR-01	0.05	Sangat Jarang
	Komputer (PC)	HR-02	0.09	Sangat Jarang
	Jaringan	HR-03	0.002	Sangat Jarang
	UPS	HR-04	0.9	Mungkin
Perangkat lunak	Sistem Informasi Management (IIS Permai)	SIS-01	0.5	Jarang
Karyawan	SM-01		0.7	Mungkin

4.7. Analisa Dampak

Pada tahap ini akan dilakukan analisis dampak dari ancaman yang terjadi pada setiap asset dan pemberian nilai tiap dampak. Tabel 8 memperlihatkan pemetaan terkait aset dan dampak terjadinya ancaman serta nilainya.

Tabel 8. Analisa Dampak dan Penilaian

No	ID Asset	Nama Asset	Dampak	Nilai
1	IN-001	Seluruh proses transaksi, produk yang dijual dan pendapatan	Mempengaruhi beberapa target bisnis atau gangguan yang terjadi dapat berdampak pada pelayanan yang sangat bergantung pada sistem informasi	5
2	HR-01	Server	Semua sasaran informasi tidak dapat dijangkau sehingga mempengruhi pelayanan *customer*	5
3	HR-02	Komputer	Mempengaruhi aktivitas yang dilakukan menggunakan komputer mejadi terganggu , seperti halnya penginputan data, sistem pembayaran pada kasir	5
4	HR-03	Jaringan	Semua akses internet dapat terganggu atau tidak dapat mengakses informasi dan data	4
5	HR-04	UPS	Tidak dapat mensuplay energi listrik akibat dari konsleting listrik.	3
6	SIS-01	Sistem informasi (IIS Permai)	Perusahaan sangat bergantung pada sistem informasi IIS Permai jika terjadi masalah berdampak pada penurunan pendapatan dan perekonomian perusahaan	5
7	SM-01	Karyawan	Memperngaruji pencapaian beberapa sasaran atau tidak tercapainya tujian-tujuan secara tepat	3

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

			waktu		

4.8. Penentuan Resiko

Pada tahap ini akan dilakukan penentuan resiko berdasarkan kemungkinan dan ancaman terjadi pada setiap asset. Tabel 9 memperlihatkan pemetaan terkait penentuan resiko berdasarkan kemungkinan dan dampaknya.

Tabel 9. Penentuan Resiko

Kategori Aset	Nama Aset	Kode Aset	Kemungkinan	Dampak	Level
Informasi	Seluruh proses transaksi, produk yang dijual dan pendapatan	IN-001	Sangat Jarang	Sangat Besar	Tinggi
Perangkat keras	Server	HR-01	Sangat Jarang	Sangat besar	Tinggi
	Komputer (PC)	HR-02	Sangat Jarang	Sedang	Sedang
	Jaringan	HR-03	Sangat Jarang	Sangat besar	Tinggi
	UPS	HR-04	Sangat Jarang	Besar	Sedang
Perangkat lunak	Sistem Informasi Management (IIS Permai)	SIS-01	Jarang	Besar	sedang
Karyawan	SM-01		Mungkin	Sedang	Sedang

4.9. Rekomendasi Kontrol

Pada tahap ini akan dilakukan pemberian rekomendasi kontrol berdasarkan BP, BR, dan PA yang didapatkan dari hasil penentuan resiko. Tabel 10 memperlihatkan pemberian rekomendasi setiap asset dengan memperhatikan nilai dari BP, BR, dan PA.

Tabel 10. Rekomendasi Kontrol

No	Nama Asset	BP	BR	PA	Kriteria
1.	Seluruh proses transaksi, produk yang dijual dan pendapatan	Low	High	Low	Risk Transfer
2.	Server	Low	High	Low	Risk Transfer
3.	Komputer (PC)	Low	High	Low	Risk Transfer
4.	Jaringan	Med	Med	Low	Risk Reduction
5.	UPS	Med	Med	Low	Risk Reduction
6.	Sistem informasi IIS Permai	Med	Med	Med	Risk Reduction
7.	Karyawan	High	Low	Med	Risk Transfer

5. KESIMPULAN DAN SARAN

Adapun kesimpulan dari penelitian ini yaitu, NIST SP 800-30, telah memberikan tahapan penliaian yang cukup mendetail, dari tahap awal penelitian hingga akhir maka didapatkan hasil bahwa PD. Indah Permai Group direkomendasikan meningkatkan spesifikasi perangkat keras yang dimiliki, dikarenakan kebanyakan status NIST memberikan kerangka kerja yang komprehensif untuk mengidentifikasi, melindungi, mendeteksi, merespon, dan memulihkan sistem informasi.

Berdasarkan hasil rekomendasi kontrol yang telah dihasilkan, didapatkan hasil untuk aset seluruh proses transaksi, produk yang dijual dan pendapatan, server, computer(PC),

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

dan karyawan akan dilakukan risk transfer. Risk transfer dalam hal ini yaitu kemungkinan ancaman yang terjadi akan dialihkan ke pihak ketiga, seperti menggunakan asuransi kontrak penyedia jasa. Sedangkan untuk asset jaringan, UPS, dan sistem informasi IIS Permai yang dimiliki akan dilakukan risk reduction. Risk reduction dalam hal ini yaitu akan dilakukan Langkah-langkah mitigasi untuk mengurangi kemungkinan ancaman terjadi atau mengurangi dampaknya.

Dengan mengikuti pedoman ini, PD. Indah Permai Group dapat memperkuat sistem keamanan mereka dan mengurangi risiko terhadap kebocoran atau penyalahgunaan informasi. Hal ini membantu perusahaan dalam menghadapi ancaman yang mungkin timbul dan melindungi data pelanggan serta informasi bisnis yang penting. Pentingnya kesadaran dan pelatihan keamanan informasi di kalangan karyawan juga menjadi faktor penting PD. Indah Permai Group perlu memastikan bahwa semua anggota tim memahami kebijakan keamanan informasi, praktik terbaik, dan protokol yang harus diikuti untuk menjaga kerahasiaan dan integritas data.

Untuk penelitian selanjutnya, terdapat beberapa saran penelitian yaitu:

a. Membandingkan efektivitas NIST 800-30 dengan framework lain, seperti ISO 27001, COBIT, atau Cybersecurity Framework (NIST CSF), dalam konteks yang sama (PD Indah Permai Group) atau di instansi yang berbeda.
b. Mengidentifikasi risiko baru yang terkait dengan ancaman siber terkini, seperti **ransomware**, **phishing**, atau serangan berbasis AI, dan bagaimana pendekatan NIST 800-30 dapat diadaptasi untuk menghadapi ancaman tersebut.
c. Menilai efektivitas pelatihan keamanan TI berdasarkan temuan risiko NIST 800-30. Fokusnya adalah meningkatkan kesadaran keamanan pada karyawan dan mengurangi risiko human error.

6. UCAPAN TERIMA KASIH

Terimakasih yang sebesar-besarnya kepada pihak PT Indah Permai Group karena telah menerima dan memberikan informasi yang dibutuhkan guna mendukung penyelesaian penelitian ini.

DAFTAR PUSTAKA:

[1] I. K. Dewi and K. Yusriyah, "Cyber Public Relation Dalam Akun Instagram @Official.Antam Pt. Aneka Tambang To Face the Industrial Revolution 4 . 0," *MEDIALOG J. Ilmu Komun.*, vol. 4, no. 1, pp. 88–95, 2021.

[2] S. Suginam, "Transformasi Digital di Masa Pandemi Covid 19: Studi Fenomenologi Pada UKM Kota Medan," *J. Bus. Econ. Res.*, vol. 3, no. 2, pp. 296–299, 2022, doi: 10.47065/jbe.v3i2.1696.

[3] N. Purba, M. Yahya, and Nurbaiti, "Revolusi Industri 4.0 : Peran Teknologi Dalam Eksistensi Penguasaan Bisnis Dan Implementasinya," *J. Perilaku Dan Strateg. Bisnis*, vol. 9, no. 2, pp. 91–98, 2021.

[4] H. Tanuwijaya, "Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 11, no. 3, p. 571, 2022, doi: 10.35889/jutisi.v11i3.993.

[5] A. Bimantoro, W. A. Pramesti, S. W. Bakti, M. A. Samudra, and Y. Amrozi, "Paradoks Etika Pemanfaatan Teknologi Informasi di Era 5.0," *J. Teknol. Inf.*, vol. 7, no. 1, pp. 58–68, 2021, doi: 10.52643/jti.v7i1.1425.

[6] B. Ariesta Kalkhove, S. Rohani, and Alhadiansyah, "Upaya Notaris Dalam Menghadapi Tantangan Perlindungan Terhadap Data Penghadap Di Era Digital," *Tanjungpura Acta Borneo J.*, vol. 1, no. 2, pp. 90–111, 2023, [Online]. Available: https://jurnal.untan.ac.id/index.php/tabj

[7] J. Wijaya, A. Megafitri, K. Khotimah, R. Astriratma, S. Kom, and M. Cs, "Analisis dan Manajemen Risiko Keamanan Informasi pada Rumah Sakit Menggunakan Metode Octave Allegro (Studi Kasus: Rumah Sakit Umum Daerah Cengkareng)," *Semin. Nas. Mhs. Ilmu Komput. dan Apl.*, pp. 762–774, 2021.

[8] Sasongko, D. P. Dwipayana, Jumangin, and C. P. Roselawati, "Konsep Perlindungan Hukum Data Pribadi dan Sanksi Hukum atas Penyalahgunaan Data Pribadi oleh Pihak Ketiga," *Proceeding*

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

Conf. Law Soc. Stud., vol. 1, no. 2, pp. 16–27, 2020, [Online]. Available: http://prosiding.unipma.ac.id/index.php/COLaS%0Ahttp://prosiding.unipma.ac.id/Index.Php/COLaS%0Ahttp://prosiding.unipma.ac.id/index.php/COLaS

[9] 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, 2020.

[10] 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 (Jurnal Ris. Komputer)*, vol. 9, no. 3, p. 591, 2022, doi: 10.30865/jurikom.v9i3.4181.

[11] A. E. Musantono, A. K. Nisa, A. Q. A'Yuni, and H. Umam, "Manajemen Risiko Default Pada Pengguna Kartu Kredit Menggunakan Framework NIST 800-30," *INFORMAL Informatics J.*, vol. 7, no. 2, pp. 115–120, 2022.

[12] E. Simanjuntak, "Manajemen Risiko Aset Perangkat IT Pada XYZ Menggunakan Standar ISO / IEC 27005 : 2008," 2021.

[13] V. P. P. Wijaya, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1295–1307, 2022, doi: 10.35957/jatisi.v9i2.2087.

[14] J. Jonny, A. Ambarwati, and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005," *Sistemasi*, vol. 10, no. 1, p. 1, 2021, doi: 10.32520/stmsi.v10i1.995.

[15] D. Pasha, A. thyo Priandika, and Y. Indonesian, "Analisis Tata Kelola It Dengan Domain Dss Pada Instansi Xyz Menggunakan Cobit 5," *J. Ilm. Infrastruktur Teknol. Inf.*, vol. 1, no. 1, pp. 7–12, 2020, doi: 10.33365/jiiti.v1i1.268.

[16] A. Elanda and R. L. Buana, "Analisis Manajemen Risikao Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus: STMIK Rosma)," *Elkom J. Elektron. dan Komput.*, vol. 14, no. 1, pp. 141–151, 2021.

[17] A. M. Ujung, M. Irwan, and P. Nasution, "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi," *JISKA J. Sist. Inf. Dan Inform.*, vol. 1, no. 2, p. 44, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis

[18] F. M. Hutabarat and A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, pp. 52–65, 2020, doi: 10.33557/binakomputer.v2i1.792.

[19] S. S. Hussein, M. W. Alfiansyah, R. Daud, S. Ya'acob, and A. M. Lokman, *Developing an Effective ICT Strategic Framework for Higher Education Institutions: A Case of Mataram University*, vol. 1825 CCIS, no. May. Springer Nature Switzerland, 2023. doi: 10.1007/978-3-031-34045-1_18.

[20] E. Khristian, H. Karamoy, and N. S. Budiarso, "Analisis Manajemen Risiko Dalam Mewujudkan Good Corporate Governance (Studi Kasus Pada PT Angkasa Pura I (Persero))," *J. Ris. Akunt. dan Audit. "GOODWILL,"* vol. 12, no. 2, pp. 112–128, 2021.

[21] Meilita Karenda Putri and A. R. Hakim, "Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005:2018 dan NIST SP 800-30 Revisi 1," *Info Kripto*, vol. 15, no. 3, pp. 134–141, 2021, doi: 10.56706/ik.v15i3.34.

[22] A. Elanda and R. L. Buana, "Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma)," *Elkom J. Elektron. dan Komput.*, vol. 14, no. 1, pp. 141–151, 2021, doi: 10.51903/elkom.v14i1.387.

[23] K. K. P. NIST, "Meningkatkan Privasi Melalui Manajemen Risiko Bisnis, Versi 1.0," *Tsapps. Nist. Gov. https//tsapps. nist. gov/publication/get_pdf. cfm*, 2020.

[24] W. P. Silalahi and R. Setyadi, "Analisis Manajemen Risiko Aplikasi DAPODIK Menggunakan COBIT 4.1," *Resolusi Rekayasa Tek. Inform. dan Inf.*, vol. 3, no. 2, pp. 168–175, 2022.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 8, Nomor 1, Januari 2025.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

[25] U. R. ISNAINI, "FORMULASI STRATEGI UNTUK ACUAN DOKUMEN PERENCANAAN KEBERLANGSUNGAN BISNIS (BCP) BERBASIS TEKNOLOGI INFORMASI DI PT. PERTAMINA REFINERY UNIT IV CILACAP".

[26] A. Syaputra, "Penilaian IT Governance dalam Manajemen Risiko IT Menggunakan Metode Quantitative dan Qualitative Risk Analysis," *J. Manaj. Inform.*, vol. 12, no. 1, pp. 63–73, 2022, doi: 10.34010/jamika.v12i1.6743.

[27] Y. Dewi, "Manajemen Risiko IT pada Sistem Iraise menggunakan Metode NIST SP 800-30," 2021.