E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333

Penilaian Risiko Keamanan Data Karyawan Pada Sistem Informasi Dengan Menggunakan Framework Nist Sp 800-30 pada PT. ABC

Nur Fitrianti Fahrudin, Aditya Nugraha S, Kurnia Ramadhan Putra
Program Studi Sistem Informasi
Institut Teknologi Nasional Bandung
Jl. PH.H. Mustofa No.23, Kota Bandung, Jawa Barat 40124

nurfitrianti@itenas.ac.id

Abstrak

Keamanan data karyawan pada sistem informasi memiliki beberapa risiko yang bisa terjadi yang tentunya dapat menyebabkan kerugian di dalam perusahaan. Risiko dapat berupa kejadian dan kondisi yang dapat mengganggu layanan dan menghambat proses pengambilan keputusan. Tujuan penelitian ini adalah untuk mendeskripsikan pelaksanaan manajemen risiko keamanan data karyawan di perusahaan PT. ABC dengan menggunakan kerangka kerja (framework) NIST SP 800-30 dan untuk mengetahui risiko yang timbul. Jika tidak ada manajemen risiko pada perusahaan maka perusahaan tidak akan tahu risiko apa saja yang terjadi dan dampak yang terjadi. Penelitian ini diawali dengan memetakan risiko, menilai risiko, memberikan rekomendasi sesuai dengan tingkat ancamannya. Hasil risiko keseluruhan terdiri dari ancaman alam, manusia dan kesalahan teknis didapatkan potensi risiko sebesar 14% untuk risiko rendah, 36% untuk risiko sedang, dan 50% untuk risiko tinggi Adapun saran yang diberikan adalah: melakukan pemeliharaan sistem secara berkala, sistem perlu ditunjang oleh software & hardware yang memadai.

Kata Kunci: manajemen risiko, NIST SP 800-30, penilaian risiko

Abstract

Security of employee data in the information system has several risks that can occur which of course can cause losses for the company. Risk can be in the form of events and conditions that can disrupt services and hinder the decision-making process. The purpose of this study is to describe the implementation of employee data security risk management in the company PT. ABC uses the NIST SP 800-30 framework to determine emerging risks. If there is no risk management in the company, the company will not know what risks occur and the impacts that occur. This research begins by mapping risks, assessing risks, and providing recommendations according to the level of threat. The overall risk results consist of natural, human, and technical errors, the potential risk is 14% for low risk, 36% for moderate risk, and 50% for high risk. The advice given is: that to perform regular system maintenance, the system needs to be supported by adequate software & hardware.

Keywords : risk management, NIST SP 800-30, risk assessment

1. PENDAHULUAN

Kemajuan teknologi yang semakin meningkat, membuat organisasi telah menyadari manfaat yang tak terbantahkan dari Teknologi Informasi (TI) untuk meningkatkan kualitas, akurasi dan kecepatan. Sebagian besar manajer telah menyadari pentingnya penggunaan TI dalam meningkatkan efisiensi dan efektivitas organisasi serta meningkatkan kepuasan pelanggan. Para manajer telah menetapkan dan menggunakan sistem informasi dalam kegiatan bisnisnya. Sementara bagi organisasi untuk menggunakan teknologi informasi, manajemen risiko memainkan peran penting dalam melindungi informasi mereka. Manajemen risiko yang efektif adalah salah satu bagian terpenting dari program keamanan di organisasi TI (Tohidi, 2011).

Manajemen risiko adalah salah satu langkah praktis yang dapat dilakukan untuk menangani risiko dalam suatu organisasi, termasuk dalam bidang keamanan informasi (Al Fikri, Putra, Suryanto, & Ramli, 2019).

Keamanan informasi sendiri merupakan salah satu aspek penting yang harus diperhatikan oleh perusahaan (Handayani, Wibowo, Sari, Satria, & Gifari, 2018). Risiko yang dapat terjadi meliputi kerusakan, kebocoran sampai dengan hilangnya suatu informasi. Hal ini tentunya dapat menimbulkan kerugian baik secara finansial maupun produktivitas perusahaan.

Perusahaan PT. ABC merupakan perusahaan pemetaan, survey, GIS, terkemuka di Indonesia yang merupakan salah satu instansi pemerintah pengelola infratsruktur kritis di Indonesia. Berdasarkan tugas pokok dan fungsi Sistem Informasi dan Teknologi Informasi yang dimiliki oleh perusahaan PT. ABC tersebut, tidak dapat dipungkiri bahwa ketergantungan akan TI sangat tinggi. Namun dalam penerapan Sistem dan layanan terhadap publik tersebut, Perusahaan PT. ABC masih belum menerapkan manajemen resiko terhadap sistem informasi. Jika tidak ada manajemen risiko pada perusahaan maka perusahaan tidak akan tahu risiko apa saja yang terjadi dan dampak yang terjadinya. Hal ini berdampak pada perusahaan untuk meminimalisir terhadap resiko yang bisa timbul dalam pengoperasian layanan publik tersebut.

Terdapat beberapa metode yang dapat digunakan untuk melakukan analisa manajemen risiko seperti Meharim Magerit, NIST 800-30 dan *Microsoft's Security Management Guide* (Putro, Ambarwati, & Setiawan, 2021). NIST SP-800-30 Memiliki 9 langkah untuk melakukan analisa risiko yaitu karakterisasi sistem, identifikasi ancaman, identifikasi kerawanan, analisa kontrol, analisa kecenderungan, analisa dampak, penentuan risiko, rekomendasi kontrol dan dokumentasi (Gary Stoneburner & and Alexis Feringa, 2002). NIST SP 800-30 adalah standar yang dikembangkan oleh Institut Nasional Standar dan Teknologi. Diterbitkan sebagai dokumen khusus yang diformulasikan untuk penilaian risiko keamanan informasi, terutama berkaitan dengan sistem TI (Ghazouani, Faris, Medromi, & Sayouti, 2014). Pada penelitian sebelumnya dengan tema manajemen risiko sistem informasi menggunakan kerangka NIST, framework tersebut memiliki keunggulan yaitu salah satunya dengan memiliki detil pelaksanaan *assessment* dan memberikan rekomendasi kontrol yang baik dan luas dibandingkan dengan framework yang lain (Elanda & Buana, 2021). Berdasarkan hasil dan pembahasan maka dapat diperoleh bahwa dari identifikasi karakteristik dan ancaman serta kerentanan didapat beberapa sumber ancaman yang dapat menimbulkan risiko pada perusahaan.

Hal tersebut mendorong penulis untuk melakukan analisa mendalam mengenai evaluasi manajemen resiko terhadap sistem informasi yang dimiliki. Hal ini harus dilakukan sejalan dalam peraturan pemerintah yang tertuang dalam permen kominfo no.6 tahun 2017 yaitu guna pencapaian sasaran organisasi, perlu menetapkan Manajemen Risiko.

2. KAJIAN LITERATUR

A. Manajemen Risiko

Manajemen risiko adalah proses untuk mengidentifikasi dan mengakses risiko dan menerapkan metode untuk menguranginya ke tingkat yang dapat diterima (Tohidi, 2011). Manajemen risiko juga dapat diartikan sebagai kemampuan seorang manajer untuk menata kemungkinan variabilitas pendapatan dengan menekan sekecil mungkin tingkat kerugian yang disebabkan oleh keputusan yang diambil dalam mengerjakan situasi yang tidak pasti (Handayani et al., 2018).

Risiko adalah kemungkinan sumber ancaman tertentu menjalankan potensi kerentanan tertentu, dan dampak yang dihasilkan dari peristiwa buruk tersebut pada organisasi (Gary Stoneburner & and Alexis Feringa, 2002). Untuk meminimalisir dampak terhadap organisasi, maka perlu dilakukan manajemen risiko. Terdapat tiga tahap manajemen risiko teknologi yakni *risk assesment*, *risk mitigation*, dan *evaluation* dan *assesment* (Putra, Ambarwati, & Setiawan, 2019).

B. Kerangka Kerja NIST SP-800-30

NIST (National Institute Standard Technology) merupakan badan federal non regulasi di Amerika Serikat yang memiliki misi dalam mengembangkan dan mempromosikan pengukuran, standar dan teknologi untuk meningkatkan produktivitas dan meningkatkan kualitas hidup manusia. NIST menerbitkan beberapa Publikasi standar. Publikasi standar yang berkaitan dengan keamanan informasi yaitu NIST SP800-30.

Pada panduan NIST SP-800-30 tahapan dalam melakukan manajemen risiko dibagi menjadi tiga tahap yaitu

1. Risk Asessment

Risk Asessment / Penilaian Risiko adalah proses pertama yang dilakukan dalam melakukan metodologi manajemen risiko. Organisasi menggunakan penilaian risiko untuk menentukan sejauh mana potensi ancaman (*threat*) dan risiko yang terkait dengan sistem TI. Keluaran dari proses ini membantu mengidentifikasi pengendalian yang tepat untuk mengurangi atau menghilangkan risiko selama proses mitigasi risiko.

2. Risk Mitigation

Mitigasi risiko, proses kedua dari manajemen risiko, melibatkan penentuan prioritas, evaluasi, dan penerapan pengendalian pengurangan risiko yang sesuai yang direkomendasikan dari proses penilaian risiko.

Karena penghapusan semua risiko biasanya tidak praktis atau hampir tidak mungkin, itu adalah tanggung jawab manajemen senior dan manajer fungsional dan bisnis untuk menggunakan pendekatan dengan biaya paling rendah dan menerapkan kontrol yang paling tepat untuk mengurangi risiko misi ke tingkat yang dapat diterima, dengan biaya minimal. dampak buruk pada sumber daya dan misi organisasi.

3. Evaluation and Assesment

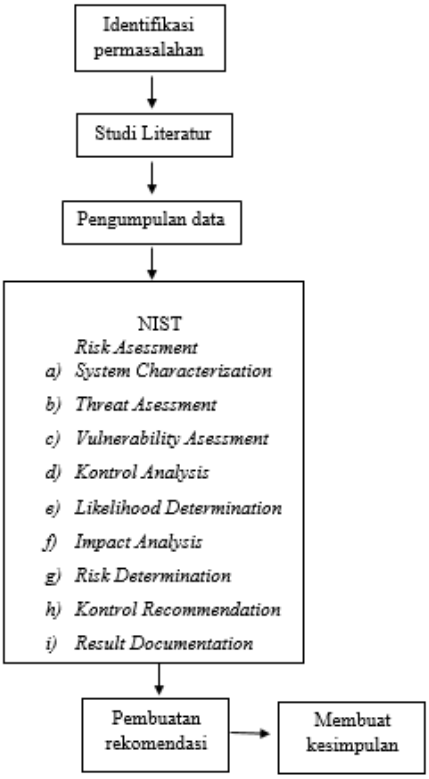
Pada Tahap Evaluasi adalah tahap dimana proses evaluasi terhadap implementasi kontrol risiko. Pekerjaan ini dilakukan setiap periode tertentu. Misalkan setiap tahun, hal ini dilakukan guna mengevaluasi kembali apakah tools atau metode mitigasi risiko masih relevant atau tidak. Atau ada komponen modul maupun software masih update atau tidak. Evaluasi ini dilakukan secara keseluruhan dimana melibatkan senior management, Risk Assessment Team, dan masing masing administrator system.

Pada sebagian besar organisasi, selalu terjadi pengembangan baik jaringan yang di perluas, perangkat luna yang diperbaharui. Selain itu, perubahan personel akan terjadi dan kebijakan keamanan kemungkinan akan berubah seiring waktu. Perubahan ini berarti bahwa risiko baru akan muncul dan risiko yang sebelumnya dimitigasi dapat kembali menjadi perhatian. Dengan demikian, proses manajemen risiko harus dilakukan secara rutin. Untuk meninjau apakah masih relevan atau tidak.

3. ANALISIS DAN PERANCANGAN

3.1 Kerangka Penelitian

Pada Gambar 1 Kerangka Penelitian berikut ini menjelaskan mengenai kerangka kerja dari penelitian manajemen risiko.



Gambar 1. Kerangka Penelitian

3.2 Identifikasi Masalah

Mengidentifikasi masalah ini dilakukan dengan observasi dan wawancara pada departemen ITnya di perusahaan PT.ABC. Pada saat melakukan observasi banyak kejadian yang bisa menimbulkan risiko keamanan system informasi dalam perusahaan dan tanpa cara penanganannya. Oleh karena itu saya memutuskan untuk mengambil tema manajemen risiko pada perusahaan PT. ABC dengan harapan perusahaan tersebut memiliki daftar risiko apa saja yang akan terjadi dan cara menanganinya.

3.3 Studi Literatur

Melakukan studi mengenai manajemen risiko teknologi informasi, sistem informasi pada departemen IT perusahaan PT.ABC, manajemen risiko teknologi informasi dan penelitian terdahulu yang terkait dengan manajemen risiko teknologi Informasi. Mencari beberapa jurnal penelitian yang terkait dengan manajemen risiko dan pemilihan framewok-nya

3.4 Pengumpulan Data

Pada Penelitian yang akan dilakukan dalam tahapan pengumpulan data untuk dapat menjadi acuan dalam melakukan analisa dan penilaian resiko untuk kemudian dijadikan landasan dalam menyusun dan menentukan langkah mitigasi resiko yaitu data primer dan data sekunder

1. Data Primer

Data primer merupakan sumber data yang diperoleh secara langsung dari beberapa sumber yang relevan diantaranya dari hasil wawancacra terhadap narasumber yang relevan, assessment tools, dan survei

2. Data Sekunder

Data sekunder merupakan data yang diperoleh dari dokumen instansi obyek penelitian. Dalam penelitian ini data sekunder diperoleh dari dokumen organisasi.

3.5 Analisis Data

Pada tahap pertama yaitu *risk assessment* melakukan beberapa tahap yaitu.

a) System Characterization
b) Threat Asessment
c) Vulnerability Asessment
d) Control Analysis
e) Likelihood Determination
f) Impact Analysis
g) Risk Determination
h) Kontrol Recommendation
i) Result Documentation

3.6 Pembuatan Rekomendasi

Pada tahapan ini dilakukan langkah prioritas aksi dimana langkah ini dilakukan guna melakukan pemeringkatan level risiko yang dimiliki dari yang paling tinggi hingga ke terendah secara berurutan, prioritas ini bertujuan untuk mengetahui risiko mana saja yang layak untuk dipertimbangkan terlebih dahulu untuk dilakukan langkah mitigasi terhadap risiko yang dimiliki.

3.7 Membuat Kesimpulan

Tahap terkahir adalah membuat kesimpulan setelah dilakukan serangkaian tahapan penilaian risiko. didapat beberapa rekomendasi kontrol terhadap residual risiko yang ada di dalam system perusahaan PT. ABC. Dilakukan tahapan penentuan risiko untuk mengetahui potensi risiko dengan cara melakukan self assessment yang berpedoman pada NIST sp800-30. Setelah dilakukan self asessment. Di hasilkan beberapa macam ancaman dan vulnerability dari risiko- risiko tersebut.

4. ANALISA DAN PEMBAHASAN

Berdasarkan kerangka kerja NIST SP 800-30, pada tahapan penilaian risiko terdapat langkah-langkah yang harus dilakukan seperti karakteristik sistem, identifikasi ancaman, identifikasi kerawanan, analisis kontrol, penentuan kesamaaan, analisis dampak, penentuan risiko, rekomendasi kontrol dan dokumentasi kontrol.

4.1 Karakterisasi Sistem

Penelitian ini hanya berfokus kepada sebuah sistem informasi yaitu sistem informasi pendataan karyawan. Sistem informasi pendataan karyawan ini hanya dapat diakses oleh staf yang ada pada departemen IT saja.

Komponen karakteristik sistem untuk system informasi meliputi: perangkat keras, perangkat lunak, peralatan jaringan, data dan informasi, serta operator. Perangkat keras untuk client menggunakan personal komputer dengan perangkat lunak windows 8 dan wihdows 10. Untuk server menggunakan apache server, mysql, pemrogram dan php yang secara umum.

4.2 Identifikasi Ancaman

Identifikasi ancaman ini akan dibagi kedalam 3 kategori yaitu ancaman yang berasal dari alam, manusia dan teknis.

A. Ancaman Alam.

Ancaman yang dapat menimbulkan kerugian secara financial yang sangat besar bagi instansi, yang tidak dapat dihindari. Tabel 1 ancaman alam menunjukkan gambaran sumber ancaman yang mungkin terjadi disebabkan oleh alam yaitu sebagai berikut:

Tabel 1. Ancaman alam

Sumber ancaman	Penyebab
Kebakaran	• Sambaran petir
Gempa Bumi/Longsor	• Lokasi yang kurang strategis • Cuaca ekstrim
Banjir	• Lokasi yang kurang strategis • Cuaca yang ekstrim

B. Ancaman Manusia

Ancaman yang dilakukan secara sengaja atau tidak sengaja. Tabel 2 Ancaman Manusia menunjukkan gambaran sumber ancaman yang disebabkan oleh manusia yaitu sebagai berikut:

Tabel 2 Ancaman Manusia

Sumber Ancaman	Penyebab
Hacker	Merubah atau merusak data
Virus	Merusak perangkat lunak
Human Error	Ketidaksengajaan

C. Ancaman Teknis

Ancaman yang terjadi karena kesalahan. Tabel 3 Ancaman Teknis menunjukkan gambaran sumber ancaman yang disebabkan oleh teknis.

Tabel 3 Ancaman Teknis

Sumber Ancaman	Penyebab
Kegagalan Jaringan	Ketidaksengajaan
Kebakaran	Kerusakan pada alat listrik

4.3 Identifikasi Kerentanan

Pada tahapan ini analisa ancaman terhadap sistem harus mencakup analisa kelemahan yang terkait dengan sistem yang dievaluasi. Tujuannya adalah untuk mengembangkan daftar kerentanan atau kelemahan sistem yang dapat dimanfaatkan oleh ancaman sumber potensial. Berikut ini beberapa identifikasi kerentanan yang terjadi di dalam sistem informasi.

4.4 Analisa Kontrol

Pada tahan ini bertujuan untuk menganalisis kontrol yang ada dan telah di-laksanakan atau yang sedang direncanakan oleh instansi untuk meminimalkan atau menghilangkan kemungkinan adanya ancaman dan kelemahan pada sistem. Berikut ini adalah Tabel 4 daftar kontrol dan rencana kontrol.

Tabel 4 Daftar Kontrol Dan Rencana Kontrol

No	Ancaman	Penyebab ancaman	Risiko	Control saat ini	Rencana control
1	kebakaran	korsleting listrik	Seluruh data dan informasi terhapus	Pengecekan kelayakan peralatan secara berkala	Membuat disaster recovery plan
		Adanya instalasi listrik yang tidak benar	Terbakar atau Rusaknya tempat	Membuat data center	Pemasangan Instalasi sesuai prosedur
		Tersambar petir	Penyimpanan data Merusak perangkat keras dan infrastruktur pendukung	Membuat Instalasi penangkal petir	Membuat data center Disaster Recovery Planning (DRP) yang Tahan terhadap bencana alam
2	Human Error	Perancangan sistem yang kurang baik	Pelaporan data Yang tidak akurat atau tidak tepat	Membuat pembatasan hak akses sesuai tingkat kepentingan nya	Melakukan Pelatihan dan pengawasan kepada User

		Skill dan pengalamanyyang kurang memadai	Terjadi kesalahan dalam masalah operasional pengambilan	Melakukan pengawalan secara internal berdasarkan jobdes masing masing	Melakukan training secara berkala
		Manajemen yang tidak menerapkan SOP	Keputusan yang salah atau kurang tepat	Melakukan perancangan SOP sesuai standar	Menerapkan SOP sesuai stadar yang berlaku
3	Virus	Penggunaan flashdisk yang tidak tertib	Hilangnya data-data penting	Membuat backup data	Membuat back up dan melarang Penggunaan flashdisk kecuali yang telah disediakan
		Tidak pernah atau jarang memperbarui antivirus	Software tidak dapat diakses	Melakukan update antivirus secara berkala	Memasang antivirusyang berlisensi
		Mengunduh file secara Sembarangan atau tidak jelas	Hilang atau rusaknya data-data penting	Melakukanupdate antivirus secara berkala	Membuat peraturan tertulis mengenai sistem kerjadalam pengunduhan file
4	Hacking	Kurangnya security awareness	Merubah dan Mengambil data secara illegal	Tidak ada dokumentasi yang dilakukan oleh sistem	Membuat file log sistemdan melakukan backup secara berkala
		Tidak adanya Audit trail atau log	Kehilangan data-data penting yang ada di system	Tidak ada dokumentasi yang dilakukan oleh sistem	Backup data rutin
		Enkripsi password pengguna masih lemah	Password mudah Diketahui oleh hacker	Tidak ada dokumentasi yang dilakukan oleh sistem	Menggunakan ekripsi yang lebih aman,
5	Kegagalan ISP jaringan	ISP terputus	System tidak dapat di akses menggunakan jaringan luar	ISP yang tersedia hanya satu	Penambahan ISP cadangan menambah akses cadangan
		Server down	Sistem tidak dapat di akses, prosespengolahan dan pelaporan terganggu.	Spesifikasi server saat ini belum dapat menangani user sekaligus	Upgrade Spesifikasi server
6	Kebakaran (teknis)	Adanya hubungan arus pendek listrik (korsleting listrik)	Seluruh data dan informasi terhapus	Pengecekan kelayakan peralatan secara berkala	Membuat *disaster recovery plan*
		Adanya instalasi listrik yang tidak benar	Terbakar atau rusaknya tempat penyimpanan	Membuat data center	Pemasangan instalasi sesuai prosedur

4.5 Penentuan Kemungkinan

Tahapan ini dilakukan untuk mendapatkan penilaian secara keseluruhan yang menunjukkan kemungkinan bahwa potensi kelemahan dapat dilaksanakan di-dalam membangun lingkungan ancaman terkait, kemungkinan jika potensi kelema.han dapat diidentifikasi oleh sumber ancaman yang dapat di kategorikan kedalam level tinggi, sedang atau rendah dapat dilihat pada Tabel 5 Penentuan Kemungkinan

Tabel 4 Penentuan Kemungkinan

Skor	Tingkat Kemungkinan	Definisi Kemungkinan
1.0	Tinggi	Sumber ancaman yang mempunyai risiko tinggi yang dapat merugikan perusahaan atau instansi,
0.5	Sedang	Sumber ancaman yang dapat merugikan instansi, tetapi instansi tersebut masih dapat melakukan control.
0.1	Rendah	Sumber ancaman yang memiliki risiko rendah, kontrol digunakan untuk mencegah ,mengurangi, atau menghambat suatu kerentanan yang akan terjadi di dalam perusahaan.

4.6 Analisa Dampak

Langkah penting berikutnya dalam mengukur tingkat risiko adalah menen-tukan dampak buruk dari akibat ancaman kelemahan tersebut. besar level dampak yang dapaat dilihat Tabel 6 Besarnya Level Dampak

Tabel 5 Besarnya Level Dampak

Skor	Besarnya Dampak	Defenisi Dampak
100	Tinggi	(a) Dapat mengakibatkan kehilangan dari aset atau sumber daya berwujud utama yang sangat mahal. (b) Dapat secara signifikan melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi.
50	Sedang	(a) Dapat mengakibatkan kehilangan yang sangat tinggi dari aset atau sumber daya berwujud utama yang sangat mahal. (b) Dapat melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi.
1	Rendah	(a) Dapat mengakibatkan hilangnya beberapa asset atau sum-ber daya (b) Secara nyata dapat mempengaruhi misi, reputasi, atau mi-nat organisasi.

4.7 Penentuan Risiko

Tahapan ini bertujuan untuk menilai tingkat risiko pada sistem informasi. Penentuan nilai akhir risiko diperoleh dengan mengalikan peringkat yang ditetapkan untuk kemungkinan ancaman (*likelihood*) dan dampak ancaman (*impact*) seperti pada Rumus 1 sebagai berikut :

Penilaian Risiko = Dampak x Peluang (1)

Untuk menentukan tingkat risiko digunakan matriks pada Tabel 7. Matriks Tabel 7 menunjukkan bagaimana tingkat risiko keseluruhan Tinggi, Sedang, dan Rendah diturunkan. Penentuan tingkat atau peringkat risiko ini mungkin subjektif berdasarkan hasil wawancara.

Tabel 6 Matriks Tingkat Risiko (sumber : (Gary Stoneburner & and Alexis Feringa, 2002)**)**

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Pada Tabel 8 Definisi Tingkat Risiko menggambarkan definisi tingkat risiko dari setiap tingkat yang dapat terjadi.

Tabel 7 Definisi Tingkat Risiko

Skor	Tingkat Kemungkinan	Definisi Kemungkinan
50-100	Tinggi	Jika observasi atau pengamatan di evaluasi sebagai risiko tinggi yang dapat mengakibatkan kerugian yang besar secara financial dan kontrol yang digunakan dapat mengurangi risiko tersebut, sehingga sesegera mungkin perlu diberlakukan tindakan korektif.
10-50	Sedang	Jika pengamatan risiko sedang dan dapat merugikan sebagian besar asset perusahaan. Tindakan korektif diperlukan danrencana harus dikembangkan untuk memasukkan tindakan ini dalam periode waktu yang wajar.
1-10	Rendah	Jika pengamatan di nilai risiko rendah mengakibatkan sebagiankecil kerugian dan kontrol yang dilakukan dapat mengurangi risiko yang terjadi.

Pada Tabel 9 Besarnya Tingkar Risiko Ancaman Alam adalah tabel menggambarkan besarnya tingkat risiko ancaman yang disebabkan oleh alam.

Tabel 8 Besarnya Tingkar Risiko Ancaman Alam

Ancaman	Penyebab Risiko	Dampak	Level		Kategori Risiko
			Peluang	Dampak	
Kebakaran	Tersambar petir	Merusak perangkat Keras dan infrastruktur pendukung	Rendah (0.1)	Rendah (10)	Rendah (1)

Pada Tabel 10 Besarnya Tingkat Risiko Ancaman Oleh Manusia dibawah ini adalah tabel menggambarkan besarnya tingkat risiko ancaman yang disebabkan oleh manusia

Tabel 9 Besarnya Tingkat Risiko Ancaman Oleh Manusia

Ancaman	Penyebab Risiko	Dampak	Level		Kategori Risiko
			Peluang	Dampak	
Human Error	Perancangan system kerja yang kurang baik	Pelaporan data yang Tidak akurat atau tidak tepat	Tinggi (1.0)	Tinggi (100)	Tinggi (100)

	Skill dan pengalaman yang kurang memadai	Terjadi kesalahan dalam menjalankan operasional perusahaan	Tinggi (1.0)	Tinggi (100)	Tinggi (100)
	Manajemen yang tidak menerapkan SOP	Pengambilan keputusan yang salah atau kurang tepat	Tinggi (1.0)	Tinggi (100)	Tinggi (100)
Virus	Penggunaan Flashdisk yang Tidak tertib	Hilangnya data/asset penting	Rendah (0.1)	Rendah (10)	Rendah (5)
	Jarang memperbarui antivirus	Software tidak dapat diakses	Sedang (0.5)	Tinggi (100)	Sedang (50)
	Mengunduh File yang tidak Jelas atau sembarangan	Hilang atau rusaknya data-data penting	Sedang (0,5)	Tinggi (100)	Sedang (25)
Hacker	Kurangnya *security awareness*	Perubahan data dan informasi yang tidak terotorisasi	Tinggi (1.0)	Tinggi(100)	Tinggi
	Tidak adanya audit trail atau *log*	Kehilangan data-data penting	Tinggi (1.0)	Sedang (50)	Sedang
	Enkripsi *password* pengguna	Password mudah ditebak oleh hacker	Tinggi (1.0)	Tinggi (100)	Tinggi

Pada Tabel 11 Besarnya Tingkat Risiko Ancaman Kesalahan Teknis dibawah ini adalah tabel menggambarkan besarnya tingkat risiko ancaman yang disebabkan oleh kesalahan teknis

Table 11. Besarnya Tingkat Risiko Ancaman Kesalahan Teknis

Ancaman	**Penyebab Risiko**	**Dampak**	**Level**		**Kategori Risiko**
			Peluang	Dampak	
Kegagalan Jaringan	ISP (Internet Service Provider) terputus	Sistemtidak dapat Diakses menggunakan jaringan luar.	Tinggi (1.0)	Sedang (50)	Sedang (50)
	Server down	Sistem tidak dapat diakses, proses dan pengolahan pelaporan terganggu.	Tinggi (1.0)	Tinggi (100)	Tinggi (100)
Kebakaran	Adanya hubungan arus pendek listrik	Seluruh data dan informasi terhapus.	Sedang (0.5)	Sedang (50)	Sedang (25)
	Adanya instalasi listrik yang tidak benar	Rusaknya tempat Penyimpanan data.	Tinggi (1.0)	Tinggi (100)	Tinggi (100)

Hasil penilaian risiko Tabel 9 kemudian dibuat presentase setiap tingkatan risiko rendah, sedang dan tinggi. Grafik risiko alam bisa dilihat pada Gambar 2 grafik risiko alam. Untuk kategori risiko rendah 100% sedang 0% dan tinggi 0%.

Gambar 2 Grafik Risiko Alam

Grafik risiko Manusia bisa dilihat pada Error! Reference source not found.. Untuk kategori risiko rendah 11% sedang 33% dan tinggi 56%

Gambar 3 Grafik Risiko Manusia

Grafik risiko teknis bisa dilihat pada Gambar 4 Grafik Risiko Teknis. Untuk kategori risiko rendah 25% sedang 25% dan tinggi 50%

Gambar 4 Grafik Risiko Teknis

Grafik risiko keseluruhan bisa dilihat pada **Error! Reference source not found..** Untuk kategori risiko rendah 7% sedang 86% dan tinggi 7%

Gambar 5 Grafik Risiko Keseluruhan

4.8 Rekomendasi Kontrol

Tujuan dari rekomendasi kontrol adalah untuk mengurangi tingkat risiko pada sistem informasi yaitu dengan memberikan rekomendasi terhadap kebijakan yang sudah ada atau yang sudah di lakukan terkait dengan penilaian risko.

Tabel 12 berikut ini adalah tabel rekomendasi pengendalian keamanan kontrol yang harus di lakukan oleh PT.ABC untuk mengurangi risiko dan mengamankan data-data yang ada di dalam sistem informasi dari ancaman yang dapat terjadi:

Table 12 Rekomendasi pengendalian keamanan control

No	Ancaman	Motivasi	Tindakan Ancaman	Rekomendasi Pengendalian Ancaman
1	kebakaran	Tidak disengaja	1. Karena adanya arus pendek aliran listrik 2. Terkena sambaran petir 3. Instalasi listrik yang tidak benar	1. Membuat distater recovery plan 2. Membuat data center distater recovery center yang kuat dan tahan terhadap bencana alam 3. Melakukan backupdan memasang instalasi listrik sesuai prosedur 4. Mengaktifkan kembali fungsi hydrant
2	Human Error	Tidak disengaja	1. Menginputkan data tidak benar 2. Penyalahgunaan hak akses 3. Merusak data Pada media penyimpanan	1. Melakukan pengawasan kepada pegawai 2. Melakukan training secara berkala kepada user 3. Melakukan pengawasan secara internal terhadap apa saja dikerjakan
3	Virus	Pengerusakan	1. Kegagalan operasi software 2. Perubahan data 3. Rusak atau kehilangan data	1. Menggunakan antivirus yang berlisensi 2. Mengelompokan data berdasarkan kegunaannya secara jelas lalu membuat backupnya 3. Membuat peraturan tertulis tentang system pengunduhan file
4	Hacking	Pengerusakan	1. Penyelundupan file 2. Perubahan data dan informasi 3. Pencurian data	Update kode sistem dan memperbaiki celah yang rentan agar sistem lebih handal.
5	Kegagalan ISP jaringan	Tidak disengaja	Permasalahan pada provider jaringan	Meningkatkan kehandalan jaringan dengan melakukan redudansi perangkat jaringan pendukung system sebagai backup jika salah satunya mengalami gangguan

4.9 Dokumentasi

Setelah penilaian risiko selesai hasilnya harus di dokumentasikan ke dalam bentuk laporan. Dokumentasi menggambarkan keseluruhan proses penilaian risiko, mulai dari ancaman dan kerentanan, pengukuran risiko dan rekomendasi control untuk diimplementasikan. Dari hasil laporan dapat membantu manajemen instansi untuk membuat sebuah keputusan tentang perubahan kebijakan, prosedur, maupun anggaran.

5. KESIMPULAN DAN SARAN

Kesimpulan

Penelitian telah dilakukan pada PT ABC, dimana penelitian dilakukan dengan cara mengukur risiko sistem informasi yaitu dengan menggunakan metode NIST SP 800-30. Berdasarkan penelitian yang telah dilakukan dapat disimpulkan beberapa hal sebagai berikut:

1. Pada proses pengolahan data dihasilkan ancaman-ancaman yang sudah teridentifikasi. Ancaman yang terjadi pada sistem informasi yaitu kebakaran, human error, virus, hacking dan kegagalan jaringan. Ancaman ancaman tersebut

yang kerap kali timbul dan menjadi permasalahan selama pelayanan berjalan dan menyebabkan proses layanan terganggu.
2. Pada proses identifikasi ancaman yang terjadi pada sistem informasi telah ditemukan tingkat risiko yang berbeda pada tiap kategori. Level risiko yang diidentifikasi berdasarkan dari hasil perhitungan kuesioner.
3. Hasil dari penilaian risiko yang terjadi pada sistem informasi mem- berikan rekomendasi kontrol yang disarankan terhadap ancaman risiko yang terjadi, sehingga dapat menjadi acuan bagi instansi untuk dapat digunakan untuk kontrol selanjutnya
4. Setelah melakukan perhitungan didapatkan risiko alam untuk kategori risiko rendah 100% sedang 0% dan tinggi 0%., Risiko manusia untuk kategori risiko rendah 11% sedang 33% dan tinggi 56%, Risiko teknis untuk kategori risiko rendah 25% sedang 25% dan tinggi 50%, Risiko keseluruhan untuk kategori risiko rendah 7% sedang 86% dan tinggi 7%

Saran

Beberapa saran yang dapat dijadikan masukan antara lain:

1. Melakukan pembaharuan informasi terhadap sistem dengan mengumpulkan risiko-risiko secara rutin yaitu sekali dalam setahun sehingga dapat memi-nimalkan terjadinya risiko atau mencegah risiko yang akan terjadi.

2. Membuat pendokumentasian untuk setiap prosedur dan kejadian risiko yang ada, sehingga memudahkan aktivitas audit dan memperkecil risiko internal yang terjadi.

3. Manajemen risiko dapat berjalan dengan baik jika adanya dukungan dengan komitmen manajemen level atas dan partisipasi bagian rektorat, serta ke-sadaran dan kerjasama dari seluruh penanggung jawab yang harus mengiku-ti prosedur dan mematuhi kontrol yang telah ditetapkan.

REFERENSI

Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Elanda, A., & Buana, R. L. (2021). Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma). *Elkom : Jurnal Elektronika Dan Komputer*, *14*(1), 141–151. https://doi.org/10.51903/elkom.v14i1.387

Gary Stoneburner, A. G., & and Alexis Feringa. (2002). Risk Management Guide for Information Technology Systems. In *Expert Opinion on Therapeutic Targets*. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Ghazouani, M., Faris, S., Medromi, H., & Sayouti, A. (2014). Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications*, *103*(8), 36–42. https://doi.org/10.5120/18097-9155

Handayani, N. U., Wibowo, A., Sari, D. P., Satria, Y., & Gifari, A. R. (2018). Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect dan Analysis Berbasis Framework ISO 27001. *Teknik*, *39*(2), 78–85. https://doi.org/10.14710/teknik.v39n2.15918

Putra, R. D. A., Ambarwati, A., & Setiawan, E. (2019). Evaluasi Manajemen Risiko Teknologi Informasi Berdasarkan Framework COBIT 5 Pada PT.BTM. *JSI: Jurnal Sistem Informasi (E-Journal)*, *11*(2), 1754–1762. https://doi.org/10.36706/jsi.v11i2.9103

Putro, A. A., Ambarwati, A., & Setiawan, E. (2021). Analisa Manajemen Risiko E-Learning Edlink

Menggunakan Metode NIST SP 800-30 Revisi 1. *Jurnal Teknologi Dan Informasi*, *11*(2), 125–136. https://doi.org/10.34010/jati.v11i2.5314

Tohidi, H. (2011). The role of risk management in IT systems of organizations. *Procedia Computer Science*, *3*(2010), 881–887. https://doi.org/10.1016/j.procs.2010.12.144