Penilaian Risiko Sistem Informasi Keamanan Data Karyawan Dengan Menggunakan Framework Nist Sp 800-30 pada Perusahaan XYZ
Institut Teknologi Nasional Bandung

ADITYA NUGRAHA SUSANTO[1], NUR FITRIANTI FAHRUDIN[2]

[1]Institut Teknologi Nasional
Email:
adityanugraha1a@gmail.com

Received DD MM YYYY | *Revised* DD MM YYYY | *Accepted* DD MM YYYY

ABSTRAK

NIST 800-30 merupakan sebuah kerangka kerja yang biasa digunakan untuk melalukan manajemen risiko. Secara umum manajemen risiko dibagi kedalam tiga tahapan yaitu risk assesment, risk mitigation dan risk evaluation. Pada paper ini peneliti hanya berfokus kepada risk assesment yang terdiri dari sembilan tahapan yaitu System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, Results Documentation. Tahapan risk assesment ini di implementasikan terhadap sebuah sistem informasi yang terdapat pada sebuah perusahaan dengan mengidentifikasi ancaman teknis seperti jaringan rusak dan kebakaran. Hasil yang didapat adalah risiko rendah 29%, risiko sedang 71% dan risiko tinggi 0%

***Kata kunci**: Risiko, Sistem Informasi, NIST SP 800-30, Data Karyawan, Penilaian Risiko*

ABSTRACT

NIST 800-30 is a framework commonly used to perform risk management. In general, risk management is divided into three stages, namely risk assessment, risk mitigation and risk evaluation. In this paper, researchers only focus on risk assessment, which consists of nine stages, namely System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, Results Documentation. This risk assessment stage is implemented on an information system contained in a company by identifying technical threats such as damaged networks and fires. The results obtained are low risk 29%, moderate risk 71% and high risk 0%

***Keywords**: Risk, Information System, NIST SP 800-30, Employee Data, Risk Assessment*

1. PENDAHULUAN

Penggunaan teknologi informasi di perusahaan telah membawa kemudahan, terutama dalam hal kemampuan mengakses informasi yang dikemas dalam sistem informasi digital dengan cepat dan mudah. Namun, dengan berkembangnya teknologi informasi, semakin banyak orang memiliki kebutuhan untuk mengakses informasi, dan informasi menjadi semakin penting. Kemudian ada individu atau kelompok, baik internal maupun eksternal, yang menggunakan aset untuk tujuan yang berbeda dan berusaha memperoleh aset informasi dengan cara yang berbeda. Teknologi informasi dapat digunakan untuk menjaga anonimitas, yang memudahkan individu untuk terlibat dalam perilaku yang tidak etis dan kriminal, termasuk merusak aset TI dan memperoleh informasi secara ilegal.

Penggunaan teknologi informasi di perusahaan membawa kemudahan, khususnya akses informasi yang dikemas dalam sistem informasi digital sangat cepat dan mudah. Namun dengan berkembangnya teknologi informasi, keinginan masyarakat untuk memiliki dan menguasai informasi semakin kuat. Kemudian ada individu atau kelompok internal dan eksternal yang menggunakan aset informasi untuk tujuan yang berbeda dan melakukan yang terbaik untuk mendapatkan aset informasi dengan cara yang berbeda. Komputer dapat digunakan untuk menjaga anonimitas, sehingga memudahkan seseorang untuk melakukan perilaku tidak etis dan kriminal, termasuk perusakan properti komputer dan akses ilegal ke informasi. lubang keamanan informasi. Jika masalah ini tidak dapat diselesaikan secara terus menerus, maka akan mempengaruhi atau membahayakan keberlangsungan sistem ini.

Metode yang dapat digunakan untuk mengelola risiko keamanan informasi adalah OCTAVE, NIST SP 800-30 dan ISO 27001. Metode OCTAVE hanya digunakan dalam organisasi (audit organisasi), ISO 27001 biasanya mengacu pada directivity tinggi. NIST SP 800-30 memberikan kontribusi lebih, seperti: menyediakan pembuat keputusan dengan informasi keamanan informasi yang konsisten dan komprehensif, pemodelan sumber daya terstruktur, identifikasi ancaman yang mudah, Pengambil keputusan dapat menerima risiko tanpa ragu-ragu, karena setiap risiko telah dipelajari. Penelitian ini akan menggunakan NIST SP 800-30 sebagai metode yang akan digunakan untuk mengatasi permasalahan di atas.

2. METODOLOGI

2.1 Pengumpulan Data

Penelitian akan dilakukan pada tahap pengumpulan data sehingga dapat digunakan seagai acuan dalam melakukan analisis dan penilaian risiko

1. Data primer

   Data primer adalah data yang diperoleh secara mandiri langsung dari sejumlah sumber yang relevan, termasuk hasil wawancara konsultasi dengan sumber yang relevan.

2. Data sekunder

   Data sekunder adalah data yang diperoleh dari artikel penelitian dan jurnal. Dalam penelitian ini, data sekunder dikumpulkan dari dokumen organisasi

2.2. NIST

NIST (National Institute Standard Technology) adalah lembaga federal non-regulasi di Amerika Serikat yang bertugas mengembangkan dan mempromosikan langkah-langkah, standar, dan teknologi untuk meningkatkan produktivitas dan meningkatkan kualitas. NIST menerbitkan sejumlah publikasi standar. Standar publikasi terkait keamanan informasi adalah:
NIST SP80030

Tahapan manajemen risiko dibagi menjadi tiga tahap, yaitu

1. Risk Asessment (Penilaian risiko)
   Penilaian risiko merupakan proses pertama yang dilakukan dalam penerapan metode manajemen risiko. Saat melakukan penilaian risiko atau penilaian risiko, ada 9 langkah untuk mengidentifikasi potensi ancaman dan risiko yang terkait dengan sistem informasi. Hasil penilaian risiko adalah mengidentifikasi tindakan pengendalian pengendalian yang tepat untuk mengurangi atau menghilangkan risiko

2. Risk Mitigation (Pengurangan risiko)
   Pengurangan risiko adalah langkah kedua setelah penilaian risiko dalam proses manajemen risiko.Langkah selanjutnya adalah memprioritaskan, mengevaluasi, dan mengimplementasikan aset

3. Assessment and Evaluation
   Tahap evaluasi merupakan tahapan dimana dilakukan penilaian terhadap penerapan pengendalian risiko. Pekerjaan ini dilakukan dalam jangka waktu tertentu. Misalnya setiap tahun hal ini dilakukan untuk menilai kemali apakah alat atau metode pengurangan risiko masih relevan. Atau ada modul atau komponen software yang selalu *up to date*. Penilaian ini dilakukan secara keseluruhan dan melibatkan manajemen senior tim penilaian risiko dan administrator sistem individu.

Penelitian ini difokuskan hanya pada tahap risk asessment. Risk assessment dibagi menjadi Sembilan tahap sesuai dengan tahapan penilaian risiko NIST SP 800-30 (Kroczak et al., 2006) yaitu:

1. *System Characterization*
   Menentukan sistem komputer sumber daya dan informasi.
2. *Threat Identification*
   Pertimabangan potensi ancaman seagai sumer potensi kerentanan dan kontrol yang ada.
3. *Vulnerability Identification*
   Mengidentifikasi kerentanan digunakan untuk mengemangkan daftar kerentanan sistem yang dapat dieksploitasi.
4. *Control Analysis*
   Analisis pengendalian atau rencana implementasi organisasi untuk mengurangi atau menghilangkan potensi ancaman.
5. *Likelihood Determination*
   Proses peringkat kerentanan potensial dapat dilakukan di lingkungan erahaya. Faktor yang perlu dipertimangkan adalah ancaman (sumer dan kapasitas) sifat kerentanan dan keeradaan dan efektivitas tindakan pengendalian jika diterapkan.
6. *Impact Analysis*
   Langkah ini membantu mengidentifikasi dampak negatif yang dihasilkan dari penerapan kerentanan keamanan yang berhasil.

7. *Risk Determination*
   Penilaian risiko dalam sistem komputer dilakukan pada tahap ini.
8. *Control Recommendations*
   Langkah ini mengevaluasi tindakan pengendalian yang dapat mengurangi atau menghilangkan risiko yang teridentifikasi. Kontrol yang direkomendasikan harus mengurangi risiko terhadap sistem dan data TI ke tingkat risiko yang dapat diterima.
9. *Results Documentation*
   Pada tahapan ini menyusun dokumentasi sesuai yang sudah direkomendasikan pada tahap sebelumnya agar dapat membantu perusahaan dalam pengambilan keputusan

2.3. Cara Perhitungan

Dalam NIST sp800-30 (Kroczak et al., 2006) terdapat matriks 3x3 yang digunakan untuk menghitung tingkatan risiko sesuai dengan nilainya. Matriks ini dapat dilihat pada

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

Gambar 1 Matriks 3x3

Untuk menentukan tingkatan risiko NIST SP 800-30 ini ada dua table yang digunakan sebagai penentunya yaitu table dan table

Tabel 1 dampak

Skor	Besarnya Dampak	Defenisi Dampak
100	Tinggi	(a) Dapat mengakibatkan kehilangan yang sangat tinggi dari aset atau sumber daya berwujud utama yang sangat mahal. (b) Dapat secara signifikan melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. (c) Dapat menyebabkan kematian manusia atau cedera serius
50	Sedang	(a) Dapat mengakibatkan kehilangan yang sangat tinggi dari aset atau sumber daya berwujud utama yang sangat mahal.

Skor	Besarnya Dampak	Defenisi Dampak
		(b) Dapat melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. (c) Dapat menyebabkan cedera pada manusia.
1	Rendah	(a) Dapat mengakibatkan hilangnya beberapa asset atau sum-ber daya (b) Secara nyata dapat mempengaruhi misi, reputasi, atau mi-nat organisasi.

Tabel 2 tingkat kemungkinan

Skor	Tingkat Kemungkinan	Definisi Kemungkinan
51-100	Tinggi	Jika observasi atau pengamatan di evaluasi sebagai risiko tinggi yang dapat mengakibatkan kerugian yang besar secara financial dan control. sesegera mungkin perlu diberlakukan tindakan korektif.
11-50	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.

Rumus yang digunakan untuk menentukan risikonya sebagai berikut

$$\text{Penilaian Risiko} = \text{Dampak x Peluang} \quad (1)$$

3. ISI

3.1 System Characterization

Komponen karakteristik sistem informasi ini meliputi: perangkat keras, aplikasi, alat-alat jaringan, data, dan operator. Perangkat keras client memakai personal personal komputer menggunakan windows 10. Server memakai, mysql dan pemrogram php .

Penggunaan system informasi pendataan karyawan ini dipakai untuk melihat data karyawan perusahaan ketika melakukan ekspedisi yang memakai system informasi

3.2 Threat Identification

Mengidentifikasi kemungkinan ancaman yang akan timbul pada perusahaan XYZ

Teknis: kesalahan yang diakibatkan oleh server atau jangkauan lain di luar kesalahan manusia/programmernya.

Tabel 3 kesalahan teknis

Sumber ancaman	Sumber Penyebab
Jaringan rusak	(a) jaringan terputus (b) ada permasalahan pada provider
Kebakaran	Kornsleting atau arus pendek listrik

3.3 Vulnerability Identification

analisis ancaman terhadap sistem harus mencakup analisis kerentanan yang terkait dengan sistem yang sedang dievaluasi. Tujuannya adalah untuk menyusun daftar kerentanan atau kelemahan dalam sistem yang dapat dimanfaatkan oleh sumber ancaman potensial.

Tabel 4 analisis dampak

Ancaman	Sumber Ancaman	penyebab	Ancaman
Human error	Manusia	1.Penyalahgunaan hak akses 2.Karyawan yang ceroboh	(a) jaringan terputus (b) ada permasalahan pada provider

3.4 Control Analysis

Tujuan tahapan ini adalah untuk meninjau kontrol yang ada, yang telah diterapkan atau yang sudah direncanakan oleh perusahaan untuk mengurangi potensi ancaman dan kelemahan sistem.

Tabel 5 Kontrol analisis

Ancaman	Penyebab ancaman	Risiko	Kontrol saat ini	Rencana Kontrol
Kerusakan ISP	Terputusnya ISP	System tidak dapat di akses menggunakan internet	Menggunakan hanya satu ISP	Menambah akses cadangan
	Server down	Mengakibatkan pengolahan dan pelaporan terganggu.	Server tidak bias menangani banyak user sekaligus	Upgrade spesifikasi server

3.5 Likelihood Determination

Mendapatkan penilaian secara keseluruhan yang menunjukkan level kemungkinan yang sudah dikategorikan pada **Tabel 2 tingkat kemungkinan**

Ancaman	Penyebab ancaman	Tingkat kemungkinan
Kerusakan ISP	Terputusnya ISP	Sedang
	Server down	Tinggi

3.6 Impact Analysis

Pada tahapan ini menganalisis dampak buruk yang akan terjadi pada kerentan yang memungkinkan terjadi

Tabel 6 dampak ancaman

ancaman	Nilai Dampak	Dampak
Kerusakan ISP	Sedang	System tidak dapat di akses menggunakan internet
	Rendah	Mengakibatkan pengolahan dan pelaporan terganggu

3.7 Risk Determination

Tujuan pada tahap ini adalah untuk menilai tingkat risiko sistem informasi. Menentukan risiko kemungkinan ancaman yang ada guna menilai tingkat risiko terhadap suatu sistem informasi.

$$\text{Penilaian Risiko} = \text{Dampak x Peluang} \quad (1)$$

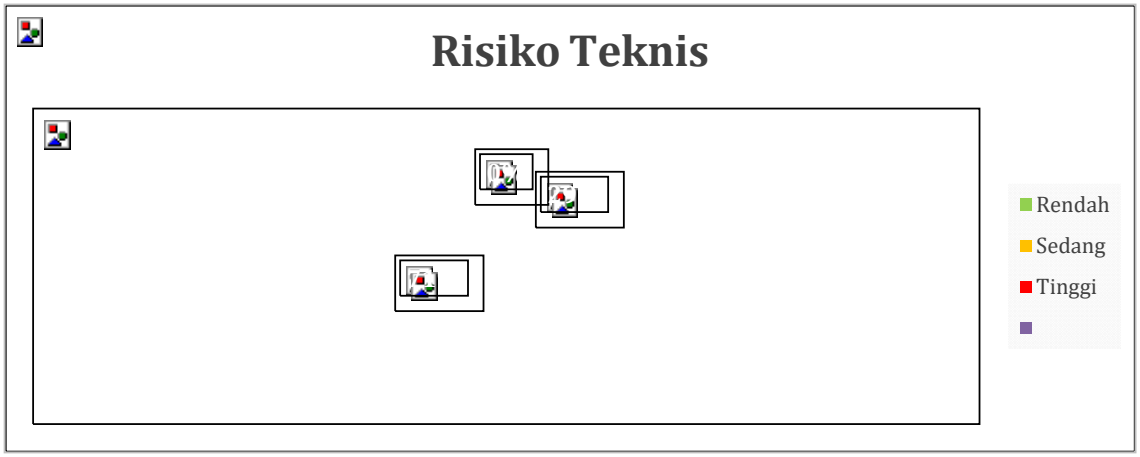
$$25 = 0.5 \text{ x} 50$$

Tabel 7 kemungkinan ancaman

Ancaman	Penyebab Risiko	Dampak	Level		Kategori Risiko
			Peluang	Dampak	
Kerusakan ISP	Terputusnya ISP Server down	System tidak dapat di akses menggunakan internet	Sedang (0.5)	Sedang (50)	Sedang (25) Rendah

Ancaman	Penyebab Risiko	Dampak	Level Peluang	Dampak	Kategori Risiko
		Mengakibatkan pengolahan dan pelaporan terganggu	Tinggi (1.0)	Rendah (10)	(10)

Gambar 2 Grafik risiko teknis menunjukan hasil risiko rendah 29%, risiko sedang 71% dan risiko tinggi 0%



Gambar 2 Grafik risiko teknis

3.8 Control Recommendations

Tahap ini, merekomendasikan pengendalian yang dapat mengurangi atau menghilangkan risiko yang telah teridentifikasi dan dievaluasi.

Tabel 8 rekomendasi pengendalian

Ancaman	Motivasi	Tindakan ancaman	Rekomendasi pengendalian ancaman
Kerusakan ISP	Tidak disengaja	Permasalahan pada provider jaringan	Meningkatkan kehandalan jaringan dengan melakukan redudansi perangkat jaringan pendukung system sebagai backup jika salah satunya mengalami gangguan.

3.9 Results Documentation

Tahapan ini, membuat laporan penilaian risiko yang menggambarkan proses penilaian risiko sebelum dan sesudah implementasi yang nantinya akan membantu manajemen presuahaan dalam pengambilan keputusan.

4. KESIMPULAN

Pada proses penilaian risiko dihasilkan ancaman-ancaman yang sudah teridentifikasi. proses identifikasi ancaman yang terjadi pada sistem informasi telah ditemukan tingkat risiko yang berbeda pada tiap kategori. Hasil dari penilaian risiko yang terjadi pada sistem informasi memberikan rekomendasi kontrol yang disarankan terhadap ancaman risiko yang terjadi. Menghasilkan risiko rendah 29%, risiko sedang 71% dan risiko tinggi 0%.

DAFTAR PUSTAKA

Dan Constantin. (2011). Information Security Standard. *Journal of Mobile Embedded and Distributed Systems*.

Kroczak, T. J., Baran, J., Pryjma, J., Siedlar, M., Reshedi, I., Hernandez, E., Alberti, E., Maddika, S., & Los, M. (2006). The emerging importance of DNA mapping and other comprehensive screening techniques, as tools to identify new drug targets and as a means of (cancer) therapy personalisation. *Expert Opinion on Therapeutic Targets*, *10*(2), 289–302. https://doi.org/10.1517/14728222.10.2.289

Mahardika, F. (2017). *Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)*. *02*(02).

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). In *Jurnal CoreIT* (Vol. 2, Issue 2).

Ashari, R. A. (2018). Rencana Penerapan Cyber-Risk Management Menggunakan NIST CSF dan COBIT 5. *Jurnal Sistem Informasi*, *14*(2), 83–89. https://doi.org/10.21609/jsi.v14i2.702

Dan Constantin. (2011). Information Security Standard. *Journal of Mobile Embedded and Distributed Systems*.

Darril Gibson. (2011). *managing Risk In Information System*.

Elanda, A., & Tjahjadi, D. (2018). Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute of Standards and Technology) Sp 800-30 (Studi Kasus Disinfolahtaau Mabes Tni Au). *Infoman's*, *12*(1), 1–13. https://doi.org/10.33481/infomans.v12i1.45

Farida, A. D. (2020). *Informasi Koperasi Syariah Menggunakan Framework*. *8*(1), 1–14.

G. Stoneburner, A. Goguen, & A. Feringa. (2002). Risk Management Guide for Information Technology System. *Recommendation of National Institute of Standards and Technology Special Publikation 800-300*, *7*.

Izatri, D. I., Rohmah, N. I., & Dewi, R. S. (2020). Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 50. https://doi.org/10.30865/jurikom.v7i1.1756