# ANALISIS RESIKO KEAMANAN SISTEM INFORMASI DITINJAU DARI SISI PROSES
## (Studi Kasus Di Pemkot XXX)

**Sony Susanto**

**ABSTRAK**

Pada era informasi ini kita perlu mengelola informasi dengan baik untuk mencapai tujuan dari yang kita inginkan. Untuk itu maka kita harus mengetahui proses dari pengelolaan informasi tersebut.

Faktor proses dari pengeloaan informasi ini sangat penting untuk mengamankan informasi yang kita kelola. Kita mengetahui bahwa keamanan informasi pada prinsipnya terdiri dari tiga komponen yang harus kita amankan yaitu kerahasiaan informasi, integrasi infromasi dan ketersediaan informasi tersebut.

Telah dilaporkan bahwa terjadi insiden jaringan pada bulan Juli sejumlah 465 dan bulan Agustus sejumlah 591 tahun 2016 sehinggal jumlah terjadinya insiden jaringan adalah 1.056 (ID-CERT 2016)

Kata Kunci : analisa, resiko, keamanan, proses, informasi

## I. PENDAHULUAN

Fokus penelitian ini adalah manajemen resiko keamanan sistem informasi. Ruang lingkupnya “analisis resiko keamanan sistem infromasi ditinjau dari sisi proses pada sistem informasi di Pemkot XXX”.

### 1.1. Identifikasi Masalah

Pada tulisan ini akan dilakukan pembahasan dan penyajian berkaitan dengan sistem iinformasi dan resiko keamanannya yang terdiri dari resiko-resiko keamanan sistem informasi, sistem keamanan, keamanan informasi, masalah keamanan dan solusinya ditinjau dari sisi proses pengelolaannya.

### 1.2. Tujuan Penelitian

Tujuan utama penelitian ini adalah untuk mengidentifikasi resiko-resiko keamanan pada sistem informasi ditinjau dari proses pengeloaan sistem informasi serta mengkategorisasikan resiko-resikonya.

Manfaat yang didapat pada penelitian ini akan membentuk suatu formula untuk mendesign sistem yang aman dalam bentuk framework untuk menanalisis resiko keamanan sistem informasi.

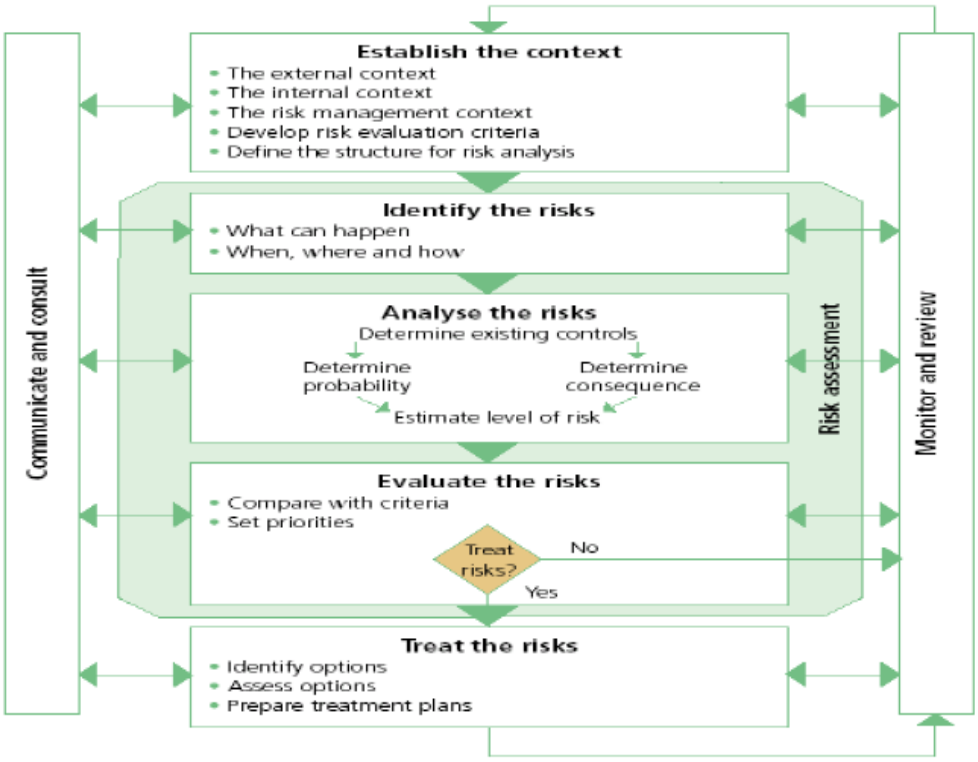
## II. LANDASAN TEORI

### 2.1. Proses Manajemen Resiko

Resiko didefinisikan sebagai posibilitas terjadinya sesuatu yang dapat berdampak pada tujuan. Resiko diukur menggunakan konsekuensi dan likehood. Manajemen resiko merupakan suatu proses berulang dari langkah-langkah yang sudah didefinisikan secara baik dan terurut dengan mengkontribusikan resiko dan dampaknya (OB/7, 1999).

### 2.2. Kerangka Manajemen Resiko Berdasarkan Standar Australia

Pada penelitian ini standar yang dipakai adalah Standar Australia/New Zealand (AS/NZS 4360:1999) untuk manajemen resikonya. Adapun elemen utama dari standar tersebut adalah sebagai berikut :




**Gambar 1. Proses Manajemen Resiko (OB/7, 1999).**

Gambar 1 tersebut merupakan proses manajemen resiko yang berdasarkan Standar Australia (OB/7, 1999) yang gunanya sebagai panduan langkah-langkah dalam menentukan resiko-resiko yang harus diidentifikasi serta dianalisis dan dievaluasi sehingga dapat dikelola resiko-resiko tersebut.

### 2.3. Pengaruh Resiko Keamanan Terhadap Resiko Bisnis

Grup Gartner (Witty, et al..2001) menyarankan bahwa resiko dapat diukur dampaknya atas jenis kerugian sebagai berikut : Finansial, Keuntungan kompetitif, Legal atau regulator, Operasional atau layanan dan Reputasi market.

### 2.4. Pelanggaran Keamanan

Telah dilaporkan bahwa terjadi insiden jaringan pada bulan Juli 465 sejumlah 465 dan bulan Agustus 591 tahun 2016 sehinggal jumlah terjadinya insiden jaringan adalah 1.056 (ID– CERT 2016)

Selain itu terjadi phising pada bulan Juli sejumlah 615 dan bulan Agustus sejumlah 591 sehingga jumlah terjadinya phising adalah 1.206 pada tahun 1916 (ID – CERT 2016).

### 2.5. Sistem Informasi

Kata ‘sistem’ mengandung arti ‘kumpulan dari komponen-komponen yang memiliki unsur keterkaitan antara satu dan lainnya’. Sistem informasi merupakan suatu kumpulan dari komponen-komponen dalam perusahaan atau organisasi yang berhubungan dengan proses penciptaan dan pengaliran informasi (Indrajit,2002).

### 2.6. Keamanan Sistem Informasi

Definisi keamanan sistem informasi menurut ITS (badan standard di swedia ) adalah “Keamanan dalam system informasi yang meliputi keamanan ADP *(Automatic Data Processing)* dan keamanan komunikasi”.

Sedangkan definisi keamanan sistem komputer menurut Gollman adalah “Berkaitan dengan teknik yang dilakukan untuk memelihara keamanan dalam sistem komputer”.

## III. PEMBAHASAN

### 3.1. Metodologi Analisis Resiko

Metodologi yang digunakan pada studi kasus ini berdasarkan Standar Australia. Alasan digunakan Standar Australia pada studi kasus ini karena standar ini sudah matang dan sudah digunakan di seluruh dunia. Pada dunia bisnis dikenal dengan level

resiko bisnis yang merupakan hasil dari *vulnerability*.Adapun formula untuk mentranslate dari *vulnerabilty* teknik terhadap level resiko bisnis itu adalah sebagai berikut:

**"Residual Risk = (Impak dari Inherent Risk) X Peluang (Vulnerabilities – Countermeasure)"**

Keterangan:

*Residual Risk* : Merupakan tingkat keseriusan setiap resiko.

Impak dari *Inherent Risk* : Merupakan tingkat negatif pada objek bisnis dimana skenario resiko itu terjadi.

Peluang : Merupakan peluang terjadinya resiko terbagi menjadi dua yaitu :

a. *Vulnerability* : Merupakan kelemahan sistem yang ada dan dapat menimbulkan resiko dari anacaman terhadap sistem itu.

b. Countermeasure : Merupakan kontrol yang dapat memberi efek untuk memitigasi terhadap resiko inherent. Ini bisa berbentuk dalam teknik, prosedur, manual, atau otomatis.

### 3.2. Ukuran Kualitatif Konsekuen atau Impak

Impak : Tingkat dampak jika terjadi eksploitasi pada *vulnerability*.

a. T (impak tinggi) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan pada opersional atau keuangan atau memalukan organisasi.

b. S (impak sedang) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan atau *unavailability (denial of service)* pada system internal.

c. R (impak rendah) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan terbukanya informasi tentang sistem dan struktur jaringan internal.

### 3.3. Ukuran Kualitatif Peluang

Peluang : Merupakan peluang terjadinya suatu resiko.

a. T (peluang tinggi) : Dimana *vulnerability* diketahui dengan baik, dapat dieksploitasi dengan tool-tool dan teknik-teknik yang tersedia di internet, serta hanya memerlukan pengalaman dan engetahuan yang sedikit.

b. S (peluang sedang) : Dimana vulnerabilty tidak langsung nyata teridentifikasi, tapi memerlukan penelitian, ketekunan, serta pembiasaan penggunaan teknik dan tool.

c. R (peluang rendah) : Dimana *vulnerability* diidentifikasi memerlukan tingkat pengetahuan dan teknik yang tinggi dan teknik serta *tool* yang tak tersedia di umum.

### 3.4. Residual Risk

Residual Risk : Tingkat keseriusan resiko terhadap bisnis organisasi.

a. T (resiko tinggi) : Dimana isu harus segera dilakukan pencegahan efek negatif pada objek bisnis.

b. S (resiko sedang) : Dimana isu harus dengan cepat dilakukan pengurangan terhadap resiko.

c. R (resiko rendah) : Dimana isu harus dengan segera meningkatkan keamanan.

**Tabel 1**
**Analisa resiko kualitatif – tingkat resiko (OB/7, 1999)**

| Konsekuen | Peluang | | |
|---|---|---|---|
| | Rendah | Sedang | Tinggi |
| Tinggi | S | T | T |
| Sedang | R | S | T |
| Rendah | R | R | S |

Keterangan :

R : Resiko rendah

S : Resiko sedang

T : Resiko tinggi

### 3.5. Kategorisasi Resiko

Kategorisasi resiko ini dilakukan berdasarkan tujuh prinsip keamanan yaitu :

a. *Intrusion* : Menjamin bahwa akses terhadap sistem dan informasi hanya dapat dilakukan melalui metode akses yang terotorisasi.

b. *Authentication* : Menjamin bahwa hanya orang yang terotorisasi yang dapat mengakses sistem dan informasi.

c. *Authorization* : Menjamin bahwa akses terhadap sistem dan informasi sesuai dengan otorisasi yang diberikan pada user.

d. *Encryption* : Proteksi informasi sehingga terlindungi ketika informasi itu dikirim dan disimpan pada storage.

e. *Accountability* : Menjamin bahwa akses terhadap sistem dan informasi oleh user tercatat secara benar.

### 3.6. Hasil Penelitian

Setelah dilakukan penelitian dan evaluasi simpeg di Pemkot XXX maka laporan hasil penelitian dan analisisnya adalah sebagai berikut :

**Tabel 2**
**Hasil Penelitian**

| No | Komponen Resiko | Peluang | Impak | Residual Risk | Penyebab Resiko |
|---|---|---|---|---|---|
| | | T/S/R | T/S/R | T/S/R | O/U/I/N |
| 1 | Intrusion | R | R | T | I |
| 2 | Authentication | T | T | R | U |
| 3 | Authorization | T | R | S | U |
| 4 | Encryption | R | R | T | O |
| 5 | Acountability | S | S | R | U |
| 6 | Availbilty | S | T | R | O |
| 7 | Endurability | T | R | S | N |

#### 3.6.1. Penjelasan Pengisian Kuesiomer

Untuk mengisi kuesioner maka penjelasannya sebagai berikut

1. Peluang : Merupakan peluang terjadinya suatu resiko.
   a. T (peluang tinggi) : Dimana *vulnerability* diketahui dengan baik, dapat dieksploitasi dengan tool-tool dan teknik-teknik yang tersedia di internet, serta hanya memerlukan pengalaman dan pengetahuan yang sedikit.
   b. S (peluang sedang ) : Dimana *vulnerabilty* tidak langsung nyata teridentifikasi, tapi memerlukan penelitian, ketekunan, serta pembiasaan penggunaan teknik dan tool.
   c. R (peluang rendah) : Dimana *vulnerability* diidentifikasi memerlukan tingkat pengetahuan dan teknik yang tinggi dan teknik serta tool yang tak tersedia di umum.
2. Impak : Tingkat dampak jika terjadi eksploitasi pada *vulnerability*.
   a. T (impak tinggi) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan pada opersional atau keuangan atau memalukan organisasi.
   b. S (impak sedang) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan kerusakan atau *unavailability* (*denial of service*) pada system internal.

c. R (impak rendah) : Dimana eksploitasi pada *vulnerability* dapat mengakibatkan terbukanya informasi tentang sistem dan struktur jaringaninternal.

3. Residual Risk : Tingkat keseriusan resiko terhadap bisnis organisasi.

a. T (resiko tinggi) : Dimana isu harus segera dilakukan pencegahan efek negatif pada objek bisnis.
b. S (resiko sedang) : Dimana isu harus dengan cepat dilakukan pengurangan terhadap resiko.
c. R (resiko rendah) : Dimana isu harus dengan segera meningkatkan keamanan.

**Tabel 3**
**Analisa resiko kualitatif – tingkat resiko (OB/7, 1999)**

| Konsekuen | Peluang | | |
|---|---|---|---|
| | Rendah | Sedang | Tinggi |
| Tinggi | S | T | T |
| Sedang | R | S | T |
| Rendah | R | R | S |

Keterangan :

R : Resiko rendah

S : Resiko sedang

T : Resiko tinggi

### 3.6.2. Penyebab Resiko Dan Solusi:

**Penyebab Resiko :** Merupakan bentuk tindakan yang kurang dalam masalah keamanan sehingga bisa menimbulkan terjadinya resiko keamanan.

a. (*oversight*) : Klien sadar adanya resiko tapi tak ada tindakan *countermeasure-nya*.
b. U (*unawareness*) : Klien tak menyadari adanya resiko sehingga tidak ada tindakan untuk menangani resiko itu.
c. I (*inadequacy*) : Klien sadar adanya resiko dan melakukan tindakan dalam menangani resiko tetapi rencana *countermeasure*-nya tak memadai.
d. N (*not available*) : Klien sadar betul adanya resiko dan melakukan *countermeasure*-nya secara tepat.

**Tabel 4**
**Jumlah Penyebab Resiko Dan Solusinya**

| No | Penyebab Resiko | Jumlah | Solusi |
|---|---|---|---|
| 1 | O (oversight) | 2 | Lakukan Countermeasure |
| 2 | U (unawareness) | 3 | Lakukan pelatihan keamanan |
| 3 | I (Inadequacy) | 1 | Lakukan countermesure yang memedai |
| 4 | N (not available) | 1 | Tak ada |

## IV. KESIMPULAN DAN SARAN

### 4.1. Kesimpulan

Dari penelitian ini dapat disimpulkan bahwa:

a. Formula yang diajukan pada penelitian ini merupakan suatu metodologi untuk menganalisa serta mengkategorisasikan resiko keamanan pada jaringan sistem informasi ditinjau dari sisi proses dapat diterapkan pada kehidupan sehari-hari.
b. Metode analisa ini dapat membantu menganalisa keamanan jaringan sistem informasi dengan fokus pada penyebab dan solusi untuk jaringan sistem informasi yang kritis pada suatu organisasi.
c. Metode analisa ini dapat membantu para perancang jaringan sistem informasi untuk membangun jaringan sistem informasi yang aman.

### 4.2. Saran

Dari penelitian ini maka disarankan bahwa :

a. Penelitian ini ditujukan pada organisasi sistem informasi secara umum maka untuk mereka yang ingin menggunakan metode analisa ini dapat digunakan terhadap berbagai jenis sistem informasi yang bersifat khusus seperti data warehousing dengan melakukan pengadaptasian terhadap objek yang diteliti.
b. Karena penelitian ini dilakukan pada hanya satu studi kasus maka para peneliti yang ingin menggunakan metode ini sebaiknya di teliti pada multi studi kasus sehingga ada perkembangan pada dunia pengetahuan.

## V. DAFTAR PUSTAKA

Alan Sugano, 2004, The Real-World Network Troubleshooting Manual, Charles River Media, Inc.

Ankit Fadia, 2003, Network Security : A Hacker’s Perspective, Macmillan India Ltd.

AusCERT, 2000, Information Security Standard, URL :

http/www/anscert.org.au/Information/standards.html.

Beny Benardi, 2004 , Membangun Firewall dengan Cisco Router, PT Bex Media Komputindo.

Budi Rahardjo, 2005, Keamanan Sistem Informasi Berbasis Internet, Versi 5.4, PT Insan Infonesia-Bandung & PT INDICISC-Jakarta.

Carl Roper, Joseph Grau, and Lynn Fischer, 2006, Security Education, Awareness, and Ttraining, From Theory to Practice, Elsevier Inc.

Chris McNab, 2004, Network Security Assessment, O'Reilly.

David Kosiur, Uderstanding Electronic Commerce, Microsoft Press.

Depkominfo, 2007, Blue Print Aplikasi E-Government Pemerintah Pusat, Depkominfo.

Deris Setiawan, 2005, Sistem Keamanan Komputer, PT Elex Media Komputindo.

Didik Subyantara, 2004, Instalasi dan konfigurasi Jaringan Microsoft Windows, PT Elex Media Komputindo.

ID-CERT, 2016, Incident Monitoring Report 2016, ID-CERT

Parag Diwan, 2002, Information System Management, Golden Books Sdn, Bhd.

Patrick T. Campbell, 1996, Jaringan di Kantor Kecil, PT Elex Media Komputindo.

R. Eko Indrajit, 2005, Manajemen Sistem Informasi dan Teknologi Informasi, Ebook

Perbanas.

Ridwan Sanjaya ..dkk, 2005, Administrasi Jaringan Komputer Lintas Platform, PT Elex Media Komputindo.

Rinaldi Munir, 2006, Kriptografi, Informatika.

Robert Richardson, 2008, Computer crime & security survey, CSI.

Rolf Oppliger, 2002, Internet and Intranet Security, Artech House, Inc.

Ron Ben Natan, 2005, Implementing Database Security and Auditing, Elsevier

Digital Press.

Straub, D.W. and Welke, RJ, 1998,Coping with system risk: security planning models for management decision, MIS Quarterly, Minneapolis.

Stuart McClure, Saumil Shah, and Shreeraj Shah, 2003, Web Hacking Serangan dan Pertahanan, ANDI.

Thomas R. Peltier, 2005, Information Security Risk Analysis, Second Edition,

Wesley J. Noonan, 2004, Hardening Network Infrastructure, The McGraw-Hill Companies, Inc.

Yin, R.K, 1993, Application of case study reserch, Sage.

[Yin, R.K, 1994, Case study reserch-design and methods, Sage.

Zikmund, W.G, 1997, Businees reserch methods, The Dryden Press.