# ANALISIS MANAJEMEN RISIKO TERHADAP KEAMANAN JARINGAN DENGAN PENDEKATAN SNI ISO/IEC 27001 DI TVRI JAWA BARAT

Muhamad Rizki Fadillah[1], Angga Setiyadi[2]
[1,2] UNIKOM
Jalan Dipatiukur No. 112-116, Lebakgede, Coblong, Kota Bandung, Jawa Barat 40132
E-mail : rizkifadillah418@gmail.com[1], angga.setiyadi@email.unikom.ac.id[2]

## ABSTRAK

TVRI Jawa Barat merupakan salah satu stasiun pemyiaran daerah milik Televisi Republik Indonesia. Pada operasionalnya sehari-hari, tingkat kesadaran terhadap keamanan informasi di TVRI Jawa Barat masih kurang sehingga diperlukan analisis terhadap manajemen risiko untuk mengetahui dan mengidentifikasi risiko yang muncul dan akan terjadi di lingkungan TVRI Jawa Barat. Serta pengujian jaringan untuk mengetahui kerentanan yang ditimbulkan pada layanan dan perangkat jaringan itu sendiri, dampak dari kerentanan diukur sesuai dengan tingkat kritikalitas pada proses bisnis di TVRI Jawa Barat. Dengan menggunakan pendekatan SNI ISO/IEC 27001 untuk persyatan terhadap sistem manajemen keamanan informasi yang dianjurkan oleh Kementrian Komunikasi dan Informatika dalam peraturan menteri nomor 4 tahun 2016.

**Kata kunci :** Manajemen Risiko, Keamanan Jaringan, PPDIOO, SNI ISO/IEC 27001, TVRI Jawa Barat.

## 1. PENDAHULUAN

TVRI Jawa Barat adalah stasiun televisi daerah yang didirikan oleh Televisi Republik Indonesia untuk wilayah Provinsi Jawa Barat. Setiap intansi membutuhkan pengelolaan yang baik terhadap data dan keamanan data/informasi, sehingga tingkat keamanan data dan informasi dapat terjamin, Karena jika mengacu kepada peraturan menteri komunikasi dan informatika nomor 4 tahun 2016 bahwa instansi harus menerapkan standar SNI ISO/IEC 27001. Berdasarkan hasil wawancara dengan Bapak Adit, selaku koordinator IT, bahwa karyawan TVRI Jawa Barat belum menyadari akan keamanan informasi sehingga kejadian-kejadian seperti kerusakan pada jaringan yang mengganggu proses bisnis bisa saja terjadi. Penanganan risiko yang terjadi dan yang akan terjadi di TVRI Jawa Barat belum terdokumentasikan. Sehingga jika terjadi insiden kehilangan, kerusakan baik dari aset fisik maupun digital belum memenuhi standar yang diberlakukan oleh Kementrian Komunikasi dan Informatika. Belum pernah dilakukannya pengujian terhadap keamanan jaringan di TVRI Jawa Barat yang dapat mengakibatkan proses bisnis jika jaringan yang ada di TVRI Jawa Barat mengalami gangguan.

Untuk mengatasi masalah yang saat ini terjadi di TVRI Jawa Barat, akan dilakukan analisis terhadap risiko-risiko yang sudah terjadi dan akan terjadi sehigga risiko yang ada di TVRI Jawa Barat dapat teridentifikasi dan terdokumentasi, serta membuat penilaian risiko yang ada di TVRI Jawa Barat untuk mengetahui tingkat kerusakan yang ditimbulkan dari risiko-risiko yang ada, dan melakukan pengujian jaringan komputer untuk mengetahui kerentanan dan tingkat kerusakan yang terdapat pada jaringan komputer di TVRI Jawa Barat.

Diharapkan dengan diimplementasikannya parameter-parameter SNI ISO/IEC 27001 dapat menjadi solusi dari permasalahan yang terjadi dimana SNI ISO/IEC 27001 menjadi persyaratan dalam penerapan Sistem Manajemen Keamanan Informasi untuk menjamin keamanan, integritas dan ketersediaan data yang dikelola oleh TVRI Jawa Barat.

## 2. ISI PENELITIAN

### 2.1 Teori Pendukung

1) Keamanan Jaringan Komputer

Keamanan jaringan adalah perlindungan jaringan perusahaan dan layanan dari pengubahan, penghancuran, atau pengungkapan data/informasi yang tidak sah yang bertujuan untuk memberikan jaminan bahwa jaringan tersebut melakukan fungsi-fungsi terkait keamanan yang penting. Dalam keamanan jaringan, organisasi/perusahaan harus mengamankan semua aspek sumber daya jaringannya. Setelah sumber daya terhubung ke jaringan, semua atribut keamanan berbasis host harus ditinjau untuk memahami bagaimana mereka dipengaruhi oleh lingkungan jaringan. Server di jaringan dapat berisi data dan informasi yang sensitif tentang cara mengakses sumber daya internal [2].

2) Keamanan Informasi

Keamanan informasi adalah perlindungan terhadap informasi dari berbagai ancaman untuk menjamin keberlangsungan proses bisnis, mengurangi tingkat risiko bisnis, dan meningkatkan peluang terhadap bisnis itu sendiri. Dalam merancang sistem keamanan sistem informasi terdapat aspek-aspek keamanan informasi yang harus di perhatikan. Aspek yang harus diperhatikan yaitu :

1. Kerahasiaan

Aspek yang menjamin kerahasiaan dari data dan informasi yang hanya bisa diakses oleh pihak yang mempunyai otoritas terhadap informasi tersebut..

2. Integritas

Aspek yang menjamin data dan informasi tidak bisa diubah tanpa sepengetahuan pihak yang berwenang, menjamin kelengkapan informasi, dan menjamin data tidak rusak yang bisa menyebabkan perubahan pada data asli.

3. Ketersediaan

Aspek yang Menjamin ketersediaan data jika data dibutuhkan dan menjamin user dapat mengakses informasi tanpa adanya gangguan [2].

3) SNI ISO/IEC 27001

SNI ISO/IEC 27001 merupakan standar untuk menetapkan persyaratan penetapan, penerapan, pemantauan, pengoperasian, peningkatan, pengkajian, dan pemeliharaan Sistem Manajemen Keamanan Informasi (SMKI) yang didokmentasikan dalam sudut pandang risiko bisnis organisasi secara keseluruhan. SMKI didesain untuk memastikan pemilihan pengendalian keamanan yang memadai dan proposional untuk melindungi aset informasi dan memberikan kepercayaan kepada pihak terkait [4].

4) Risiko

Risiko adalah bahaya atau konsekuensi yang terjadi akibat proses yang sedang berlangsung atau kejadian yang akan datang. Risiko selalu menghadang setiap individu maupun berbagai institusi, termasuk organisasi bisnis. dalam manajemen resiko, terdapat beberapa tingkatan yaitu resiko besar dan resiko kecil [2].

5) Manajemen Risiko

Manajemen risiko merupakan proses mengidentifikasi tingkat kerentanan dan ancaman terhadap informasi yang digunakan oleh organisasi untuk mencapai tujuan bisnis, dan memutuskan tindakan penanggulangan untuk meminimalisir risiko ke tingkat yang dapat diterima, berdasarkan nilai sumber informasi untuk organisasi/perusahaan [2].

6) Penanganan Risiko

Penanganan risiko perlu direncanakan dan dipertimbangkan semua alternatif solusinya, sebelum dilakukan mitigasinya, agar hasil yang diharapkan efektif dan efisien. Beberapa alternatif bisa dipertimbangkan untuk digunakan Tabel likelihood untuk menentukan penanganan dalam risiko dapat dilihat pada tabel 2.1 [2].

Tabel 1 *Likelihood*

| Faktor Probabilitas | Dampak Konsekuensi | | | | |
|---|---|---|---|---|---|
| | Sangat Rendah | Rendah | Sedang | Tinggi | Kritikal |
| Sangat Jarang | Rendah | Rendah | Sedang | Tinggi | Tinggi |
| Jarang | Rendah | Rendah | Sedang | Tinggi | Ekstrim |
| Kadang-Kadang | Rendah | Sedang | Tinggi | Ekstrim | Ekstrim |
| Sering | Sedang | Tinggi | Tinggi | Ekstrim | Ekstrim |
| Sangat Sering | Tinggi | Tinggi | Ekstrim | Ekstrim | Ekstrim |

7) Aset

Informasi adalah salah suatu aset bagi sebuah perusahaan atau organisasi, aset lainnya memiliki nilai tertentu bagi setiap perusahaan atau organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan pada perusahaan atau organisasi, mengurangi kerusakan yang disebabkan oleh kebocoran sistem keamanan informasi, meningkatkan kembalinya investasi dan memperluas peluang usaha [2].

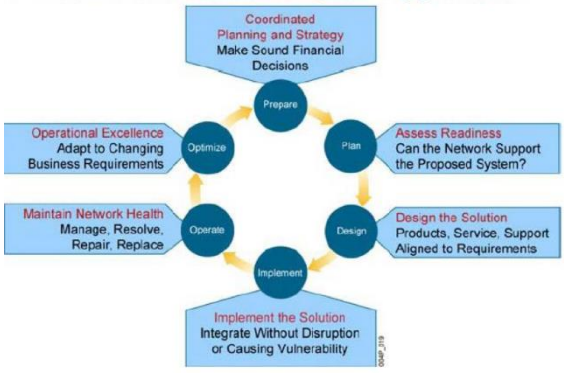
8) Jaringan Komputer

Jaringan komputer adalah sekelompok komputer yang saling dihubungkan menggunakan protokol komunikasi melalui media komunikasi. Dengan adanya jaringan komputer maka antar komputer, dapat saling bertukar data dan informasi, aplikasi-aplikasi, Sistem Informasi dan program-program lainnya [1].

**2.2 Analisis Manajemen Risiko**

1) Metodologi Analisis Manajemen Risiko

Metode penelitian yang digunakan dalam penelitian ini adalah metode PPDIOO (*Prepare, Plan, Design, Implement, Operate, and Optimize*). Metode pengembangan jaringan PPDIOO ini diciptakan oleh Cisco Systems Inc. untuk mendukung proses bisnis yang dilakukan. Metode ini memiliki fase-fase yang berkelanjutan, dan setiap fasenya memiliki langkah untuk mensukseskan perencanaan, desain, implementasi, dan operasi sebuah sistem jaringan komputer [9].




Gambar 1 Metode PPDIOO

a) *Prepare*

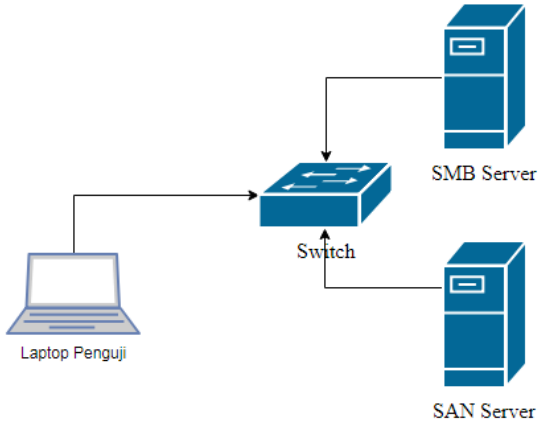
Penelitian dalam tugas akhir ini adalah menganalisa risiko-risiko yang terjadi dan akan terjadi di TVRI Jawa Barat. Terdapat berbagai masalah yang terjadi dalam penanganan risiko-risiko yang terjadi di TVRI Jawa Barat, diantaranya adalah karyawan TVRI Jawa Barat belum memperdulikan terkait keamanan informasi, pihak TVRI Jawa Barat belum mempunyai dokumentasi terkait penanganan risiko yang ada, dan pihak TVRI Jawa Barat belum pernah melakukan pengujian jaringan komputer.

b) *Plan*

Solusi yang akan ditawarkan untuk menghadapi permasalahan yang terjadi adalah untuk mempermudah TVRI Jawa Barat dalam meningkatkan kepedulian terhadap keamanan informasi, mempermudah TVRI Jawa Barat dalam membuat dokumentasi terkait risiko yang terjadi dan yang akan terjadi dan mempermudah TVRI Jawa Barat dalam mengetahui kerentanan jaringan komputer.

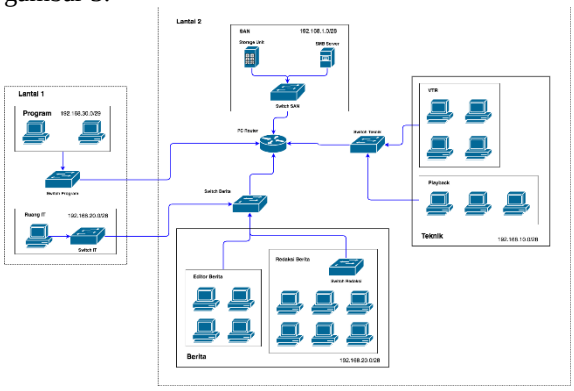
c) *Design*

Skenario pengujian keamanan jaringan di TVRI Jawa Barat adalah dengan mengidentifikasi keberadaan dan kemungkinan eksploitasi celah keamanan pada jaringan, yang mencakup perangkat server di TVRI Jawa Barat . skenario pengujian dapat dilihat pada gambar 2.




Gambar 2 Skenario Pengujian Jaringan

Untuk topologi jaringan komputer di TVRI Jawa Barat terdiri dari 2 jaringan utama; 1 jaringan SAN, dan 1 jaringan utama menghubungkan semua bagian kerja. Jaringan SAN terdiri dari storage unit, dan server-server penyedia layanan. Jaringan SAN ini kemudian terhubung ke jaringan utama melalui PC Router. Jaringan utama adalah gabungan dari beberapa jaringan kecil di tiap-tiap bagian, yang dihubungkan ke PC Router. Topologi jaringan komputer di TVRI Jawa Barat dapat dilihat pada gambar 3.



Gambar 3 Topologi jaringan komputer

d) *Implement*

Tahapan ini dilakukan analisis dan pengujian jaringan komputer untuk mengetahui kerentanan dan dampak yang mempengaruhi proses bisnis TVRI Jawa Barat, pengujian jarigan komputer dilakukan pada server SMB dan server Storage dimana kedua server tersebut adalah server utama yang menunjang proses bisnis di TVRI Jawa Barat.

Yang dilakukan pada implementasi ini meliputi analisis kendali jaringan di TVRI Jawa Barat, analisis keamanan layanan jaringan, dan analisis pemisahan dalam jaringan.

**2.2 Hasil Pengujian**

Setelah tahap perancangan dan implementasi dilakukan, tahap selanjutnya dilakukan pengujian terhadap kendali jaringan, pengujian terhadap keamanan layanan jaringan dan pengujian terhadap pemisahan dalam jaringan, serta membuat rekomendasi terkait pengujian kendali jaringan, pengujian keamanan layanan jaringan dan pengujian pemisahan dalam jaringan.

1) Pengujian kendali jaringan

Pengujian kendali jaringan untuk menguji kepatuhan TVRI Jawa Barat dalam mengelola kendali jaringan terhadap persyaratan yang terdapat pada SNI ISO/IEC 27001. Pengujian kendali jaringan dapat dilihat pada tabel 2

Tabel 2 Hasil Pengujian Kendali Jaringan

| No | Keterangan | Diterap-kan | Didoku mentasi kan | Belum Diaplika -sikan |
|---|---|---|---|---|
| 1 | Apakah jaringan sudah dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi? | v | | |
| 2 | Apakah mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari layanan jaringan sudah diidentifikasi dan dimasukan dalam perjanjian layanan jaringan? | | v | |

| | | | | |
|---|---|---|---|---|
| 3 | Apakah layanan informasi, pengguna dan sistem informasi sudah dipisahkan pada jaringan? | v | | |
| 4 | Apakah ada kebijakan, prosedur dan kendali perpindahan yang resmi untuk melindungi perpindahan informasi melalui penggunaan semua jenis faslitas komunikasi. | v | | |

Berdasarkan tabel 2 dapat disimpulkan bahwa TVRI Jawa Barat sudah melakukan kendali jaringan yang sesuai dengan SNI ISO/IEC 27001, namun belum didokumentasikan sehingga pihak TVRI Jawa Barat harus membuat dokumentasi terhadap kendali jaringan yang ada.

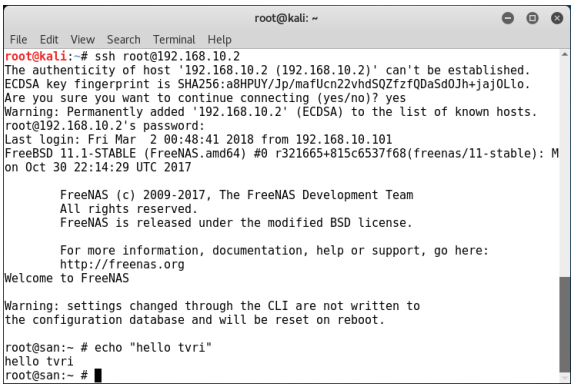
2) Analisis dan Rekomendasi Kendali Jaringan

Hasil pengujian kendali jaringan, pihak TVRI Jawa Barat sudah beberapa aspek terkait kendali jaringan. Rekomendasi dari pengujian kendali jaringan adalah membuat dokumentasi dan menerapkan aspek kendali jaringan.

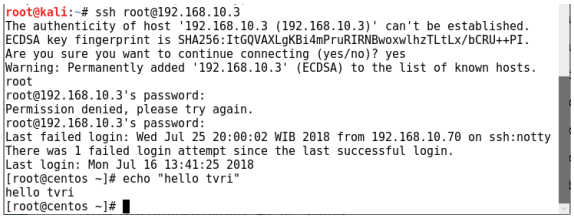
3) Pengujian Keamanan Layanan Jaringan

Pengujian keamanan layanan jaringan dilakukan pada jaringan komputer di TVRI Jawa Barat untuk mengidentifikasi keberadaan dan kemungkinan melakukan eksploit terhadap celah keamanan pada jaringan, yang mencakup perangkat server di TVRI Jawa Barat. Proses pengujian keamanan jaringan komputer penguji mendapatkan beberapa celah keamanan dan mencoba melakukat eksploitasi pada celah keamanan tersebut. Terdapat beberapa temuan pada celah keamanan jaringan pada server SAN dan SMB di TVRI Jawa Barat, sebagai berikut:

a) Weak password, kerentanan ini terdapat pada kedua server dengan IP Address 192.168.10.2 dan 192.168.10.3. Adanya penggunaan weak password ini memungkinkan penguji dapat login ke server. Hasil verifikasi pengujian dapat dilihat pada gambar 4 dan 5.

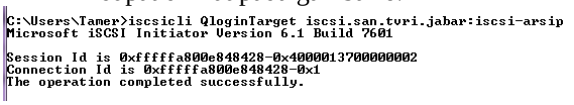



Gambar 4 Hasil Pengujian Weak Password pada ip 192.168.10.2




Gambar 5 Hasil Pengujian Weak Password pada ip 192.168.10.2

b) *iSCSI Unauthinticated Target Detection*, kerentanan ini terdapat pada SAN server dengan ip 192.168.10.2. kondigurasi iSCSI yang belum menggunakan mekanisme autentikasi memungkinkan penguji dapat mengakses iSCSI tanpa adanya autentikasi terlebih dahulu. Hasil verifikasi pengujian dapat dilihat pada gambar 6.




Gambar 6 Hasil Pengujian *iSCSI Unauthinticated Target Detection*

4) Analisis dan Rekomendasi Keamanan Layanan Jaringan

Dari uraian hasil pengujian pada bagian Pengujian keamanan layanan jaringan, berikut ini adalah tabel analisis dan rekomendasi terhadap pengujian keamanan layanan jaringan di TVRI Jawa Barat. Analisis dan rekomendasi dapat dilihat pada tabel 3.

| IP | Kerentanan | Kategori | Dampak | Rekomendasi |
|---|---|---|---|---|
| 192.168.10.2 | *Weak Password* | *Security Misconfiguration* | Terdapat penggunaan weak password pada server sehingga sistem dapat diambil alih (root | Ganti password SSH sesuai dengan ketentuan kebijakan password di TVRI Jawa Barat |

| | | | | |
|---|---|---|---|---|
| | | | compromised) | |
| 192.168.10.3 | *Weak Password* | *Security Misconfiguration* | Terdapat penggunaan weak password pada server sehingga sistem dapat diambil alih (root compromised) | Ganti password SSH sesuai dengan ketentuan kebijakan password di TVRI Jawa Barat |
| | *iSCSI Unauthinticated Target Detection* | *Security Misconfiguration* | Terdapat penggunaan konfigurasi bawaan yang belum menggunakan mekanisme autentikasi sehingga penguji dapat mengakses iSCSI tanpa adanya autentikasi terlebih dahulu | Tambahkan mekanisme autentikasi pada konfigurasi iSCSI |

5) pengujian pemisahan dalam jaringan

Pengujian pemisahan dalam jaringan untuk menguji kepatuhan TVRI Jawa Barat dalam mengelola pemisahan dalam terhadap persyaratan yang terdapat pada SNI ISO/IEC 27001. Pengujian pemisahan dalam jaringan dapat dilihat pada tabel 4.

| | SAN | Teknik | Berita | Program |
|---|---|---|---|---|
| Subnet Mask | 255.255.255.240 | 255.255.255.240 | 255.255.255.240 | 255.255.255.240 |
| Jumlah host | $2^4$-2=14 | $2^4$-2=14 | $2^4$-2=14 | $2^3$-2=6 |
| Alamat jaringan | 192.168.1.0/28 | 192.168.10.0/28 | 192.168.20.0/28 | 192.168.30.0/29 |
| Alamat host pertama | 192.168.1.1 | 192.168.10.1 | 192.168.20.1 | 192.168.30.1 |
| Alamat host terakhir | 192.168.1.15 | 192.168.10.15 | 192.168.20.15 | 192.168.30.7 |
| Alamat *broadcast* | 192.168.1.16 | 192.168.10.16 | 192.168.20.16 | 192.168.30.8 |

6) Analisis dan rekomendasi

Hasil pengujian pemisahan dalam jaringan, pihak TVRI Jawa Barat sudah menerapkan seluruh aspek pemisahan dalam jaringan. Rekomendasi dari pengujian pemisahan dalam jaringan adalah membuat dokumentasi terkait pemisahan dalam jaringan.

## 3. PENUTUP

1) Kesimpulan

Berdasarkan uraian pada bab-bab sebelumnya, dapat ditarik beberapa kesimpulan dari penelitian ini, diantaranya adalah:

1. Penelitian ini terbukti dapat memudahkan bidang IT dalam melakukan identifikasi, analisis, dan dokumentasi risiko terhadap jaringan komputer di TVRI Jawa Barat..
2. Penelitian ini dapat membantu tugas bidang IT dalam mengamankan jaringan komputer di TVRI Jawa Barat.
3. Penelitian ini dapat memberikan arahan untuk persiapan penerapan Sistem Manajemen Keamanan Informasi yang didasari oleh peraturan menteri komunikasi dan informatika nomor 4 tahun 2016 bahwa instansi harus menerapkan standar SNI ISO/IEC 27001.

2) Saran

Penelitian ini masih memiliki segala keterbatasan dan kekurangan baik dari segi kesiapan, dan kelengkapan yang ada. Maka dari itu diperlukan

saran-saran untuk memperbaiki keterbatasan dan kekurangan tersebut, diantaranya:

1. Diperlukan kesiapan dari semua elemen kepegawaian TVRI Jawa Barat untuk menerapkan semua parameter SNI ISO/IEC 27001.
2. Diperlukan sosialisasi keamanan informasi untuk semua pegawai TVRI Jawa Barat.
3. Diperlukan pengujian/audit secara berkala untuk menjaga keamanan semua aspek demi kelancaran proses bisnis di TVRI Jawa Barat.

## DAFTAR PUSTAKA


[1] B. A. Forouzan and S. C. Fegan, Data Communications and Networking, 4th ed., McGraw-Hill, 2007.
[2] B. G. Ragard, Information Security Management: Concepts and Practice, CRC PRESS, 2010.
[3] *CISA Review Manual*, 2006.
[4] SNI ISO/IEC 27001, BSN, 2013.
[5] https://nmap.org/, diakses pada tanggal 7 Juni 2018
[6] https://tenable.com/, diakses pada tanggal 5 juni 2018
[7] S. Wilkins, "PPDIOO Stages > Cisco's PPDIOO Network Cycle," 2011. [Online]. [Accessed 27 Oktober 2017].