

**DESAIN SISTEM KEAMANAN INFORMASI BERDASARKAN
PERATURAN BSSN NOMOR 4 TAHUN 2021 DAN INDEKS
KEAMANAN INFORMASI (KAMI)**

Skripsi



**UIN SUNAN AMPEL
S U R A B A Y A**

**Disusun Oleh :
AHMAD FANY RIZQIYANTO
NIM : H96218050**

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL
SURABAYA
2023**

LEMBAR PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama : AHMAD FANY RIZQIYANTO

NIM : H96218050

Program Studi : Sistem Informasi

Angkatan : 2018

Menyatakan dengan sesungguhnya bahwa skripsi berjudul: "DESAIN SISTEM KEAMANAN INFORMASI BERDASARKAN PERATURAN BSSN NOMOR 4 TAHUN 2021 DAN INDEKS KEAMANAN INFORMASI (KAMI)" benar-benar hasil karya saya sendiri. Hal-hal yang bukan karya saya dalam penulisan ini ditunjukkan dalam daftar pustaka. Apabila suatu saat nanti saya terbukti melakukan Tindakan plagiasi, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan ini dibuat dengan sesungguhnya.

Surabaya, 26 Juni 2023

Yang membuat pernyataan,



(Ahmad Fany Rizqiyanto)

NIM. H96218050

LEMBAR PERSETUJUAN PEMBIMBING

JUDUL : DESAIN SISTEM KEAMANAN INFORMASI
BERDASARKAN PERATURAN BSSN NOMOR 4 TAHUN
2021 DAN INDEKS KEAMANAN INFORMASI (KAMI).
NAMA : AHMAD FANY RIZQIYANTO
NIM : H96218050


Mahasiswa telah melakukan proses bimbingan dan dinyatakan layak untuk mengikuti
Sidang Skripsi

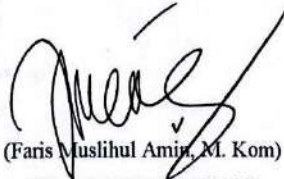
Surabaya, 12 Juli 2023

Menyetujui,

Dosen Pembimbing I

Dosen Pembimbing II


(Indri Sudanawati Rozas, M. Kom)
NIP. 198207212014032001


(Faris Muslihul Amin, M. Kom)
NIP. 198808132014031001

PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi Ahmad Fany Rizqiyanto ini telah dipertahankan di depan tim penguji skripsi di Surabaya, 12 Juli 2023

Mengesahkan,
Dewan Penguji,

Dosen Penguji I



Moch Yasin, M.Kom, M.B.A, MTCNA

NIP. 198808302014031001

Dosen Penguji II



Andhy Permadi, M. Kom

NIP. 198110142014031002

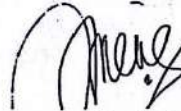
Dosen Penguji III



Indri Sudanawati Rozas, M. Kom

NIP. 198207212014032001

Dosen Penguji IV



Faris Muslihul Amin, M. Kom

NIP. 198808132014031001

Mengetahui,

Dekan Fakultas Sains dan Teknologi
Universitas Jember



Hamdani, M.Pd

NIP. 196507312000031002



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN

Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama : Ahmad Fany Rizqiyanto
NIM : H96218050
Fakultas/Jurusan : Sistem Informasi
E-mail address : fanirizqiyanto@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :

Sekripsi Tesis Desertasi Lain-lain (.....)

yang berjudul :

DESAIN SISTEM KEAMANAN INFORMASI BERDASARKAN PERATURAN

BSSN NOMOR 4 TAHUN 2021 DAN INDEKS KEAMANAN INFORMASI (KAMI)

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Eksklusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara *fulltext* untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 17 Agustus 2023

Penulis

(Ahmad Fany Rizqiyanto)

ABSTRAK

DESAIN SISTEM KEAMANAN INFORMASI BERDASARKAN PERATURAN BADAN NASIONAL SIBER DAN SANDI NEGARA NOMOR 4 TAHUN 2021 DAN INDEKS KEAMANAN INFORMASI (KAMI)

Oleh:

Ahmad Fany Rizqiyanto

Teknologi informasi (TI) berkembang pesat setiap hari, dan perkembangan ini berdampak pada setiap organisasi dan perusahaan di setiap sektor. Khususnya pada ranah Pengamanan Keamanan Informasi, merupakan upaya untuk melindungi aset informasinya dengan maksud untuk melindungi infrastruktur teknologi informasi dari gangguan internal maupun eksternal pada suatu jaringan. Lokasi objek penelitian ini berada di TVRI Jawa Timur. Untuk pengumpulan data yakni dengan cara wawancara dengan narasumber staff IT TVRI Jawa Timur. Dengan menggunakan pedoman BSSN No. 4 Tahun dan Indeks Keamanan Informasi (KAMI). Untuk output penelitian ini yakni berupa hasil rekomendasi yakni berupa Standard Operating Procedure (SOP) yang dilengkapi dengan alur prosedur yang berjumlah 3 SOP. Yakni Autentikasi, Manajemen Sesi, dan Kontrol Akses. Sebaiknya dokumen rekomendasi SOP yang telah dibuat untuk diuji, diimplementasikan, dan diaudit secara internal guna untuk mengetahui sejauh mana dampak terhadap keamanan informasi pada TVRI Jawa Timur. Selain itu, penelitian ini hanya sebatas pembuatan dokumen rekomendasi keamanan berupa SOP, untuk penelitian selanjutnya mungkin dapat dilakukan evaluasi keefektifan dokumen SOP yang telah dibuat terhadap keamanan informasi TVRI Jawa Timur.

Kata Kunci: Manajemen Keamanan, Keamanan Informasi, BSSN No. 4 Tahun 2021, Indeks KAMI, TVRI Jawa Timur

ABSTRACT

INFORMATION SECURITY SYSTEM DESIGN BASED ON REGULATION OF THE NATIONAL CYBER AND CRYPTO NATIONAL AGENCY NUMBER 4 OF 2021 AND INFORMATION SECURITY INDEX (KAMI)

By:

Ahmad Fany Rizqiyanto

Information technology (IT) is advancing rapidly every day, and these developments impact every organization and company in every sector. Particularly in the realm of Information Security Security, it is an effort to protect its information assets with the aim of protecting information technology infrastructure from internal and external disturbances on a network. The location of this research object is in TVRI East Java. For data collection, namely by way of interviews with informants, IT staff of TVRI East Java. By using BSSN No. guidelines. 4 Years and the Information Security Index (US). The output of this research is in the form of recommendations, namely in the form of a Standard Operating Procedure (SOP) equipped with a flow of procedures totaling 3 SOPs. Namely Authentication, Session Management, and Access Control. We recommend that the SOP recommendation document that has been made is tested, implemented and audited internally in order to determine the extent of the impact on information security on TVRI East Java. In addition, this research is only limited to making security recommendation documents in the form of SOPs. For further research, it may be possible to evaluate the effectiveness of the SOP documents that have been made on TVRI East Java's information security.

Keywords: *Security Management, Information Security, BSSN No. 4 of 2021, KAMI Index, TVRI Jawa Timur*

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	1
LEMBAR PERNYATAAN KEASLIAN	Error! Bookmark not defined.
PENGESAHAN TIM PENGUJI SKRIPSI.....	iv
KATA PENGANTAR	Error! Bookmark not defined.
ABSTRAK	1
ABSTRACT	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN.....	Error! Bookmark not defined.
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian	3
1.5. Manfaat Penelitian	4
1.5.1 Bagi Penulis	4
1.5.2 Bagi Universitas	4
1.5.3 Bagi TVRI.....	4
1.6. Sistematika Penulisan Skripsi	4
BAB II TINJAUAN PUSTAKA.....	6
2.1. Tinjauan Penelitian Terdahulu	6
2.2. Profil TVRI Jawa Timur	12
2.2.1 Visi TVRI Jawa Timur.....	12
2.2.2 Misi TVRI Jawa Timur	13
2.2.3 Struktur Organisasi TVRI Jawa Timur	14
2.3.1 Keamanan Informasi	15
2.3.2 Sistem Pemerintahan Berbasis Elektronik (SPBE).....	16
2.3.3 Pedoman BSSN No. 4 Tahun 2021	18
2.3.4 Indeks KAMI	22
2.3.5 Domain Teknologi dan Keamanan Informasi	24

2.3.6 RACI	25
2.3.7 ISO 27001	25
2.3.8 Hubungan ISO 27001 dengan BSSN 2021	26
2.3 Integrasi Keilmuan	27
BAB III METODOLOGI	30
3.1 Metodologi Penelitian	30
3.2 Tahapan Penelitian	31
3.2.1 Penetapan Ruang Lingkup	31
3.2.2 Penetapan Penanggung Jawab	31
3.2.3 Perencanaan	32
3.2.4 Dukungan Pengoperasian	32
3.2.5 Evaluasi Kinerja	32
3.2.6 Perbaikan Berkelanjutan	32
3.3 Lokasi Penelitian	33
3.4 Waktu Penelitian	33
BAB IV HASIL DAN PEMBAHASAN	34
4.1 Proses Mapping Dokumen	34
4.1.1 Gambaran Umum Objek	34
4.1.2 Penetapan Ruang Lingkup	36
4.1.3 Penetapan Penanggung Jawab	37
4.1.4 Perencanaan	38
4.2 Desain Dokumen Rekomendasi	41
4.2.1 Dukungan Pengoperasian	41
4.2.2 Evaluasi Kinerja	41
4.2.3 Perbaikan Berkelanjutan	48
BAB V PENUTUP	58
5.1 Kesimpulan	58
5.2 Saran	58
DAFTAR PUSTAKA	60

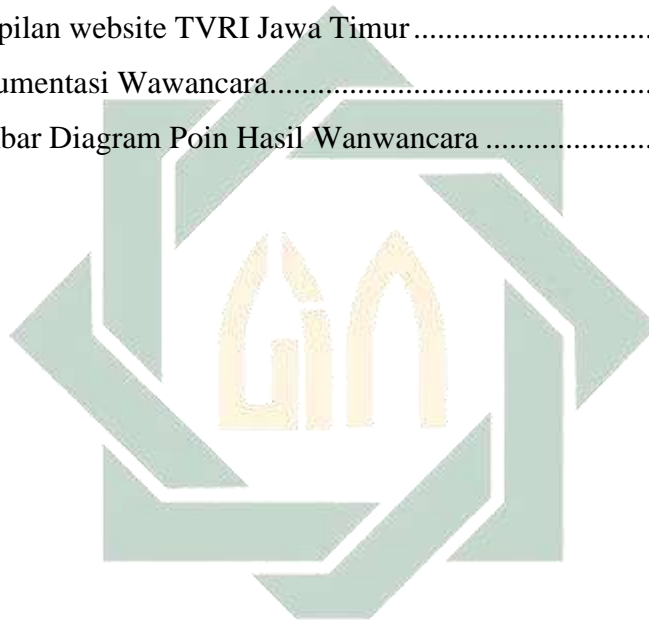
DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	6
Tabel 3. 1 Timeline Penelitian	33
Tabel 4. 1 Indikator Mapping Indeks KAMI dan BSSN 2021	38
Tabel 4. 2 Mapping control bagian 1	39
Tabel 4. 3 Mapping control bagian 2	40
Tabel 4. 4 Mapping Kontrol bagian 3	40
Tabel 4. 5 Hasil Survey Wawancara Indeks KAMI.....	42
Tabel 4. 6 Rincian Hasil Wawancara Indeks KAMI.....	47
Tabel 4. 7 List Hasil Rekomendasi Dokumen Keamanan	48
Tabel 4. 8 Pemetaan Kontrol BSSN No. 4 Dengan SOP	52
Tabel 4. 9 <i>Bagian SOP Autentikasi</i>	52
Tabel 4. 10 Struktur Konten Bagian Autentikasi	53
Tabel 4. 11 Bagian <i>SOP Manajemen Sesi</i>	54
Tabel 4. 12 Struktur isi bagian SOP Manajemen Sesi	54
Tabel 4. 13 Bagian <i>SOP Kontrol Akses</i>	56
Tabel 4. 14 Stuktur isi bagian SOP Kontrol Akses.....	56

UIN SUNAN AMPEL
S U R A B A Y A

DAFTAR GAMBAR

Gambar 2. 1 Struktur Organisasi TVRI Jawa Timur	14
Gambar 2. 2 Indeks KAMI versi 4.2 - Mei 2021	23
Gambar 2. 3 Domain Teknologi dan Keamanan Informasi bagian 1	24
Gambar 2. 4 Domain Teknologi dan Keamanan Informasi bagian 2	25
Gambar 3. 1 Alur Penelitian.....	30
Gambar 4. 1 Logo TVRI Jawa Timur	35
Gambar 4. 2 Tampilan website TVRI Jawa Timur.....	35
Gambar 4. 3 Dokumentasi Wawancara.....	36
Gambar 4. 4 Gambar Diagram Poin Hasil Wanwancara	47



UIN SUNAN AMPEL
S U R A B A Y A

BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi (TI) berkembang pesat setiap hari, dan perkembangan ini berdampak pada setiap organisasi dan perusahaan di setiap sektor. Khususnya pada ranah Pengamanan Keamanan Informasi, merupakan upaya untuk melindungi aset informasinya dengan maksud untuk melindungi infrastruktur teknologi informasi dari gangguan *internal* maupun *eksternal* pada suatu jaringan. Menjaga keamanan informasi berarti memperhatikan faktor keamanan semua perangkat pendukung, jaringan dan fasilitas lainnya yang secara langsung maupun tidak langsung berhubungan dengan proses pengolahan informasi. Pengolahan informasi yang baik tidak hanya meningkatkan kualitas pengambilan keputusan, tetapi juga kualitas keuntungan dan daya saing pada suatu organisasi ataupun instansi.

Pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) pada 19 Mei 2017. Keputusan Presiden menetapkan bahwa BSSN adalah lembaga pemerintah nonkementerian yang melapor dan bertanggung jawab kepada Presiden melalui Menteri yang membidangi koordinasi politik, hukum, dan keamanan. “Untuk menghindari ketergantungan pada produk asing di masa depan.” (Kominfo.go.id, 2017). Pengelolaan keamanan informasi SPBE dilaksanakan oleh masing-masing otoritas pusat dan pemerintah daerah berdasarkan Pedoman Pengelolaan Keamanan Informasi SPBE (PERATURAN PERUNDANG-UNDANGAN KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA, 2021). Tujuan dari keamanan informasi adalah untuk menjamin kerahasiaan, integritas dan ketersediaan data dan informasi (Sheikhpour & Modiri, 2012).

Instansi yang telah mengimplementasikan TI adalah TVRI Jawa Timur, salah satu jaringan televisi publik berskala nasional di Indonesia. Dimana TVRI Jawa Timur dipimpin oleh seorang Direktur Utama, dalam menjalankan tugasnya membawahi beberapa divisi direktorat. Dimana semua divisi tersebut dalam pengawasan oleh seorang Dewan Pengawas. Dalam memenuhi visi dari TVRI Jawa Timur, yaitu “Menjadi lembaga penyiaran utama yang memotivasi dan

memberdayakan melalui program informasi, pendidikan dan hiburan yang memperkuat persatuan dan keragaman untuk meningkatkan martabat bangsa”, maka TVRI Jawa Timur telah menggunakan berbagai macam teknologi informasi salah satunya layanan didalam sebuah website yang dapat diakses melalui web pada www.tvri.go.id, dimana dengan adanya layanan ini dapat menggunakan layanan pengaduan kualitas dan isi siaran program berita, kegiatan kebudayaan dan lain sebagainya. Dalam website tersebut juga berisikan tinjauan jadwal penayangan acara.

Berdasarkan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, semua penyelenggara sistem elektronik wajib menggunakan informasi untuk kepentingan umum, pelayanan publik, dan demi kelancaran fungsi sistem elektronik, sistem harus dikumpulkan. Oleh karena itu, sangat diperlukan Desain Sistem Keamanan Informasi, untuk meningkatkan keterampilan dan layanan manajemen TVRI kepada publik, dibutuhkan keamanan informasi untuk mengelola semua informasi dan menjaganya tetap aman dan rahasia. Mengacu pada anjuran Pemerintah dalam ranah Keamanan Informasi, yakni menggunakan BSSN 2021. Hasil dari Dokumen Keamanan Informasi diharapkan dapat membantu meningkatkan keamanan informasi pada TVRI Jawa Timur serta membantu dalam memperbaiki keamanan informasi pada instansi.

Penelitian terdahulu oleh (Damar Apri Sudarmadi, 2019) berjudul ”Strategi BSSN Dalam Menghadapi Ancaman Siber di Indonesia”, dengan hasil Penyelenggaraan Keamanan Siber di Indonesia. Berdasarkan 5 (Lima) Pilar GCI Penyelenggaraan keamanan siber di Indonesia pada aspek hukum yaitu Indonesia sudah mempunyai peraturan dengan substansi yang berkaitan dengan kejahatan siber dan keamanan siber, meskipun bentuk peraturan tidak berdiri sendiri dan secara khusus serta mendalam mengatur tentang kejahatan siber dan keamanan siber. BSSN diharapkan untuk dapat mendorong penyusunan UU keamanan siber, sehingga kebijakan tersebut dapat menjadi acuan bagi BSSN serta seluruh pemangku kepentingan. Indonesia sudah menyelenggarakan pelatihan bagi anggota Polris secara rutin dan berkala, tetapi belum menyeluruh kepada seluruh aktor

hukum di Indonesia. Penelitian terdahulu oleh (Faturachman Husin Muh, 2017) dengan objek Tingkat kematangan keamanan informasi di Universitas Sam Ratulangi, yang masih tergolong rendah dan butuh perbaikan walaupun peran/tingkat ketergantungan akan TIK tergolong Tinggi. Pada aspek Teknologi dan Tata Kelola jauh lebih baik dibanding area keamanan lainnya. Hal sebaliknya terjadi pada Area Pengelolaan Aset dan Pengelolaan Risiko yang skornya masih rendah.

Berdasarkan kondisi dari TVRI dan permasalahan yang telah dijabarkan, maka penelitian skripsi ini berjudul **“Desain Sistem Keamanan Informasi berdasarkan Peraturan BSSN No. 4 Tahun 2021 dan Indeks Keamanan Informasi (KAMI)”**.

1.2. Rumusan Masalah

1. Bagaimana Mapping kontrol antara manajemen keamanan informasi BSSN No. 4 Tahun 2021 dengan Indeks KAMI?
2. Bagaimana Desain dokumen rekomendasi untuk memenuhi standar BSSN No. 4 Tahun 2021?

1.3. Batasan Masalah

Berikut adalah batasan masalah dari penelitian ini.

1. Desain serta Mapping Kontrol disini menghubungkan antara BSSN No. 4 Tahun 2021 dengan Indeks KAMI.
2. Untuk wawancara atau responden penelitian ini terbatas, yakni hanya pada ruang lingkup di TVRI Jatim.
3. Domain yang digunakan pada mapping kontrol Indeks KAMI yakni hanya pada domain Teknologi.

1.4. Tujuan Penelitian

1. Mendapatkan hasil persyaratan BSSN No. 4 Tahun 2021 yang belum terpenuhi berdasarkan domain Teknologi indeks KAMI.
2. Mapping kontrol keamanan informasi pada BSSN No. 4 Tahun 2021 dengan Indeks KAMI.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini merupakan hasil yang dapat dirasakan bagi semua pihak yang terlibat dalam penelitian ini. Adapun manfaat dari penelitian ini sebagai berikut:

1.5.1 Bagi Penulis

Penelitian ini sebagai wujud latihan serta pengembangan kemampuan dalam bidang teori yang telah diperoleh pada perkuliahan serta diharapkan mampu menjadi skripsi yang berkualitas.

1.5.2 Bagi Universitas

Penelitian ini diharapkan dapat dijadikan untuk menambah referensi sebagai bahan penelitian lanjutan yang lebih mendalam pada masa yang akan datang.

1.5.3 Bagi TVRI

- a. Memberikan rekomendasi melalui evaluasi keamanan informasi pada TVRI Jawa Timur serta membantu dalam memperbaiki keamanan informasi pada instansi.
- b. Memberikan solusi serta masukan pada pengelola keamanan informasi TVRI Jawa Timur yang dapat digunakan untuk perbaikan keamanan informasi dalam mendukung peningkatan kualitas keamanan informasi terutama pada domain Teknologi dari TVRI Jawa Timur.

1.6. Sistematika Penulisan Skripsi

BAB I PENDAHULUAN

Bab pendahuluan ini berisi tentang gambaran penelitian, yang terdiri dari uraian masalah, latar belakang, keterbatasan penelitian, tujuan penelitian, kegunaan penelitian, dan struktur penyusunan proposal penelitian.

BAB II TINJAUAN PUSTAKA

Pada bab kedua ini menjelaskan mengenai tinjauan dari penelitian terdahulu, teori dasar yang dipakai pada penelitian ini dan integrasi keilmuan dari penelitian yang dilakukan.

BAB III METODOLOGI PENELITIAN

Pada bab ketiga ini menjelaskan mengenai langkah-langkah penelitian yang logis serta terstruktur mulai dari awal perencanaan penelitian hingga akhir laporan yang

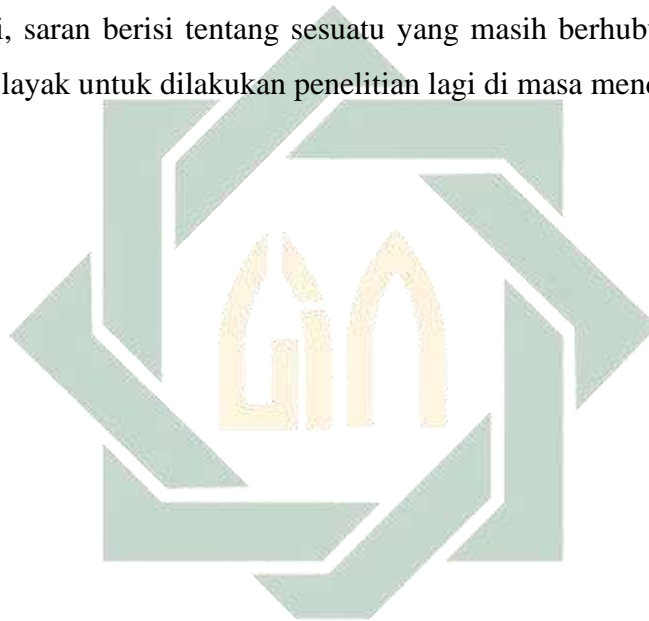
meliputi metode penelitian yang dipakai, alur penelitian serta jadwal penelitian dan lokasi penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab empat membahas mengenai hasil dari desain struktur serta mapping kontrol keamanan informasi BSSN No. 4 2021 dengan Indeks KAMI.

BAB V PENUTUP

Bab ini merupakan kesimpulan dari penelitian yang terdiri dari kesimpulan dan saran. Kesimpulan berisi tentang jawaban dari perumusan masalah yang dipakai dari penelitian ini, saran berisi tentang sesuatu yang masih berhubungan dengan penelitian ini dan layak untuk dilakukan penelitian lagi di masa mendatang.



UIN SUNAN AMPEL
S U R A B A Y A

BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Penelitian Terdahulu

Tinjauan penelitian terdahulu adalah referensi yang digunakan untuk dijadikan bahan pertimbangan materi. Penelitian terdahulu digunakan untuk mengutip beberapa pendapat dari beberapa hasil karya ilmiah yang telah dilakukan sebagai bahan pendukung. Berikut adalah beberapa hasil penelitian terdahulu yang memiliki tema dan pembahasan yang sama untuk dapat dijadikan rujukan maupun referensi. Adapun untuk referensi penelitian terdahulu dapat dilihat dibawah pada tabel 2.1.

Tabel 2. 1 Penelitian Terdahulu

Judul Penelitian	Nama Penulis (Tahun)	Hasil Penelitian
“Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks Kami (Studi Kasus: Dinas Komunikasi Dan Informatika Kota Pontianak)”.	“(Rahayu et al., 2021)”.	“Divisi ini menguji keutuhan kesesuaian serta daya guna pemakain teknologi pada perlindungan informasi, keluaran hasil penilaian tahapan teknologi keamanan informasi DISKOMINFO Kota Pontianak adalah 61 poin, total pertanyaan 26. sehingga diklasifikasikan ke dalam kategori keempat IV (Terkelola dan Terukur)

		”.
<p>“Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia”.</p>	<p>“(Damar Apri Sudarmadi, 2019)”.</p>	<p>“Penyelenggaraan Keamanan Siber di Indonesia. Berdasarkan 5 (Lima) Pilar GCI Penyelenggaraan keamanan siber di Indonesia pada aspek hukum yaitu Indonesia sudah mempunyai peraturan dengan substansi yang berkaitan dengan kejahatan siber dan keamanan siber, meskipun bentuk peraturan tidak berdiri sendiri dan secara khusus serta mendalam mengatur tentang kejahatan siber dan keamanan siber. BSSN diharapkan untuk dapat mendorong penyusunan UU keamanan siber, sehingga kebijakan tersebut dapat menjadi acuan bagi</p>

		<p>BSSN serta seluruh pemangku kepentingan. Indonesia sudah menyelenggarakan pelatihan bagi anggota POLRI secara rutin dan berkala, tetapi belum menyeluruh kepada seluruh aktor hukum di Indonesia”.</p>
<p>“Implementasi Indeks KAMI di Universitas Sam Ratulangi”.</p>	<p>“(Faturachman Husin Muh, 2017)”.</p>	<p>“Tingkat kematangan keamanan informasi di Universitas Sam Ratulangi masih tergolong rendah dan butuh perbaikan walaupun peran/tingkat ketergantungan akan TIK tergolong Tinggi. Pada aspek Teknologi dan Tata Kelola jauh lebih baik dibanding area keamanan lainnya. Hal sebaliknya terjadi pada Area Pengelolaan Aset dan Pengelolaan Risiko yang skornya</p>

		masih rendah”.
“Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1”.	“(Kornelia & Irawan, 2021)”.	<p>“Dari hasil penelitian yang sudah dilakukan tersebut bisa ditarik kesimpulan jika rentang tingkat Kelengkapan dan kematangan Keamanan informasi di Universitas Bina Darma saat ini masih ada dalam posisi TK II+ atau telah mencapai tingkat kematangan III yang dimana masih berstatus “Cukup Baik” untuk melaksanakan sertifikasi ISO/IEC 27001: 2013. Universitas Bina Darma diberikan rekomendasi untuk dilaksanakan pada keamanan informasi supaya bisa disebut layak dalam melaksanakan sertifikasi ISO-27001:2013 dan</p>

		juga bisa mengamankan semua informasi yang sebuah instansi kelola”.
<p>“Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi menggunakan Indeks KAMI dan ISO 27001 (Studi kasus Kominfo Jawa Timur)”.</p>	<p>“(Rizky Pratama & Reza Perdanakusuma, 2018)”.</p>	<p>“Kematangan keamanan informasi layanan Teknologi komunikasi dan informasi di Jawa Timur masih rendah. Informasi ini adalah bahwa KOMINFO tidak menerapkan semua ketentuan keamanan informasi atau direncanakan. level rendah Kelengkapan ini ditunjukkan dengan grafik batang berwarna merah Skor keseluruhan 245, yang berarti keamanan informasi layanan Teknologi komunikasi dan informasi di Jawa Timur tidak layak tetapi perlu memperbaiki. Selama jatuh tempo area keamanan individu</p>

		Informasi ada di I+”.
<p>“Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0”.</p>	<p>“(Budi et al., 2021)”.</p>	<p>“Disimpulkan bahwa saat ini Indonesia tengah dalam keadaan darurat cyber security dan sudah mencapai tahap memprihatinkan. Strategi cyber security yang harus dilakukan Indonesia untuk mewujudkan keamanan nasional di era society 5.0, adalah dengan: 1) capacity building pada semua stakeholder, 2) Pembentukan UndangUndang Khusus tentang Tindak Pidana Siber agar terwujud kepastian hukum untuk cyber security di Indonesia, 3) Peningkatan sumberdaya manusia dengan mendidik dan merekrut tenaga profesional yang memiliki integritas dan</p>

		<p>etika yang baik untuk mendukung penguatan cyber security. 4) Kerjasama stakeholder di dalam negeri melalui multi stakeholderism dan kerjasama internasional dalam pengembangan dan penguatan kapasitas kemampuan cyber security baik itu untuk infrastruktur, sarana prasarana maupun dalam pengembangan kemampuan sumberdaya dalam bidang cyber security”.</p>
--	--	--

2.2. Profil TVRI Jawa Timur

TVRI Jawa Timur adalah saluran televisi lokal yang didirikan oleh Televisi Republik Indonesia untuk wilayah Jawa Timur. TVRI Jawa Timur didirikan pada tanggal 3 Maret 1978 dengan nama TVRI Surabaya. TVRI Jawa Timur berkantor di Jl. Mayjen Jenderal Sungkono No. 124, Kota Surabaya. TVRI Jawa Timur menyediakan 92 saluran kepada TVRI milik negara, dan sisanya TVRI Jawa Timur memproduksi program khusus untuk provinsi Jawa Timur yang disiarkan di saluran TVRI Jawa Timur.

2.2.1 Visi TVRI Jawa Timur

Visi lembaga penyiaran publik Indonesia adalah menjadi lembaga penyiaran utama yang memotivasi dan memberdayakan melalui program informasi, pendidikan dan hiburan yang memperkuat persatuan dan keragaman untuk meningkatkan martabat bangsa.

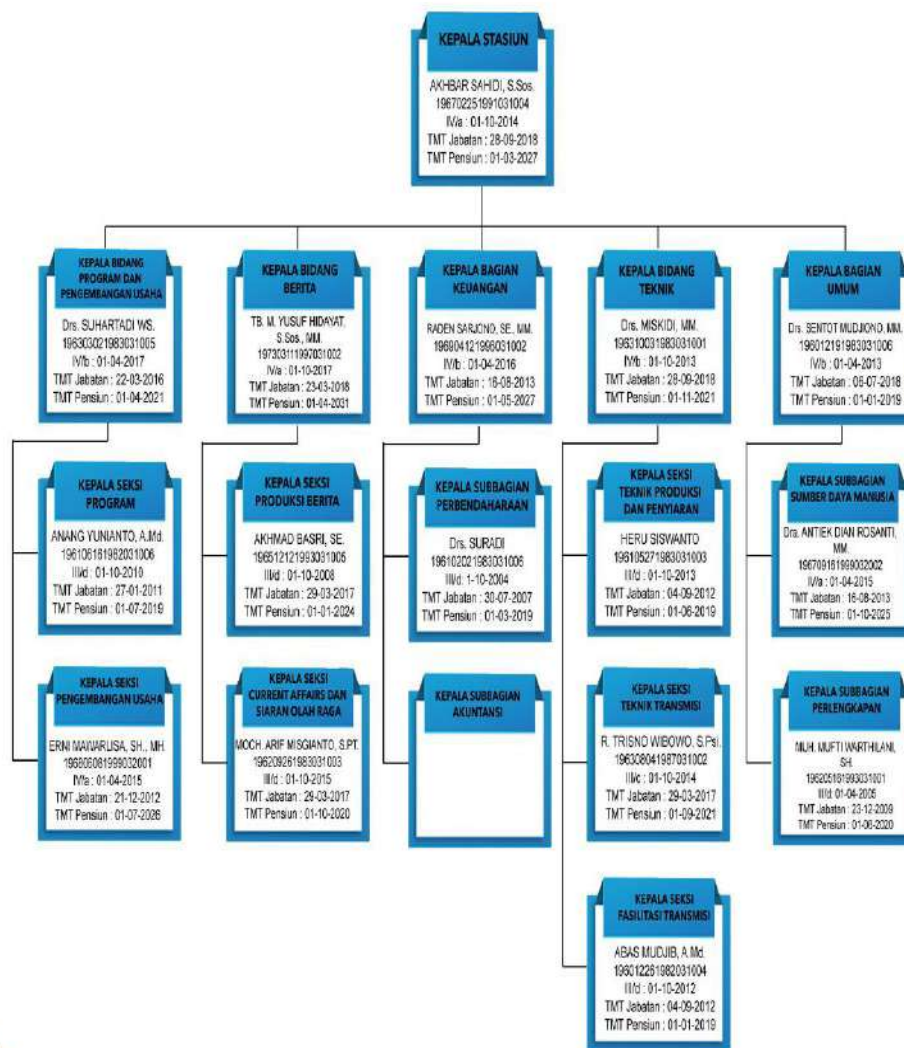
2.2.2 Misi TVRI Jawa Timur

Misi dari TVRI adalah :

1. Menyelenggarakan program siaran yang kredibel, memotivasi, dan memberdayakan yang memperkuat persatuan dan kebhinekaan untuk meningkatkan harkat dan martabat bangsa.
2. Kami mengelola sumber daya keuangan kami secara profesional, modern, dan terukur dengan kepemimpinan yang transparan, akuntabel, dan dapat dipercaya.
3. Menyelenggarakan penyiaran berbasis konvergensi digital berupa layanan lintas platform dengan menggunakan teknologi terkini. Dikelola dengan cara yang modern dan efisien serta dapat diakses di seluruh dunia.
4. Menyelenggarakan kepemimpinan yang berkualitas tinggi, kompeten, kreatif dan beretika secara transparan, berdasarkan meritokrasi dan menghormati keragaman.
5. Organisasi tata kelola kelembagaan melalui alur kerja yang ramping dan dinamis serta pengelolaan aset yang optimal dan efektif berdasarkan peraturan perundang-undangan.
6. Optimalisasi pemanfaatan aset, peningkatan pendapatan komersial, usaha lain yang terkait dengan penyelenggaraan penyiaran, dan pengembangan usaha berdasarkan peraturan perundang-undangan.

UIN SUNAN AMPEL
S U R A B A Y A

2.2.3 Struktur Organisasi TVRI Jawa Timur



Gambar 2.1 Struktur Organisasi TVRI Jawa Timur

Sumber : Website TVRI Jawa Timur (2019)

Berdasarkan gambar 2.1 tentang struktur organisasi TVRI Jawa Timur dapat dijelaskan bahwa TVRI Jawa Timur dipimpin oleh seorang kepala stasiun. Seorang Kepala Stasiun dalam menjalankan tugasnya membawahi kepala bidang program dan pengembangan usaha, kepala bidang berita, kepala bagian keuangan, kepala bidang Teknik kepala bagian umum. Untuk setiap kepala pada bagian tersebut juga membawahi beberapa divisi, diantaranya kepala bidang program dan pengembangan usaha membawahi kepala seksi program dan kepala seksi pengembangan usaha, kepala bidang berita membawahi kepala seksi produksi berita dan kepala seksi

current affairs dan olahraga, kepala bagian keuangan membawahi kepala subbagian perbendaharaan dan kepala subbagian akuntansi, kepala bidang Teknik membawahi kepala seksi teknik produksi dan penyiaran dan kepala seksi Teknik transmisi serta kepala seksi fasilitasi transmisi, yang terakhir kepala bagian umum membawahi kepala subbagian sumber daya manusia dan kepala subbagian perlengkapan.2.3. Dasar Teori

2.3.1 Keamanan Informasi

2.3.1.1 Definisi Informasi

Data diproses dan nilai yang dirasakan adalah informasi. Keputusan yang dibuat berdasarkan pemahaman informasi di atas harus mencakup data yang diolah menjadi informasi akhir (Sutabri, 2012). Oleh sebab itu, akurasi dari data yang terkumpul diperlukan agar dapat diolah menjadi informasi yang akurat dan valid yang dapat dipertimbangkan untuk digunakan lebih lanjut dalam proses pengambilan keputusan.

2.3.1.2 Keamanan Informasi

Keamanan informasi merupakan upaya untuk melindungi aset informasi dari potensi ancaman. Keamanan informasi secara tidak langsung menjamin kelangsungan bisnis, mengurangi risiko dan mengoptimalkan laba atas investasi. Semakin banyak informasi perusahaan disimpan, dikelola, dan dibagikan, semakin besar risiko korupsi, kehilangan, atau pengungkapan data kepada pihak eksternal yang tidak diinginkan (Iffano & Sarno, 2009).

Menurut G.J. Simons, keamanan sistem informasi adalah kemampuan untuk mencegah, atau setidaknya mendeteksi, penipuan (fraud) dalam sistem berbasis informasi dimana informasi itu sendiri tidak memiliki arti fisik. Menurut buku John D. Howard *An Analysis of Security Incidents on the Internet*, keamanan komputer adalah perlindungan terhadap serangan oleh pengguna komputer atau titik akses jaringan.

Berikut merupakan aspek keamanan dalam informasi yang harus menjadi fokus perhatian.

1. Confidentiality (Kerahasiaan)

Kerahasiaan mengacu pada aspek memastikan bahwa hanya pihak yang berwenang yang memiliki akses ke informasi dan data.

2. Integrity (Keutuhan)

Integritas adalah aspek yang menjamin dan dapat menjamin bahwa data tidak dapat diubah.

3. Availability (Ketersediaan)

Availability adalah sesuatu yang dapat memastikan bahwa pengguna dapat dengan mudah mengambil data kapanpun mereka membutuhkannya.

Keamanan informasi telah menjadi hal utama bagi sebuah instansi perusahaan (baik pemerintah maupun swasta), sehingga audit keamanan informasi menjadi suatu keharusan untuk menjaga nilai suatu informasi (Ciptanigrum Dwi, 2015).

Informasi yang berkualitas diperoleh dari seluruh proses yang dilakukan dengan berbagai cara. Menghasilkan informasi yang berkualitas memerlukan langkah-langkah keamanan untuk mencegah pengancaman dan gangguan yang dapat mempengaruhi nilai kualitas informasi (Whitman & Rahman, n.d.) Mengancam terkait dapat terjadi dimanapun kapanpun dan mempengaruhi operasi dan stabilitas proses bisnis organisasi.

2.3.2 Sistem Pemerintahan Berbasis Elektronik (SPBE)

SPBBE atau *E-Government* menjelaskan bahwa pemanfaatan TIK bertujuan untuk meningkatkan efisiensi, efektivitas dan transparansi dalam pertukaran dana dan informasi di lingkungan pemerintahan. *E-government* merupakan metode yang digunakan oleh pemerintah untuk memberikan pelayanan kepada publik, dengan tujuan untuk meningkatkan efisiensi kinerja pemerintah dan mempermudah akses publik terhadap informasi terkait pemerintahan. (Perpres No. 95, 2018)

Layanan SPBE atau *e-Government* dibagi menjadi 8 jenis (Angelopoulos et al., 2010):

1. Government to Citizen (Pemerintah untuk Warga Negara).

Menjelaskan bahwa penyelenggaraan pelayanan publik dilakukan secara online (online) melalui layanan elektronik yang terintegrasi, memberikan informasi dan komunikasi dari pemerintah kepada masyarakat.

2. *Citizen to Government* (Masyarakat untuk Pemerintah).

Penyediaan layanan pemerintah secara online, yang ditandai dengan layanan elektronik untuk pertukaran data dan informasi, serta penyampaian layanan publik dari masyarakat umum kepada pemerintah.

3. *Government to Business* (Pemerintah ke Bisnis).

Peningkatan inisiatif perdagangan elektronik seperti B. Pengembangan pengadaan elektronik dan pasar elektronik untuk pembelian barang-barang pemerintah dan penawaran elektronik untuk pengadaan pemerintah dari pemerintah ke perusahaan/swasta.

4. *Business to Government* (Bisnis untuk Pemerintah).

Meningkatkan sejumlah inisiatif elektronik untuk memungkinkan pengadaan pemerintah dan lelang publik untuk menjual barang dan jasa sebagai layanan elektronik dari bisnis/perseorangan kepada otoritas publik; Menyediakan dan mengembangkan pasar elektronik.

5. *Government to Employee* (Pemerintah untuk Pegawai).

Sarana pengelolaan layanan pegawai dan komunikasi internal dengan petugas melalui pengembangan aplikasi dan layanan transportasi elektronik untuk mengurangi konsumsi kertas dengan menggunakan sistem *electronic office* sebagai layanan pemerintah bagi pegawai.

6. *Government to Government* (Pemerintah untuk Pemerintah).

Mengadakan komunikasi online dan sarana kerjasama antara instansi pemerintah lainnya untuk meningkatkan efisiensi dan hasil efektivitas sebagai melayani atau aplikasi.

7. *Government to NGO* (Pemerintah untuk Nirlaba).

Pemerintah menyediakan informasi serta komunikasi dalam bentuk layanan atau aplikasi pada organisasi nirlaba seperti partai politik, organisasi sosial, komunitas atau organisasi nirlaba.

8. *NGO to Government* (Nirlaba untuk Pemerintah).

Pertukaran informasi dan komunikasi antara pemerintah dan organisasi nirlaba seperti partai politik, organisasi sosial dan organisasi masyarakat lainnya dalam bentuk layanan yang diberikan oleh LSM kepada lembaga pemerintah.

2.3.3 Pedoman BSSN No. 4 Tahun 2021

Sistem *E-Government* yang selanjutnya disingkat SPBE. Pemerintah menggunakan teknologi informasi dan komunikasi untuk memberikan pelayanan kepada pengguna SPBE. Badan Siber dan Sandi Negara yang disingkat BSSN adalah instansi pemerintah yang bertanggung jawab melaksanakan tanggung jawab keamanan siber pemerintah.

Manajemen Keamanan Informasi adalah sebaris proses untuk mencapai penyebaran keamanan SPBE yang efektif, layanan dukungan yang efisien dan berkelanjutan, dan SPBE berkualitas tinggi. Pada tahapan Pedoman Manajemen Keamanan Informasi ini mencakup beberapa proses antara lain; definisi ruang lingkup, identifikasi manajer, perencanaan, dukungan operasional, penilaian hasil kinerja dan pada akhirnya kondisi berkelanjutan.

2.3.3.1 Penetapan Ruang Lingkup

Penetapan ruang lingkup lingkup dalam hal ini menjelaskan :

- A. Topik internal keamanan informasi SPBE dalam organisasi.
- B. Topik external keamanan informasi pada SPBE.

Topik internal menjelaskan adalah bagaimana keamanan informasi SPBE pada suatu organisasi ditentukan berdasarkan bidang prioritas organisasi untuk menerapkan keamanan informasi SPBE. Bidang prioritas organisasi untuk menerapkan keamanan informasi SPBE adalah:

- a. Data serta informasi pada SPBE.
- b. Aplikasi ke SPBE.
- c. Nilai pada infrastruktur untuk SPBE.
- d. Prosedur keamanan informasi SPBE yang ada.

Kedua, masalah eksternal keamanan informasi SPBE sesuai dengan huruf b ayat (2) Peraturan BSSN Nomor 4 Tahun 2021 yang ditetapkan menurut ketentuan hukum.

2.3.3.2 Penetapan Penanggung Jawab

Penetapan penanggung jawab dalam hal ini dilakukan oleh petinggi kantor pusat serta pimpinan daerah. Penanggung jawab menjelaskan dalam Peraturan

BSSN Nomor 4 Tahun 2021 menjabat menjadi Sekretaris Daerah Pemerintah Daerah. Sekretaris Kantor Pusat dan Sekretaris Daerah Pemerintah Daerah yang juga disebut sebagai pengurus SPBE dalam melaksanakan tugasnya sebagai tanggung jawab pengamanan SPBE.

Dalam mengemban tugas untuk menjadi penanggung jawab keamanan SPBE, pengurus SPBE menetapkan rencana dari teknis Keamanan SPBE. Pelaksanaan teknik yang dimaksud terdiri atas:

- A. Pegawai Senior merupakan mereka yang punya tanggung jawab dan fungsi teknis, informasi dan komunikasi di Otoritas Pusat dan pemerintah daerah masing-masing.
- B. Personil yang mengawasi, membangun, memelihara, dan pengembangan beberapa aplikasi SPBE.

Pegawai Senior yang melaksanakan tanggung jawab dan fungsi keamanan teknis, informasi dan komunikasi di instansi pusat dan pemerintah memiliki tanggung jawab sebagai berikut:

- a. Memastikan implementasi standar dan rancangan dari teknis pengamanan SPBE.
- b. Menyusun, mengkoordinasikan, serta melaksanakan program kerja dan dana pengamanan SPBE.
- c. Memberitahukan pelaksanaan pengelolaan keamanan informasi SPBE dan pelaksanaan standar dari teknis pengamanan SPBE kepada koordinator SPBE otoritas pusat atau koordinator SPBE pada pemerintah daerah.

Seorang senior yang telah membawahi, membuat, merawat dan meluas permohonan SPBE sesuai dengan Pasal 6 (2) Peraturan BSSN No. 4 Tahun 2021 (b) bertanggung jawab untuk:

- 1. Penerapan standar teknis serta prosedur keamanan aplikasi di setiap unit kerja.
- 2. Menentukan dari aplikasi SPBE dan pembangunan infrastruktur, atau pembangunan melakukan dari pihak ketiga, mengikuti standar teknis dan rancangan pengamanan SPBE yang telah diputuskan.
- 3. Menentukan kelangsungan pada proses mengenai bisnis SPBE.

4. Koordinasi dengan beberapa pejabat senior Pratama yang melaksanakan tanggung jawab dan fungsi pengamanan teknis, data informasi dan komunikasi, serta instansi pemerintah pusat dan daerah terkait dalam penyusunan rancangan kerja dan dana SPBE.

2.3.3.3 Perencanaan

Perencanaan sebagaimana yang dimaksud yakni dilakukan oleh pelaksana teknis Keamanan SPBE. Dilakukan yakni dengan:

- A. Rencana Kerja Pengamanan SPBE dirancang berdasarkan bagian Risiko Pengamanan SPBE.
- B. Tujuan pelaksanaan Rencana Kerja Aman SPBE.

Kategori risiko keselamatan SPBE adalah huruf a ayat (2) Peraturan BSSN Nomor 4 Tahun 2021 yang menjelaskan bahwa hal itu dinyatakan sesuai dengan ketentuan undang-undang. Dijelaskan, pelaksanaan program kerja keselamatan SPBE akan ditetapkan dalam Peraturan BSSN Nomor 4 Tahun 2021 ayat (2) b, berdasarkan kebutuhan masing-masing otoritas pusat dan pemerintah daerah.

Rencana kerja Keamanan SPBE yang menjelaskan pada ayat (2) huruf a *Peraturan BSSN Nomor 4 Tahun 2021* yakni menjelaskan:

- a. Pelatihan kesadaran mengenai Keamanan SPBE.

Pelatihan kesadaran Keamanan SPBE mengartikan bahwa hal tersebut melalui kegiatan: sosialisasi serta pelatihan.

- b. Penilaian kerentanan Keamanan SPBE.

Mengenai kerentanan SPBE, setidaknya melalui: Menginventarisir seluruh aset SPBE, termasuk data dan informasi, aplikasi dan infrastruktur, mengidentifikasi kerentanan dan ancaman terhadap aset SPBE, serta mengukur tingkat risiko keamanan SPBE.

- c. Peningkatan Keamanan pada SPBE.

Peningkatan keamanan SPBE berdasarkan Klausul 8 (3) (c) didasarkan pada hasil Penilaian Kerentanan Keamanan SPBE berdasarkan Klausul 10. Setidaknya dilakukan oleh: Menerapkan standar dan rancangan teknis keamanan SPBE dan mengkaji fitur keamanan aplikasi SPBE dan infrastruktur SPBE.

d. Penanganan insiden Keamanan SPBE.

Penanganan Insiden Pengamanan SPBE sebagaimana dimaksud pada huruf d pada Pasal 3 dilakukan paling sedikit oleh: Memperhitungkan berbagai sumber serangan, menganalisis informasi insiden berikutnya, memprioritaskan respons insiden berdasarkan besarnya dampak yang dihadapi, mendokumentasikan temuan dan bukti pertemuan insiden, dan menilai dampak kerentanan SPBE berkurang atau berkurang.

e. Audit Keamanan pada SPBE.

Audit Keamanan SPBE berarti Pasal 8 (3) (e) dilakukan sesuai dengan ketentuan pada undang-undang.

2.3.3.4 Dukungan Pengoperasian

Dukungan operasional berdasarkan Pasal 3(1) huruf d Peraturan BSSN Nomor 4 Tahun 2021 melakukan petugas dari SPBE. Dukungan operasional mengartikan yaitu pada ayat (1) melakukan dimana peningkatan kapasitas sebagai berikut:

A. Petugas Keamanan SPBE

Petugas Keamanan SPBE sebagaimana dimaksud pada huruf a pada ayat (2) paling kurang memiliki kemampuan sebagai berikut: Keamanan infrastruktur teknologi, informasi dan komunikasi. Keamanan aplikasi. Untuk memenuhi kapasitas sumber daya manusia yang telah ditetapkan, kantor pusat dan pemerintah daerah paling kurang melakukan kegiatan sebagai berikut: Pelatihan dan sertifikasi kompetensi keamanan di bidang teknis, informasi, komunikasi, dan infrastruktur keamanan aplikasi, serta bimbingan teknis standar keamanan SPBE.

B. Dana Keamanan pada SPBE.

Dana pengamanan SPBE dari ayt (2) huruf b menyusun sejumlah rencana yang akan dilaksanakan pada pedoman atau ketetapan yang ditentukan peraturan pada undang-undang.

2.3.3.5 Evaluasi Kinerja

Dilakukan oleh Koordinator SPBE sehubungan dengan evaluasi kinerja berdasarkan Pasal 3 (1) (e) Peraturan BSSN Nomor 4 Tahun 2021. Evaluasi kinerja pada ayat (1) menjelaskan tentang pelaksanaan pengamanan SPBE. Penilaian kinerja menjelaskan dari pada ayat (2) dilakukan:

- A. Identifikasi tempat proses yang berisiko ketinggian pada keberhasilan implementasi keamanan SPBE.
- B. Tetapkan petunjuk kinerja untuk setiap tempat proses.
- C. Rencanakan implementasi keamanan SPBE Anda dengan mengukur kinerja yang berdasarkan konsep jumlah.
- D. Analisis efektivitas penerapan pengamanan SPBE.
- E. Dukungan dan pelaksanaan program audit keamanan SPBE.

Pasal 15 (4) Ayat 1 Evaluasi kinerja dilakukan sekurang-kurangnya satu kali dalam setahun.

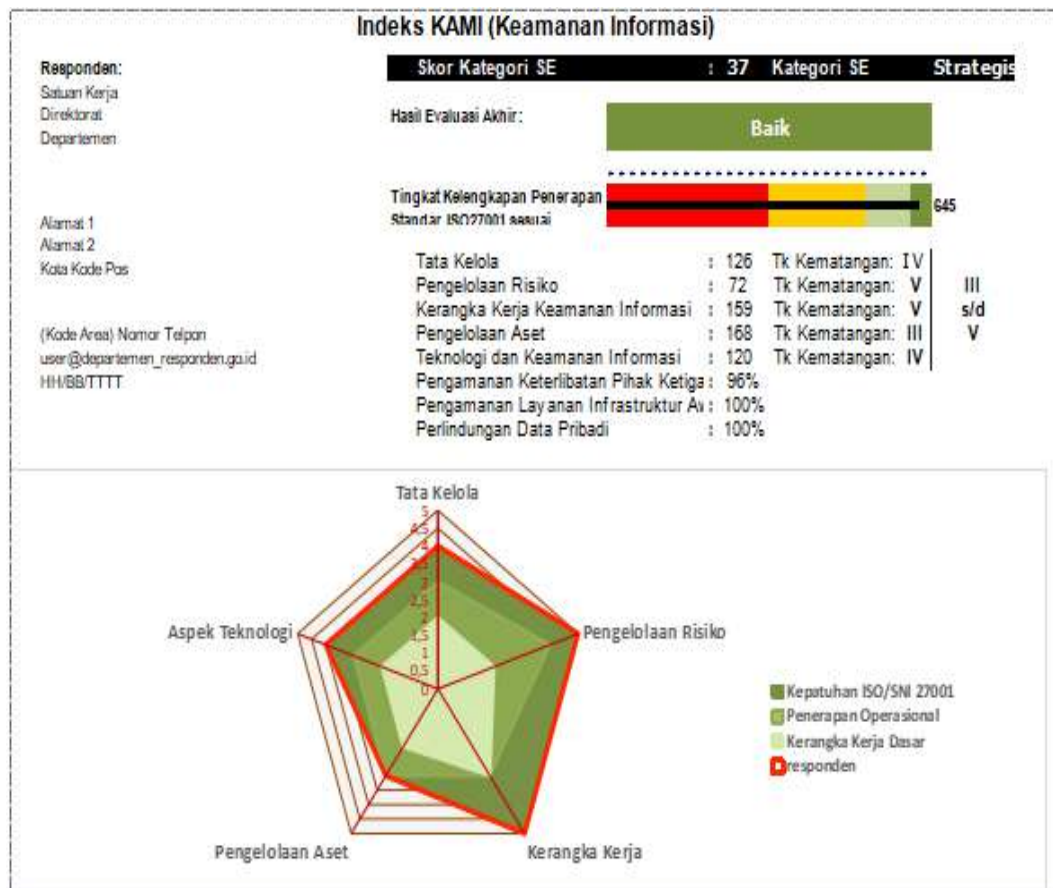
2.3.3.6 Perbaikan Berkelanjutan

Perbaikan Berkelanjutan diatur dalam Pasal 3 Ayat (1) Huruf f Peraturan BSSN Nomor 4 Tahun 2021 yang dilaksanakan oleh pelaksana rancangan Teknis Pengamanan SPBE. Perbaikan berkelanjutan menjelaskan dari ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja. Dijelaskan bahwa yang dimaksud dengan perbaikan terus-menerus pada ayat (1) adalah sebagai berikut:

- A. Menguasai permasalahan dalam rancangan untuk pengamanan SPBE.
- B. Penyempurnaan implementasi keamanan SPBE langsung berkala.

2.3.4 Indeks KAMI

Indeks KAMI digunakan sebagai alat untuk memberikan gambaran umum tentang kesiapan (kelengkapan dan kematangan) dari kerangka keamanan informasi mereka kepada para pemimpin Lembaga (RPM Pusat Koordnasi Penanganan Insiden Keamanan Informasi Pemerintah, 2011). organisasi atau institusi. Berikut adalah mind mapping dari Indeks KAMI, dapat dilihat pada gambar 2.2.



Gambar 2. 2 Indeks KAMI versi 4.2 - Mei 2021

Indeks Keamanan Informasi (KAMI) adalah aplikasi yang digunakan sebagai alat untuk menilai dan menilai maturitas (kelengkapan dan kematangan) aplikasi keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001. Proses evaluasi dilakukan melalui serangkaian pertanyaan di bidang-bidang berikut:

1. “Kategori Sistem Elektronik yang digunakan.”
2. “Tata Kelola Keamanan Informasi.”
3. “Pengelolaan Risiko Keamanan Informasi.”
4. “Kerangka Kerja Keamanan Informasi.”
5. “Pengelolaan Aset Informasi.”
6. “Teknologi dan Keamanan Informasi.”
7. “Suplemen (Pengukuran tambahan telah dilakukan pada aspek outsourcing pihak ketiga dari penyedia layanan, keamanan layanan infrastruktur cloud (layanan cloud) dan perlindungan data pribadi).”

2.3.5 Domain Teknologi dan Keamanan Informasi

Fokus pada penelitian ini yakni pada domain ke-enam pada Indeks KAMI, yaitu Teknologi dan Keamanan Informasi berisi mengenai kegiatan mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Berisikan 26 standar teknis pelaksanaan yang dikategorikan melalui empat tingkat kematangan, yakni tingkat I - IV tingkat kematangan.

Berikut untuk isi dari domain Teknologi dan Keamanan Informasi dapat dilihat pada gambar dibawah pada 2.4 – 2.5.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?
6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?
6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian <i>password</i> secara otomatis, termasuk menon-aktifkan <i>password</i> , mengatur kompleksitas/panjangnya dan penggunaan kembali <i>password</i> lama?

Gambar 2. 3 Domain Teknologi dan Keamanan Informasi bagian 1

6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses <i>timeouts</i> , <i>lockout</i> setelah kegagalan <i>login</i> dan penarikan akses?
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?
6.19	II	1	Apakah sistem operasi untuk setiap perangkat <i>desktop</i> dan <i>server</i> dimutakhirkan dengan versi terkini?
6.20	II	1	Apakah setiap <i>desktop</i> dan <i>server</i> dilindungi dari penyerangan virus (<i>malware</i>)?
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - <i>audit trail</i>) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?
6.25	III	3	Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?

Gambar 2. 4 Domain Teknologi dan Keamanan Informasi bagian 2

2.3.6 RACI

Matriks RACI adalah bagian dari RAM (Responsibility Assignment Matrix), sebuah alat yang digunakan untuk menunjukkan penugasan setiap aktivitas untuk setiap anggota proyek. Penugasan setiap anggota dapat bervariasi tergantung pada keterampilan dan tanggung jawab yang ditugaskan (Setiaji & Widiyanti, n.d.). Perbedaan diwakili oleh huruf R-A-C-I. Uraian peran dan fungsi dalam RACI di bawah ini memiliki definisi yang lebih spesifik, yaitu:

1. **R-Responsible.** Pihak yang bertanggung jawab untuk melakukan kegiatan. Setiap aktivitas mungkin memiliki beberapa orang.
2. **A-Accountable.** Pihak yang memiliki wewenang dan tanggung jawab atas kegiatan yang bersangkutan. Artinya pihak ini memiliki tanggung jawab utama atas keberhasilan kegiatan tersebut. Hanya satu orang yang dapat berpartisipasi dalam setiap aktivitas.
3. **C-Consulted.** Pihak yang mencari konsultasi atau saran mengenai kegiatan yang bersangkutan. Setiap aktivitas mungkin memiliki beberapa orang.
4. **I-Informed.** Pihak yang akan diberitahu tentang kemajuan pekerjaan yang bersangkutan. Setiap aktivitas mungkin memiliki beberapa orang.

2.3.7 ISO 27001

Didirikan pada 23 Februari 1947, *Organisasi International Standardisasi (ISO)* mengumumkan standar industri dan komersial yang digunakan di seluruh

dunia dan berkantor pusat di Jenewa, Swiss (Schneider et al., 2017). ISO 27001 kini menjadi Standar Nasional Indonesia (SNI) dan standar kriteria umum untuk memberikan persyaratan bagi pembentukan, penerapan, pemeliharaan, dan peningkatan berkelanjutan Sistem Manajemen Keamanan Informasi (SMKI). ISO 27001 bertujuan untuk memastikan pemilihan yang benar dan keseimbangan langkah-langkah keamanan untuk melindungi aset informasi. Standar ini umumnya diterapkan pada semua jenis organisasi, baik swasta maupun publik (Calder & Watkins, 2008).

Standar ini memiliki beberapa penjelasan dalam persyaratan untuk penanganan dan penilaian risiko keamanan informasi yang akan menyesuaikan dengan masing-masing kebutuhan pada organisasi. Persyaratan yang ditetapkan pada standar ini bersifat umum bertujuan agar bisa diterapkan pada seluruh organisasi terlepas dari jenis, sifat serta beberapa ukuran dari organisasi tersebut.

Hal ini dirancang untuk menjaga Integritas, kerahasiaan dan ketersediaan pada informasi atau data yang dibutuhkan. Standar ini bisa digunakan baik dari pihak organisasi atau *internal* maupun pihak *eksternal* dari organisasi dengan tujuan untuk dapat mengukur kemampuan organisasi atau perusahaan dalam syarat dari masing-masing organisasi. Selain standar ISO 27001, terdapat standar-standar lain untuk keamanan informasi seperti ISO 27002, ISO 27004 dan ISO 27005. Namun standar yang paling sering digunakan untuk organisasi atau perusahaan adalah ISO/IEC 27001.

2.3.8 Hubungan ISO 27001 dengan BSSN 2021

Pada dasarnya, standar pelaksanaan teknis dari BSSN 2021 merupakan sebuah produk lokal yang diadopsi yang bertujuan agar tidak ada ketergantungan dengan produk framework dari luar, berisi 14 klausul yang ada dalam ISO 27001 : 2013 yang mencakup : “Kebijakan Keamanan Informasi, Keamanan Informasi Organisasi, Keamanan sumber daya manusia, Pengelolaan Aset, Akses Kontrol, Cryptographic, Keamanan Fisik dan lingkungan, Operasi keamanan, Komunikasi Keamanan, Akuisisi sistem, pengembangan, dan pemeliharaan, Supplier Relationship, Manajemen Insiden Keamanan Informasi, Aspek Keamanan

Informasi of Business Continuity Management, serta Kepatuhan”. Selanjutnya Pemerintah kemudian mengesahkan serta membuat peraturan agar seluruh instansi maupun organisasi *e-goverment* yang ada di Indonesia agar menggunakan BSSN 2021.

2.3 Integrasi Keilmuan

Isu kedua setelah memenuhi kebutuhan pangan adalah masalah keamanan umat Islam. Membangun keselamatan dan keamanan umat Islam sama dengan membangun keimanan. Hal ini dapat dilihat pada nabi Ibrahim yang melakukan perjalanan untuk mencari Tuhan, menemukan iman, dan menjaga keamanan komunitasnya (bangsa). QS An-Nur:55 :

وَعَدَ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَعَمِلُوا الصَّالِحَاتِ لَيَسْتَخْلِفَنَّهُمْ فِي الْأَرْضِ كَمَا اسْتَخْلَفَ الَّذِينَ مِن قَبْلِهِمْ وَلَيُمَكِّنَنَّ لَهُمْ دِينَهُمُ الَّذِي ارْتَضَى لَهُمْ وَلَيُبَدِّلَنَّهُم مِّن بَعْدِ خَوْفِهِمْ أَمْنًا يَعْبُدُونَنِي لَا يُشْرِكُونَ بِي شَيْئًا وَمَن كَفَرَ بَعْدَ ذَلِكَ فَأُولَٰئِكَ هُمُ الْفَاسِقُونَ

Yang berarti: “Dan Allah telah berjanji kepada orang-orang yang beriman dan mengerjakan amal saleh di antara kamu bahwa Dia akan menjadikan mereka kuat dan Dia benar-benar akan meneguhkan agama mereka yang Dia kehendaki bagi mereka dan Dia benar-benar akan mengubah mereka (keadaan) setelah mereka takut. mereka damai. Mereka terus menyembah Aku tanpa mempersekutukan Aku dengan apapun. Dan siapa (tetap) kafir setelah itu (berjanji), mereka itulah orang-orang fasik”

Manajemen Keamanan pada suatu instansi maupun organisasi dalam sudut pandang Islam menurut bapak Ali Imron, SQ, SH, MH salah satu penghafal Al-Quran sekaligus civitas akademika yang menekuni bidang Hukum Islam Indonesia. Beliau mengemukakan hal penting yang perlu dilakukan dalam menciptakan keamanan yaitu dengan menyebarkan dakwah pada akidah yang benar kepada umat manusia dan menghilangkan penghindaran, besar atau kecil. Dengan demikian, janji Allah akan digenapi. Allah tidak mengingkari janji-Nya.

Sikap Nabi Muhammad SAW dalam menghadapi realitas dakwah seringkali membuat orang yang membaca syirahnya terheran-heran. Dalam hal ini termasuk masalah sosial dan budaya. Beliau selalu menunjukkan sikap yang mengutamakan

keadilan, toleransi dan kasih sayang, tidak terkecuali terhadap yang non-Muslim, baik yang mendukung maupun yang menentangnya (HR, Al-Bukhari).

QS. Al-Anbiya' : 107 :

وَمَا أَرْسَلْنَاكَ إِلَّا رَحْمَةً لِّلْعَالَمِينَ

Yang artinya: “Dan Kami tidak mengutus engkau (Muhammad) melainkan untuk (menjadi) rahmat bagi seluruh alam”.

Kisah lain yang sangat menarik adalah ketika Nabi Muhammad pertama kali memasuki Yatsrib. Di sana ia menemukan masyarakat yang pluralistik. Ada kelompok pendatang yang disebut Muhajirin, ada kelompok pribumi yang disebut Ansar, dan ada yang non-Muslim (Yahudi). Bani Qainuqa, Bani Quraizhah, Bani Nadhir. Nabi Muhammad SAW kemudian meliputi kekhawatiran tentang bagaimana menyikapi kenyataan pluralisme, namun pada akhirnya, setelah mempertimbangkan dan mengkaji segala sesuatu dari sudut pandang yang berbeda, beliau memutuskan bahwa pluralisme ini tercapai Sebuah konsensus yang dapat diintegrasikan ke dalam komunitas sosial, struktur berdasarkan Tamadun (Hubungan non-agama). Konsensus tersebut akhirnya dideklarasikan dengan nama Sahifa Medina (Piagam Madinah). Ini adalah konstitusi progresif dan revolusioner yang mengatur komitmen bersama untuk melindungi Madinah dari apapun yang dapat mengganggu hubungan sosial, properti, dan stabilitas lingkungan. Dalam konteks hal tersebut dapat diartikan stabilitas lingkungan sebagai manajemen keamanan.

Sudut pandang islam dalam menerima informasi, Ketika datang Jadal Al-Qur'an (debat dalam Al-Qur'an), hal ini dilakukan untuk meyakinkan lawan bicara bahwa setiap pernyataan dalam Al-Qur'an disertai dengan penalaran yang kuat. Argumen orang-orang yang tidak percaya padanya. Misalnya, antara lain, ada argumen untuk melemahkan orang-orang yang mengingkari Al-Qur'an.

QS Al-Baqoroh : 23(tafsifweb.com):

وَإِن كُنْتُمْ فِي رَيْبٍ مِّمَّا نَزَّلْنَا عَلَىٰ عَبْدِنَا فَأْتُوا بِسُورَةٍ مِّثْلِهِ وَادْعُوا شُهَدَاءَكُمْ مِّن دُونِ اللَّهِ إِنْ كُنْتُمْ صَادِقِينَ

Yang artinya: *“Dan jika kamu (tetap) dalam keraguan tentang Al Quran yang Kami wahyukan kepada hamba Kami (Muhammad), buatlah satu surat (saja) yang semisal Al Quran itu dan ajaklah penolong-penolongmu selain Allah, jika kamu orang-orang yang benar”*.

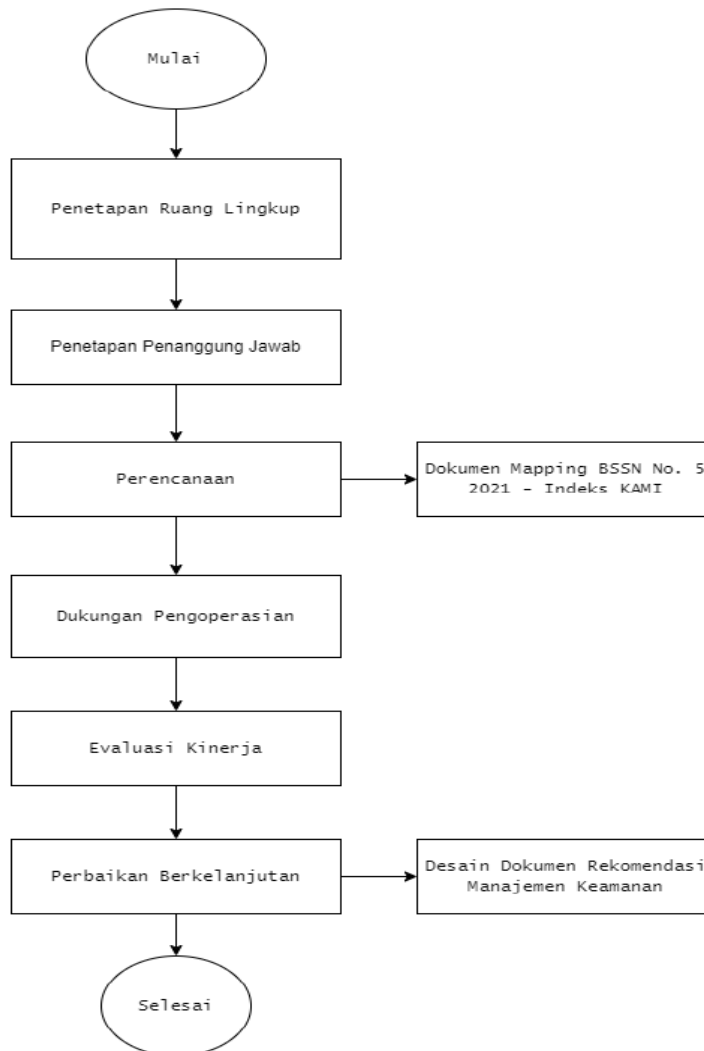


UIN SUNAN AMPEL
S U R A B A Y A

BAB III METODOLOGI

3.1 Metodologi Penelitian

Metodologi Penelitian adalah susunan metode atau prosedur yang digunakan pada sebuah penelitian agar dapat mencapai tujuan penelitian. Untuk prosedur serta alur pada penelitian ini dapat dilihat dibawah pada Gambar 3.1.



Gambar 3. 1 Alur Penelitian

Dalam Gambar 3.1 menunjukkan alur metode penelitian dengan penjelasan sebagai berikut:

1. Memulai Penetapan Ruang Lingkup dengan melakukan observasi serta wawancara kepada bidang teknologi informasi pada TVRI Jawa Timur.

2. Melakukan tahapan Penetapan Penanggung Jawab yakni pemilihan penanggung jawab dengan menggunakan metode RACI.
3. Melakukan Perencanaan yakni mapping control dengan menggunakan pedoman standar teknis dari BSSN 4 2021 dan Indeks KAMI.
4. Melakukan Dukungan Pengoperasian yaitu *chrosschek* ulang hasil mapping control serta pencocokan ulang pasal-pasal yang ada pada BSSN 4 2021 dan Indeks KAMI.
5. Melakukan Evaluasi Kinerja dari hasil Mapping Kontrol yang berupa hasil tingkat kelengkapan serta kematangan Keamanan Informasi berupa Dokumen Pembukti.
6. Melakukan Perbaikan Berkelanjutan yaitu membuat Rekomendasi berdasarkan BSSN 2021 serta domain Teknologi pada Indeks KAMI.

3.2 Tahapan Penelitian

3.2.1 Penetapan Ruang Lingkup

Langkah awal penyelidikan ini adalah Penetapan ruang lingkup. Proses mengumpulkan informasi melalui wawancara kepada bidang infrastruktur teknologi pada TVRI Jawa Timur. Teknik wawancara merupakan cara sistematis untuk memperoleh informasi-informasi dalam bentuk pernyataan-pernyataan lisan mengenai suatu obyek atau peristiwa pada masa lalu, kini, dan akan datang (IDA BAGUS GDE PUJAASTAWA, 2016). Wawancara adalah sesi tanya jawab tatap muka dengan mengajukan pertanyaan spesifik terkait dengan studi kasus yang diangkat. Hasil wawancara akan ditulis diatas kertas dan tanda tangan dari responden akan diperlukan sebagai bukti bahwa wawancara telah dilakukan dan didokumentasikan.

3.2.2 Penetapan Penanggung Jawab

Proses Penetapan Penanggung Jawab dilakukan dengan menggunakan metode Matriks RACI (*Responsibility assignment matrix*), yang didalamnya terdapat 4 kriteria dalam hal penetapan penanggung jawab, diantaranya: Responsible, Accountable, Consulted, dan Informed. Metode ini secara efektif mengurangi kebingungan tentang target yang ditetapkan dan meningkatkan kinerja dan efisiensi.

3.2.3 Perencanaan

Proses Perencanaan yakni Upaya untuk menentukan berbagai hal yang akan dicapai di masa yang akan datang dan berbagai tahapan yang diperlukan untuk mencapai tujuan tersebut. Dalam tahap ini yang direncanakan yakni proses Mapping control BSSN 4 2021 dan Indeks KAMI. Mapping dalam tahapan ini peneliti menggunakan standar teknis keamanan dari Pedoman BSSN 2021 yang dikorelasikan dengan Indeks KAMI. Output dari proses ini yakni mapping control dari BSSN No. 5 Tahun 2021 dengan Indeks KAMI.

3.2.4 Dukungan Pengoperasian

Proses Dukungan Pengoperasian dalam tahap ini yakni Pengecekan ulang mapping antara BSSN No. 4 2021 dengan Indeks KAMI, serta membuat Dokumen Desain yang berdasarkan Standar Teknis Keamanan sebagaimana dimaksud pada pasal 25 (1) tentang standar aplikasi web, yakni mencakup terpenuhinya: autentikasi, manajemen sesi, persyaratan kontrol akses, validasi input, kriptografi pada verifikasi statis, penanganan error dan pencatatan log, proteksi data, keamanan komunikasi, pengendalian kode berbahaya, logika bisnis, *file*, keamanan API dan *web service*, dan keamanan konfigurasi.

3.2.5 Evaluasi Kinerja

Setelah melakukan proses wawancara serta dilakukanya Kontrol Mapping, maka dilakukan evaluasi penilaian terhadap syarat-syarat dari BSSN 2021. Dengan hasil yang didapatkan peneliti akan melihat syarat dari BSSN yang telah terpenuhi dan belum terpenuhi. Kemudian dari syarat yang belum terpenuhi itu akan diberikan rekomendasi serta crosschek ulang terhadap dokumen desain mapping yang telah dibuat pada proses sebelumnya.

3.2.6 Perbaikan Berkelanjutan

Pembuatan rekomendasi didasarkan pada hasil Mapping Kontrol serta Desain dokumen yang telah dilakukan pada proses sebelumnya. Rekomendasi dibuat sebagai acuan bagi organisasi agar tata kelola keamanan informasi yang ada sekarang dapat sesuai dengan standar BSSN 4 2021. Rekomendasi dapat dijalankan secara bertahap sehingga rekomendasi ini dapat dikembangkan dan digunakan oleh instansi.

3.3 Lokasi Penelitian

Lokasi penelitian pada penelitian dengan judul “Desain Sistem Keamanan Informasi berdasarkan Peraturan BSSN No. 4 Tahun 2021 dengan Indeks KAMI” ini dilakukan di TVRI Jawa Timur, berkantor di Jl. Mayjen Sungkono No. 124, Kota Surabaya.

3.4 Waktu Penelitian

Penelitian yang berjudul “Desain Keamanan Informasi berdasarkan Peraturan BSSN No.4 Tahun 2021 dan Indeks KAMI” dilaksanakan kurang lebih selama 3 bulan, terhitung sejak April 2023 – Juni 2023. Dapat dilihat dibawah pada tabel 3.4.

Tabel 3. 1 Timeline Penelitian

No	Kegiatan	April				Mei				Juni			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Penetapan Ruang Lingkup												
2	Penetapan Penanggung Jawab												
3	Perencanaan												
4	Dukungan Pengoperasian												
5	Evaluasi Kinerja												
6	Perbaikan Berkelanjutan												
7	Pembuatan Laporan												

BAB IV HASIL DAN PEMBAHASAN

4.1 Proses Mapping Dokumen

4.1.1 Gambaran Umum Objek

TVRI Jawa Timur merupakan stasiun televisi pertama di Indonesia yang melakukan siaran berita maupun hiburan sebelum bermunculan stasiun-stasiun TV swasta. Pada mulanya TVRI Jatim berdiri dengan adanya stasiun pemancar relay di Comorosewu dan Surabaya yang telah diresmikan.

TVRI Stasiun Jawa Timur berdiri pada waktu stasiun pemancar relay di Comorosewu dan Surabaya diresmikan. Kedua stasiun pemancar relay mulai dioperasikan pada bulan Juni dan Juli 1971 dengan merelay sepenuhnya siaran dari Jakarta. Sejak Tanggal 3 Maret 1978 TVRI Stasiun Surabaya diresmikan, TVRI Stasiun Surabaya memulai siaran secara resmi. Siaran pertama Televisi di Indonesia berupa siaran percobaan dilakukan pada tanggal 17 Agustus 1962, dalam bentuk siaran langsung Upacara Peringatan Detik-detik Proklamasi di Istana Merdeka Jakarta. Siaran secara teratur baru dapat dilakukan pada tanggal 24 Agustus 1962, bertepatan dengan upacara pembukaan ASIAN GAMES IV.

Oleh karena itu pada tanggal 24 Agustus 1962 di peringati sebagai hari lahirnya TVRI Stasiun Jawa Timur, tetapi pada jaman dahulu TVRI Stasiun Jawa Timur lebih di kenal dengan TVRI Surabaya. TVRI Surabaya berubah sabagai TVRI Jawa Timur karena tuntutan berbagai macam pihak. TVRI Surabaya di rasa hanya milik orang Surabaya saja, maka di gantilah sebagai TVRI Stasiun Jawa Timur. Pemberian nama ini bertujuan agar TVRI Stasiun Jawa Timur bukan hanya milik masyarakat Surabaya saja.

Alamat : Jl. Mayjen Sungkono No. 124 Surabaya 60189

Phone : (031) 5678298, 5768453, 5677352, 5678452

Website : <http://www.tvri.co.id>

4.1.1.1 Logo TVRI Jawa Timur



Gambar 4. 1 Logo TVRI Jawa Timur

Gambar diatas merupakan logo saat ini dari instansi TVRI Jawa Timur.

4.1.1.2 Website TVRI Jawa Timur

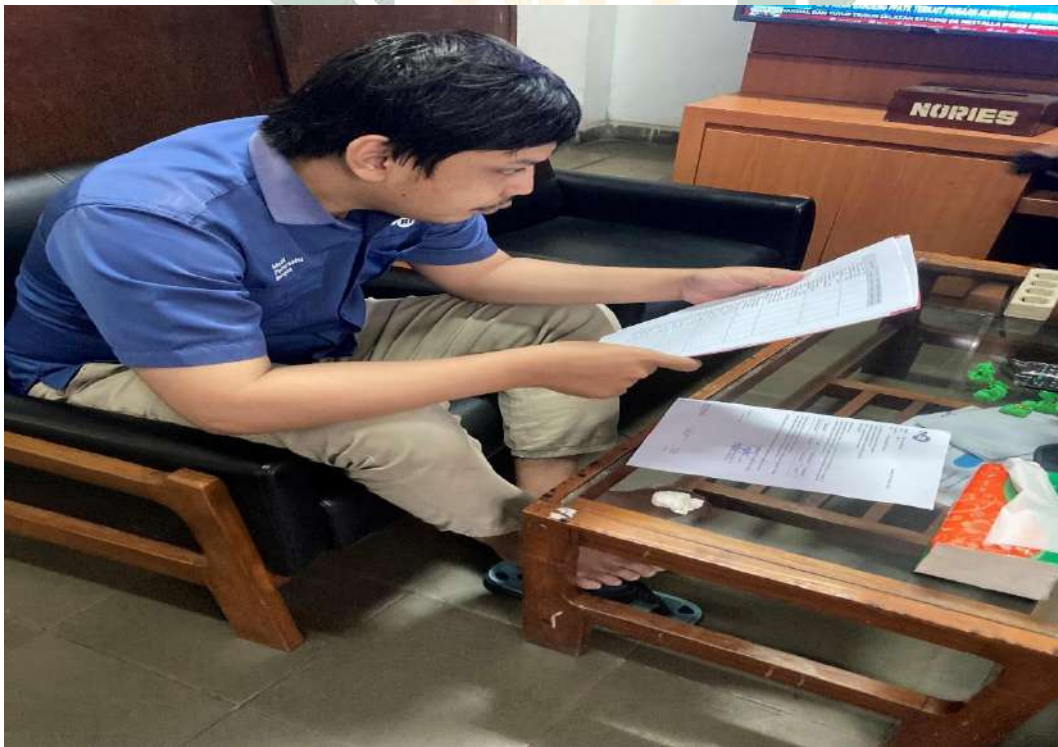


Gambar 4. 2 Tampilan website TVRI Jawa Timur

Gambar diatas merupakan tampilan utama dari salah satu produk teknologi dari TVRI Jawa Timur yakni website yang berisi layanan informasi serta berita dan acara pada TVRI Jawa Timur, dapat diakses pada <https://tvri.go.id/stasiun/jatim>.

4.1.2 Penetapan Ruang Lingkup

Oobservasi serta wawancara mengenai manajemen keamanan informasi pada TVRI Jawa Timur dengan menggunakan form validasi mapping antara Indeks KAMI dengan BSSN No. 4 Tahun 2021. Dengan tujuan mendapatkan informasi serta maksud terhadap manajemen keamanan informasi yang jelas pada TVRI Jawa Timur. Untuk bukti responden penelitian yang dilakukan dengan metode wawancara yakni dengan salah satu staff IT yang mempunyai wewenang dalam mengatur sarana prasarana dalam bidang Jaringan dan IT yang sebagai perwakilan dalam wawancara dari pihak TVRI Jawa Timur yang bernama Aditya Wijaya. Sedangkan untuk bukti dokumentasi lainnya ada pada lampiran berikut beberapa foto dokumentasi seperti pada Gambar 4.4 sebagai berikut.



Gambar 4. 3 Dokumentasi Wawancara

4.1.3 Penetapan Penanggung Jawab

Dalam tahapan penetapan penanggung jawab yakni mendefinisikan tugas masing masing dalam hal ini menggunakan standar RACI. Metode ini secara efektif mengurangi kebingungan tentang tujuan yang ditetapkan dan meningkatkan kinerja dan efisiensi. Dengan kata lain, RACI membantu membuat keputusan lebih cepat dan lebih bertanggung jawab, dan pembagian tugas tidak tumpang tindih. Berikut adalah pembagian berdasarkan RACI pada TVRI Jawa Timur.

1. Responsible

Siapa yang bertugas menyelesaikan tugas.

Nama : Drs. Miskidi, MM.

Jabatan : Kepala Bidang Teknik

TMT Jabatan : 28 - 09 - 2018

2. Accountable

Siapa yang berhak mengambil keputusan dan tindakan strategis terkait dengan tugas.

Nama : Akhbar Sahidi, S. Sos.

Jabatan : Kepala Stasiun

TMT Jabatan : 28 - 09 - 2018

3. Consulted

Orang yang dapat dihubungi untuk keputusan dan tugas yang tertunda.

Nama : Drs. Sentot Mudjiono, MM.

Jabatan : Kepala Bagian Umum

TMT Jabatan : 06 - 07 - 2018

4. Informed

Siapa yang harus secara teratur diberitahu tentang semua keputusan dan tindakan strategis selama proyek berlangsung.

Nama : Drs. Antiek Dian Rosanti, MM.

Jabatan : Kepala Subbagian Sumber Daya Manusia

TMT Jabatan : 16 - 06 - 2013

4.1.4 Perencanaan

Adanya proses perencanaan yakni upaya untuk menentukan berbagai hal yang akan dicapai di masa depan serta berbagai tahapan yang diperlukan untuk mencapai tujuan tersebut. Dalam tahapan ini peneliti menggunakan standar teknis keamanan dari Pedoman BSSN 2021 serta Indeks KAMI.

Untuk metode yang digunakan yakni mapping BSSN 2021 dengan Indeks KAMI, untuk status indikator dapat dilihat Tabel dibawah.

Tabel 4. 1 Indikator Mapping Indeks KAMI dan BSSN 2021

1	2	3	0	1	2	3
ID	Pertanyaan Indeks KAMI	Peraturan BSSN No 4 Tahun 2021	Tidak dilakukan	Dalam perencanaan	Diterapkan sebagian	Diterapkan menyeluruh
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Pasal 26 (a) autentikasi, Pasal 26 (b) manajemen sesi				
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Pasal 26 (h) keamanan komunikasi				
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Pasal 26 (d) validasi input				
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Pasal 26 (m) keamanan konfigurasi				
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Pasal 26 (g) proteksi data				
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Pasal 26 (j) logika bisnis				
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Pasal 26 (m) keamanan konfigurasi				
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Pasal 26 (f) penanganan error dan pencatatan log				

Adapun status indikator pada seluruh kuisisioner pertanyaan pada gambar diatas dapat diartikan sebagai berikut:

1. ID Kode Pertanyaan
2. Daftar Pertanyaan Indeks KAMI
3. Peraturan BSSN No. 4 Tahun 2021
4. Status Penerapan

Untuk hasil dari Mapping antara BSSN No. 4 2021 dengan Indeks KAMI dapat dilihat pada tabel 4.2-4.4 dibawah.

Tabel 4. 2 Mapping control bagian 1

Domain Teknologi		26 (a) autentikasi	26 (b) manajemen sesi	26 (c) persyaratan kontrol akses	26 (d) validasi input	26 (e) kriptografi pada verifikasi statis	26 (f) penanganan error dan pencatatan log	26 (g) proteksi data	26 (h) keamanan komunikasi	26 (i) pengendalian kode berbahaya	26 (j) logika bisnis	26 (k) file	26 (l) keamanan API dan web service	26 (m) keamanan konfigurasi
ID	Indeks KAMI	Peraturan BSSN No. 4 Tahun 2021												
6.1	"Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?"													
6.2	"Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?"													
6.3	"Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?"													
6.4	"Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?"													
6.5	"Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?"													
6.6	"Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?"													
6.7	"Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?"													
6.8	"Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?"													

Data mapping tabel diatas menunjukkan bahwa setiap poin sub pada indeks KAMI semuanya berhubungan dengan Peraturan BSSN No. 4 Tahun 2021 pada Pasal 26 yakni standar teknis keamanan basis web yang terdiri dari: autentikasi, manajemen sesi, persyaratan kontrol akses, validasi input, kriptografi pada verifikasi statis, penanganan eror dan pencatatan log, proteksi data, keamanan komunikasi, pengendalian kode berbahaya, logika bisnis, *file*, keamanan API dan *web service*, dan keamanan konfigurasi. Untuk indikator status warna hijau pada tabel menunjukkan korelasi atau hubungan antara sub pertanyaan Indeks KAMI dengan BSSN No. 4 2021.

Dari tabel diatas didapatkan hasil mapping, proses ini didapat berdasarkan korelasi antara Peraturan BSSN No. 4 Tahun 2021 dengan Indeks KAMI khususnya pada domain Teknologi yang berjumlah 26 sub poin Indeks.

4.2 Desain Dokumen Rekomendasi

4.2.1 Dukungan Pengoperasian

Proses Dukungan Pengoperasian dalam tahap ini yakni Pengecekan ulang mapping antara BSSN No. 4 2021 dengan Indeks KAMI, serta membuat Dokumen Desain yang berdasarkan Standar Teknis Keamanan sebagaimana dimaksud pada pasal 26 BSSN No. 4 2021 tentang standar aplikasi web, yakni mencakup terpenuhinya: autentikasi, manajemen sesi, persyaratan kontrol akses, validasi input, kriptografi pada verifikasi statis, penanganan eror dan pencatatan log, proteksi data, keamanan komunikasi, pengendalian kode berbahaya, logika bisnis, *file*, keamanan API dan *web service*, dan keamanan konfigurasi. Dari semua standar aplikasi web pada proses di sub bab selanjutnya yakni *crosscheck* serta memfokuskan desain dokumen rekomendasi keamanan pada indeks yang sedang dalam perencanaan.

4.2.2 Evaluasi Kinerja

Dengan hasil wawancara yang prosesnya ada pada penetapan ruang lingkup dilakukan evaluasi menyeluruh yakni dengan *crosscheck* ulang seluruh pertanyaan pada indeks KAMI serta *crosscheck* ulang terkait hasil dari wawancara tersebut.

Untuk hasil dari wawancara dengan pihak TVRI Jawa Timur dapat dilihat pada tabel dibawah.

Tabel 4. 5 Hasil Survey Wawancara Indeks KAMI

#	INDEKS KAMI	Tidak dilakukan	Dalam perencanaan	Diterapkan Sebagian	Diterapkan menyeluruh
6.1	“Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?”				√
6.2	“Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?”				√
6.3	“Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?”			√	
6.4	“Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?”			√	
6.5	“Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?”				√
6.6	“Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi				√

	dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?"				
6.7	“Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?”				√
6.8	“Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?”		√		
6.9	“Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?”				√
6.10	“Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?”			√	
6.11	“Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?”		√		
6.12	“Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?”		√		
6.13	“Apakah instansi/perusahaan		√		

	anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?”				
6.14	“Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian <i>password</i> secara otomatis, termasuk menon-aktifkan <i>password</i> , mengatur kompleksitas/panjangnya dan penggunaan kembali <i>password</i> lama?”			√	
6.15	“Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?”		√		
6.16	“Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses <i>timeouts</i> , <i>lockout</i> setelah kegagalan <i>login</i> , dan penarikan akses?”		√		
6.17	“Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?”				√

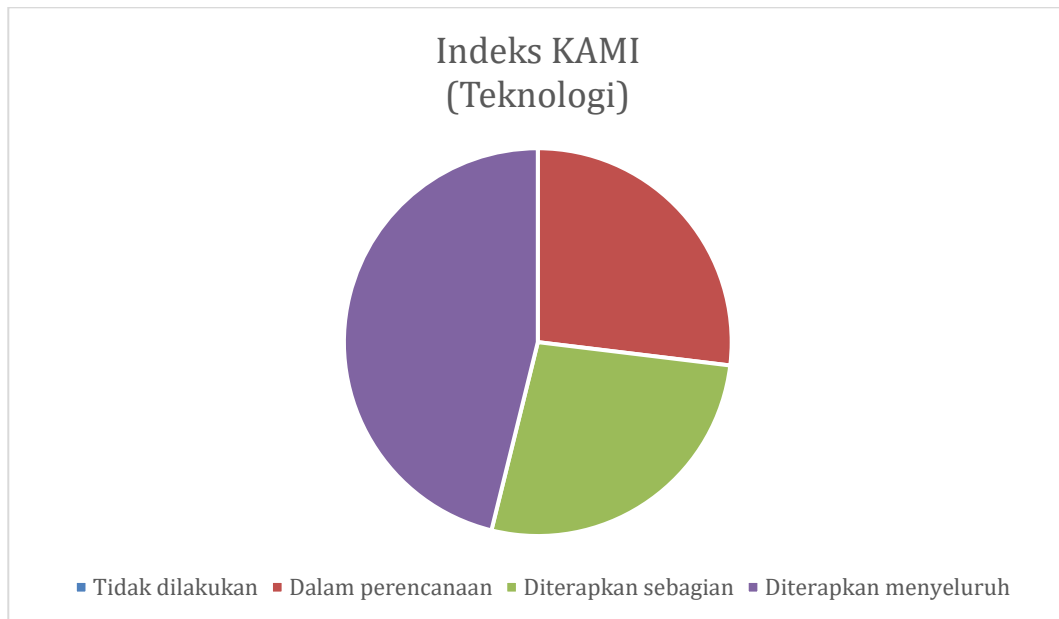
6.18	“Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?”				√
6.19	“Apakah sistem operasi untuk setiap perangkat <i>desktop</i> dan <i>server</i> dimutakhirkan dengan versi terkini?”			√	
6.20	“Apakah setiap <i>desktop</i> dan <i>server</i> dilindungi dari penyerangan virus (<i>malware</i>)?”				√
6.21	“Apakah ada rekaman dan hasil analisa (jejak audit - <i>audit trail</i>) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?”				√
6.22	“Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?”			√	
6.23	“Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?”				√
6.24	“Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?”			√	

6.25	“Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?”		√		
6.26	“Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?”				√

Untuk respon yang dapat dipilih responden untuk menjawab seluruh pertanyaan di setiap area diartikan sebagai berikut:

1. Tidak Dilakukan
2. Dalam Perencanaan
3. Diterapkan Sebagian
4. Diterapkan Secara Menyeluruh

Berdasarkan data hasil wawancara yang mengacu pada Indeks KAMI yang berjumlah 26 survey pertanyaan, pada tabel diatas didapatkan data sebagai berikut :



Gambar 4. 4 Gambar Diagram Poin Hasil Wanwancara

Dari gambar diatas dapat diketahui bahwa pada TVRI Jawa Timur dalam penerapan Teknologi Informasi utamanya dalam perihal Manajemen Keamanan sudah lebih dari setengah persyaratan dalam domain Teknologi pada Indeks KAMI sudah terpenuhi meskipun ada 7 poin yang masih dalam tahap perencanaan.

Untuk 7 poin yang sedang dalam tahap perencanaan yang akan dibuat dokumen rekomendasi keamanan yang bertujuan memberikan saran serta apa hal yang harus dilaksanakan untuk membuat instansi TVRI Jawa Timur khususnya pada Domain Teknologi kedepanya bisa menjadi lebih baik serta meningkatkan kinerja serta keamanan Manajemen Informasi yang sesuai standar yang di berikan oleh Pemerintah yakni Peraturan BSSN No. 4 Tahun 2021.

Tabel 4. 6 Rincian Hasil Wawancara Indeks KAMI

Tidak dilakukan	Dalam Perencanaan	Diterapkan Sebagian	Diterapkan Menyeluruh
	6.8	6.3	6.1
	6.11	6.4	6.2
	6.12	6.10	6.5
	6.13	6.14	6.6
	6.15	6.19	6.7

	6.16	6.22	6.9
	6.25	6.24	6.17
			6.18
			6.20
			6.21
			6.23
			6.26

- Tidak Dilakukan : 0 poin
- Dalam Perencanaan : 7 poin
- Diterapkan Sebagian : 7 poin
- Diterapkan Menyeluruh : 12 poin

4.2.3 Perbaikan Berkelanjutan

Setelah dilakukan evaluasi serta skoring maka dilakukan rekomendasi apa saja yang diperlukan untuk TVRI Jawa Timur dalam rangka meningkatkan kualitas manajemen keamanan terutama pada hal atau domain Teknologi yang berdasarkan BSSN No. 4 Tahun 2021.

Berdasarkan hasil wawancara pada pihak TVRI yang berjumlah 26 poin pertanyaan yang menjadi fokus untuk desain dokumen rekomendasi yakni 7 poin yang masih dalam tahap perencanaan pada TVRI. Untuk 7 hasil desain dokumen rekomendasi keamanan manajemen keamanan informasi serta berisi requirements kepada TVRI bertujuan perbaikan berkelanjutan sesuai sub bab disini agar menjadikan TVRI kedepanya menjadi lebih baik dalam ranah keamanan teknologi informasi dapat dilihat pada tabel 4.7 dibawah.

Tabel 4. 7 List Hasil Rekomendasi Dokumen Keamanan

No	Indeks KAMI	BSSN No. 4 2021	Requirements ke TVRI	Mapping SOP
6.8	Apakah setiap perubahan pada	26 (f) penanganan eror dan pencatatan log	- Mengatur konten pesan yang ditampilkan ketika	SOP Kontrol Akses

	sistem tercatat secara otomatis pada log?		<p>terjadi kesalahan log terjadi</p> <ul style="list-style-type: none"> - Menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani pada web TVRI - Tidak mencantumkan informasi yang dikecualikan dalam pencatatan log. 	
6.11	Sesuai kebijakan pengelolaan yang ada, apakah organisasi atau bisnis Anda menerapkan enkripsi untuk melindungi aset informasi penting?	26 (a) autentikasi	<ul style="list-style-type: none"> - Tidak mencantumkan informasi yang dikecualikan dalam pencatatan log. - Menerapkan verifikasi kata sandi pada sisi server. - Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi. 	<i>SOP Standar Autentikasi</i>
6.12	Apakah ada aturan untuk menggunakan enkripsi di organisasi atau perusahaan Anda?	26 (c) persyaratan kontrol akses	<ul style="list-style-type: none"> - Menetapkan otorisasi pengguna untuk membatasi kontrol akses pada user. - Mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus- 	<i>SOP Standar Kontrol Akses</i>

			<p>menerus pada fungsi kontrol akses.</p> <ul style="list-style-type: none"> - Mengatur antarmuka pada sisi administrator dan mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan. 	
6.13	Apakah organisasi atau bisnis Anda menggunakan sistem keamanan untuk mengawasi kunci enkripsi (termasuk e-certiff) yang digunakan, termasuk siklus penggunaannya?	26 (d) validasi input	<ul style="list-style-type: none"> - Menerapkan fungsi validasi input pada sisi server pada TVRI. - Menerapkan mekanisme penolakan input jika terjadi kesalahan validasi. - Memastikan runtime environment aplikasi tidak rentan terhadap serangan validasi input. 	<i>SOP Manajemen Sesi</i>
6.15	Apakah ada metode keamanan khusus yang digunakan untuk mengakses manajemen sistem (administrasi sistem)?	26 (a) autentikasi	<ul style="list-style-type: none"> - Tidak mencantumkan informasi yang dikecualikan dalam pencatatan log. - Menerapkan verifikasi kata sandi pada sisi server. - Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi. 	<i>SOP Standar Autentikasi</i>
6.16	Apakah sistem dan aplikasi yang digunakan sudah	26 (b) manajemen sesi	<ul style="list-style-type: none"> - Menggunakan pengendali sesi untuk proses manajemen sesi 	<i>SOP Manajemen Sesi</i>

	menerapkan pembatasan waktu akses, termasuk otomatisasi proses timeout, lockout setelah kegagalan login, dan penarikan akses?		<ul style="list-style-type: none"> - Menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi - Mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi 	
6.25	Apakah lembaga/perusahaan menerapkan lingkungan pengembangan dan pengujian yang dijamin sesuai dengan standar platform teknologi yang ada dan digunakan selama masa pakai sistem yang sedang dibangun?	26 (1) keamanan API dan web service	<ul style="list-style-type: none"> - Melakukan konfigurasi layanan website TVRI - Memverifikasi uniform resource identifier API tidak menampilkan informasi yang berpotensi sebagai celah keamanan - Membuat keputusan otorisasi dan menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid 	SOP Kontrol Akses

Tabel diatas yakni hasil list rekomendasi dokumen keamanan Manajemen Keamanan Informasi yang bertujuan kepada TVRI Jawa Timur berjumlah 7 poin yang menjadi prioritas karena masih dalam tahap perencanaan berdasarkan hasil wawancara dengan pihak TVRI Jawa Timur. Proses pembuatan dokumen rekomendasi keamanan ini sudah berdasarkan Standar dari Pemerintah yakni Pedoman Peraturan BSSN No. 4 Tahun 2021.

A. Pemetaan Kontrol BSSN No. 4 2021 dengan *Standard Operating Procedure*

Setelah dilakukan analisis secara mendalam sesuai dengan hasil rekomendasi pada prioritas dalam perencanaan. Selanjutnya yaitu melakukan pemetaan kontrol BSSN No. 4 Tahun 2021 dengan SOP yang ditunjukkan pada tabel 4.8 dibawah.

Tabel 4. 8 Pemetaan Kontrol BSSN No. 4 Dengan SOP

ID	Nama Prosedur	Kontrol BSSN No. 4 Tahun 2021
6.11	SOP Standar Autentikasi	Pasal 26 (a) fungsi autentikasi
6.15	SOP Standar Autentikasi	Pasal 26 (a) fungsi autentikasi
6.13	SOP Standar Manajemen Sesi	Pasal 26 (d) fungsi validasi input
6.16	SOP Standar Manajemen Sesi	Pasal 26 (b) fungsi manajemen sesi
6.8	SOP Standar Kontrol Akses	Pasal 26 (f) fungsi penanganan eror dan pencatatan log
6.12	SOP Standar Kontrol Akses	Pasal 26 (c) fungsi persyaratan kontrol akses
6.25	SOP Standar Kontrol Akses	Pasal 26 (l) fungsi keamanan API dan <i>web service</i>


B. *Standard Operating Procedure (SOP)*

Setelah dilakukan pemetaan control BSSN No. 4 2021 dengan SOP yang akan dibuat. Kemudian disusun pembuatan format pembuatan SOP. SOP pada gambar di bawah ini merupakan SOP Standar Autentikasi, Manajemen Sesi, Kontrol Akses yang diusulkan kepada TVRI Jawa Timur.

a. SOP Autentikasi

1. Bagian Isi SOP Autentikasi

Tabel 4. 9 Bagian SOP Autentikasi

	TVRI JAWA TIMUR Jl. Mayjen Sungkono No. 124 Surabaya	Nomor SOP	
		Tanggal Pembuatan	26 Juni 2023
		Tanggal Revisi	-
		Tanggal Pengesahan	-
		Disahkan Oleh	-
		Nama SOP	Standar Autentikasi Website
Dasar Hukum :		Kualifikasi Pelaksana :	
1. Peraturan BSSN Nomor 4 Tahun 2021		Staff IT TVRI, atau lebih tinggi	
Keterkaitan :		Peralatan/Perlengkapan :	
1. SOP Standar Autentikasi Website		1. Komputer Server	
		2. Internet	
		3. OS	
Referensi :		Pencatatan dan Pendataan :	
ISO/IEC 27001 <i>Information Security Management System</i>		1. Pencatatan password dan karakter	
		2. Pencatatan pemulihan sandi	
Peringatan :			

Pada bagian SOP Autentikasi, pemetaan didalamnya yakni pada ID 6. 11 dan 6. 15, untuk struktur konten dijelaskan pada Tabel 4.10 sebagai berikut.

Tabel 4. 10 Struktur Konten Bagian Autentikasi

Konten	Keterangan
Nama SOP	Berisi nama prosedur
Nomor SOP	Nomor SOP sesuai dengan tata naskah dinas yang berlaku di instansi
Tanggal pembuatan	Tanggal pertama kali pembuatan SOP yang berupa tanggal selesainya pembuatan SOP
Tanggal Revisi	Tanggal revisi dari SOP atau tanggal rencana di tinjau ulang
Disahkan oleh	Pengesahan SOP oleh pejabat yang bertanggung jawab
Dasar Hukum	Peraturan perundang-undangan yang mendasari pembuatan prosedur
Kualifikasi pelaksana	Penjelasan mengenai kualifikasi pelaksana yang dibutuhkan
Keterkaitan	Keterkaitan dengan dokumen lain
Referensi	Referensi isian prosedur
Peralatan/perlengkapan	Keterangan mengenai daftar perlengkapan dan peralatan yang dibutuhkan untuk melaksanakan prosedur

Pencatatan	Pencatatan dan pendataan yang diperlukan dalam pelaksanaan SOP
Peringatan	Keterangan mengenai kemungkinan apa saja yang terjadi saat SOP dilaksanakan, dan SOP tidak dilaksanakan


2. Alur Prosedur

Bagian alur prosedur berisi uraian mengenai langkah-langkah (prosedur) kegiatan beserta keterangan dokumen yang diperlukan. Untuk Tabel alur prosedur dari SOP Autentikasi selengkapnya dapat dilihat pada lampiran.

b. SOP Manajemen Sesi

1. Bagian Isi SOP Manajemen Sesi

Tabel 4. 11 Bagian SOP Manajemen Sesi

 <p>TVRI JAWA TIMUR Jl. Mayjen Sungkono No. 124 Surabaya</p>	Nomor SOP	
	Tanggal Pembuatan	26 Juni 2023
	Tanggal Revisi	-
	Tanggal Pengesahan	-
	Disahkan Oleh	-
	Nama SOP	Standar Manajemen Sesi
Dasar Hukum :	Kualifikasi Pelaksana :	
1. Peraturan BSSN Nomor 4 Tahun 2021	Staff IT TVRI, atau lebih tinggi	
Keterkaitan :	Peralatan/Perlengkapan :	
1. SOP Standar Manajemen Sesi	1. Komputer Server	
Referensi :	2. Internet	
ISO/IEC 27001 <i>Information Security Management System</i>	3. OS	
Peringatan :	Pencatatan dan Pendataan :	
	1. Pencatatan jangka waktu sesi	
	2. Pencatatan persetujuan pengguna	

Pada bagian SOP manajemen sesi, pemetaan didalamnya yakni berisi pada ID 6.13 dan 6.16, untuk struktur konten dijelaskan pada Tabel 4.13 sebagai berikut.

Tabel 4. 12 Struktur isi bagian SOP Manajemen Sesi

Konten	Keterangan
Nama SOP	Berisi nama prosedur
Nomor SOP	Nomor SOP sesuai dengan tata naskah dinas yang berlaku di instansi

Tanggal pembuatan	Tanggal pertama kali pembuatan SOP yang berupa tanggal selesainya pembuatan SOP
Tanggal Revisi	Tanggal revisi dari SOP atau tanggal rencana di tinjau ulang
Disahkan oleh	Pengesahan SOP oleh pejabat yang bertanggung jawab
Dasar Hukum	Peraturan perundang-undangan yang mendasari pembuatan prosedur
Kualifikasi pelaksana	Penjelasan mengenai kualifikasi pelaksana yang dibutuhkan
Keterkaitan	Keterkaitan dengan dokumen lain
Referensi	Referensi isian prosedur
Peralatan/perlengkapan	Keterangan mengenai daftar perlengkapan dan peralatan yang dibutuhkan untuk melaksanakan prosedur
Pencatatan	Pencatatan dan pendataan yang diperlukan dalam pelaksanaan SOP
Peringatan	Keterangan mengenai kemungkinan apa saja yang terjadi saat SOP dilaksanakan, dan SOP tidak dilaksanakan


2. Alur Prosedur

Bagian alur prosedur berisi uraian mengenai langkah-langkah (prosedur) kegiatan beserta keterangan dokumen yang diperlukan. Untuk Tabel alur prosedur dari SOP Prosedur selengkapnya dapat dilihat pada lampiran.

c. SOP Kontrol Akses

1. Bagian Isi SOP Kontrol Akses

Tabel 4. 13 Bagian SOP Kontrol Akses

 <p style="text-align: center;">TVRI JAWA TIMUR Jl. Mayjen Sungkono No. 124 Surabaya</p>	Nomor SOP	
	Tanggal Pembuatan	26 Juni 2023
	Tanggal Revisi	-
	Tanggal Pengesahan	-
	Disahkan Oleh	-
	Nama SOP	Standar Kontrol Akses Website
Dasar Hukum : 1. Peraturan BSSN Nomor 4 Tahun 2021	Kualifikasi Pelaksana : Staff IT TVRI, atau lebih tinggi	
Keterkaitan : 1. SOP Standar Kontrol Akses Website	Peralatan/Perlengkapan : 1. Komputer Server 2. Internet 3. OS	
Referensi : ISO/IEC 27001 <i>Information Security Management System</i>	Pencatatan dan Pendataan : 1. Pencataan jangka waktu sesi 2. Pencatatan validasi pencatuman session id	
Peringatan :		

Pada bagian SOP Kontrol Akses, pemetaan didalamnya yakni pada ID 6.8, 6.12 dan 6.25, untuk struktur konten dijelaskan pada Tabel 4.16 sebagai berikut.

Tabel 4. 14 Stuktur isi bagian SOP Kontrol Akses

Konten	Keterangan
Nama SOP	Berisi nama prosedur
Nomor SOP	Nomor SOP sesuai dengan tata naskah dinas yang berlaku di instansi
Tanggal pembuatan	Tanggal pertama kali pembuatan SOP yang berupa tanggal selesainya pembuatan SOP
Tanggal Revisi	Tanggal revisi dari SOP atau tanggal rencana di tinjau ulang
Disahkan oleh	Pengesahan SOP oleh pejabat yang bertanggung jawab
Dasar Hukum	Peraturan perundang-undangan yang mendasari pembuatan prosedur
Kualifikasi pelaksana	Penjelasan mengenai kualifikasi pelaksana yang dibutuhkan
Keterkaitan	Keterkaitan dengan dokumen lain

Referensi	Referensi isian prosedur
Peralatan/perlengkapan	Keterangan mengenai daftar perlengkapan dan peralatan yang dibutuhkan untuk melaksanakan prosedur
Pencatatan	Pencatatan dan pendataan yang diperlukan dalam pelaksanaan SOP
Peringatan	Keterangan mengenai kemungkinan apa saja yang terjadi saat SOP dilaksanakan, dan SOP tidak dilaksanakan

2. Alur Prosedur

Bagian alur prosedur berisi uraian mengenai langkah-langkah (prosedur) kegiatan beserta keterangan dokumen yang diperlukan. Untuk Tabel alur prosedur dari SOP Kontrol Akses selengkapnya dapat dilihat pada lampiran.



UIN SUNAN AMPEL
S U R A B A Y A

BAB V PENUTUP

5.1 Kesimpulan

Dari seluruh penjelasan diatas dapat disimpulkan bahwa penelitian ini mempunyai beberapa kesimpulan yaitu:

1. Berdasarkan hasil data wawancara yang sudah didapatkan TVRI Jawa Timur mempunyai 12 Poin Manajemen Keamanan Informasi yang sudah diterapkan menyeluruh, 7 Poin Diterapkan Sebagian, 7 Poin dalam tahap Perencanaan, serta 0 Poin Tidak Dilakukan. Dalam konteks ini menandakan bahwasanya Manajemen Keamanan Informasi pada TVRI Jawa Timur terbilang cukup, karena masih ada 7 standar keamanan yang harus dipenuhi.
2. Berdasarkan analisis pada ranah Manajemen Keamanan Informasi menggunakan Peraturan BSSN No. 4 Tahun 2021. Untuk fokus prioritas dari hasil dokumen rekomendasi Keamanan Informasi yakni pada poin yang sedang dalam tahap Perencanaan. Hasil rekomendasi keamanan diharapkan dapat membuat TVRI Jawa Timur menjadi lebih baik di masa depan.
3. Untuk output penelitian ini yakni berupa hasil rekomendasi yakni berupa *Standard Operating Procedure (SOP)* yang dilengkapi dengan alur prosedur yang berjumlah 3 *SOP*. Yakni Autentikasi, Manajemen Sesi, dan Kontrol Akses.

5.2 Saran

Pada penelitian ini mempunyai beberapa saran untuk pengembangan penelitian kedepannya yaitu sebagai berikut.

1. Pertama, penelitian harus dilakukan dengan lebih banyak responden berkualitas atau dalam posisi yang lebih tinggi sebelumnya untuk lebih memahami keadaan keamanan informasi untuk jawaban yang lebih spesifik dan pelatihan juga diharapkan untuk responden potensial membantu menyelesaikan survei.
2. Kedua, sebaiknya dokumen rekomendasi SOP yang telah dibuat untuk diuji, diimplementasikan, dan diaudit secara internal guna untuk mengetahui sejauh mana dampak terhadap keamanan informasi pada TVRI Jawa Timur. Selain itu, penelitian ini hanya sebatas pembuatan dokumen rekomendasi keamanan

berupa SOP, untuk penelitian selanjutnya mungkin dapat dilakukan evaluasi keefektifan dokumen SOP yang telah dibuat terhadap keamanan informasi TVRI Jawa Timur.



UIN SUNAN AMPEL
S U R A B A Y A

DAFTAR PUSTAKA

- Angelopoulos, S., Kitsios, F., & Papadopoulos, T. (2010). New service development in e-government: Identifying critical success factors. *Transforming Government: People, Process and Policy*, 4(1), 95–118. <https://doi.org/10.1108/17506161011028821>
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, 3, 223–234. <https://doi.org/10.54706/senastindo.v3.2021.141>
- Calder, A., & Watkins, S. (2008). *IT governance : a manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Ltd.
- Ciptanigrum Dwi, Dr. Ir. E. N. M. Si. ; D. A. S. Si. , M. T. (2015). *AUDIT KEAMANAN SISTEM INFORMASI PADA KANTOR PEMERINTAH KOTA YOGYAKARTA MENGGUNAKAN COBIT 5*.
- Damar Apri Sudarmadi. (2019). *Strategi BSSN Dalam Menghadapi Ancaman Siber di Indonesia*.
- Faturachman Husin Muh. (n.d.). *Implementasi Indeks KAMI di Universitas Sam Ratulangi*. <https://doi.org/https://doi.org/10.35793/jti.12.1.2017.17869>
- IDA BAGUS GDE PUJAASTAWA. (2016). *TEKNIK WAWANCARA DAN OBSERVASI UNTUK PENGUMPULAN BAHAN INFORMASI*.
- Iffano, R. S., & Sarno. (2009). *Sistem Manajemen Keamanan Informasi*. 26.
- Ketentuan, B. I., & Pasal, U. (n.d.). *PRES IDEN REPUBLIK INDONESIA-2*.
- Kominfo.go.id. (2017, October 4). *Badan Siber dan Sandi Negara di Bawah Komando Kemenko Polhukam*. https://www.kominfo.go.id/content/detail/10818/badan-siber-dan-sandi-negara-di-bawah-komando-kemenko-polhukam/0/sorotan_media
- Kornelia, A., & Irawan, D. (2021). Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1. In *Jurnal Pengembangan Sistem Informasi dan Informatika* (Vol. 2, Issue 2).
- PERATURAN PERUNDANG-UNDANGAN KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA. (2021). Peraturan BSSN

Nomor 4. *PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.*

- Rahayu, S. F., Prawira, D., Rusi, I., Informasi, J. S., Mipa, F., Jalan, U., & Nawawi, H. H. (2021). PENGUKURAN TINGKAT KEAMANAN INFORMASI MENGGUNAKAN METODE INDEKS KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kota Pontianak). In *Coding : Jurnal Komputer dan Aplikasi* (Vol. 09, Issue 03).
- Rizky Pratama, E., & Reza Perdanakusuma, A. (2018). *Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur)* (Vol. 2, Issue 11). <http://j-ptiik.ub.ac.id>
- RPM Pusat Koordnasi Penanganan Insiden Keamanan Informasi Pemerintah. (n.d.).
- Schneider, F., Maurer, C., & Friedberg, R. C. (2017). International organization for standardization (ISO) 15189. In *Annals of Laboratory Medicine* (Vol. 37, Issue 5, pp. 365–370). Seoul National University, Institute for Cognitive Science. <https://doi.org/10.3343/alm.2017.37.5.365>
- Setiaji, B., & Widiarti, U. D. (n.d.). *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA) SISTEM INFORMASI MANAJEMEN PROYEK DI PT. PANORAMA GRAHA ASRI.*
- Sheikhpour, R., & Modiri, N. (2012). An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls. In *Article in International Journal of Security and its Applications* (Vol. 6, Issue 2). <https://www.researchgate.net/publication/292833500>
- Sutabri, T. (2012). *Analisis Sistem Informasi Yogyakarta: CV. Andi Offset.* 1.
- Whitman, R. L., & Rahman, A. A. (n.d.). *Research and Practice Code Metrics For Predicting Risk Levels of Android Applications.* <http://digitalcommons.kennesaw.edu/ccerp/2016/Student/>