



UNIVERSITAS
Dinamika

**AUDIT KEAMANAN SISTEM INFORMASI PADA DINAS KOMUNIKASI
DAN INFORMATIKA KOTA MOJOKERTO BERDASARKAN STANDAR
ISO 27001:2013**

LAPORAN TUGAS AKHIR



**Program Studi
S1 Sistem Informasi**

Oleh:

APRIENE SHALSABILA

18410100076

UNIVERSITAS
Dinamika

FAKULTAS TEKNOLOGI DAN INFORMATIKA

UNIVERSITAS DINAMIKA

2024

**AUDIT KEAMANAN SISTEM INFORMASI PADA DINAS KOMUNIKASI
DAN INFORMATIKA KOTA MOJOKERTO BERDASARKAN STANDAR
ISO 27001:2013**

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk menyelesaikan
Program Sarjana Komputer



UNIVERSITAS
Dinamika

Oleh:

Nama : APRIENE SHALSABILA
NIM : 18410100076
Program Studi : S1 (Strata Satu)

**FAKULTAS TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS DINAMIKA**

2024

Tugas Akhir

AUDIT KEAMANAN SISTEM INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA MOJOKERTO BERDASARKAN STANDAR ISO 27001:2013

Dipersiapkan dan disusun oleh

Apriene Shasabila

NIM: 18410100076

Telah diperiksa, diuji, dan disetujui oleh Dewan Pembahas

Pada :

Susunan Dewan Pembahas

Pembimbing:

I. Slamet M,T.

NIDN: 0701127503


Digitally signed
by Slamet A.
Date:
2024.08.20
09:37:55 +0700'

II. Rudi Santoso, S.Sos., M.M.

NIDN: 0717107501


Digitally signed
by Rudi Santoso
Date:
2024.08.20
10:07:43 +0700'

Pembahas:

Dr. Haryanto Tanuwijaya, S.Kom., M.MT.


NIDN: 0710036602


Digitally signed by
Haryanto Tanuwijaya
DN: cn=Haryanto
Tanuwijaya,
o=Universitas
Dinamika, ou,
email=haryanto@dina
mika.ac.id, c=ID
Date: 2024.08.21
16:58:16 +0700'

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana

Dr. Anjik Sukmaaji, S.Kom., M.Eng.

NIDN: 0731057301


Digitally signed by Anjik
Sukmaaji
Date: 2024.08.23 08:36:03
+07'00'

Dekan Fakultas Teknologi dan Informatika

UNIVERSITAS DINAMIKA



UNIVERSITAS
“Belajar untuk hidup, hidup untuk belajar”

Dinamika

PERNYATAAN
PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa **Universitas Dinamika**, Saya :

Nama : **Apriene Shalsabila**
NIM : **18410100076**
Program Studi : **S1 Sistem Informasi**
Fakultas : **Fakultas Teknologi dan Informatika**
Jenis Karya : **Tugas Akhir**
Judul Karya : **AUDIT KEAMANAN SISTEM INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA MOJOKERTO BERDASARKAN STANDAR ISO 27001:2013**

Menyatakan dengan sesungguhnya bahwa :

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, Saya menyetujui memberikan kepada **Universitas Dinamika** Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalty Free Right*) atas seluruh isi/sebagian karya ilmiah Saya tersebut diatas untuk disimpan, dialihmediakan, dan dikelola dalam bentuk pangkalan data (*database*) untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama Saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.
2. Karya tersebut diatas adalah hasil karya asli Saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya, atau pendapat orang lain yang ada dalam karya ilmiah ini semata-mata hanya sebagai rujukan yang dicantumkan dalam Daftar Pustaka Saya.
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiasi pada karya ilmiah ini, maka Saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada Saya.

Surabaya, 09 Juli 2024


Apriene Shalsabila
NIM : **18410100076**

ABSTRAK

Dinas Komunikasi dan Informatika (Diskominfo) Kota Mojokerto sering menghadapi kendala sistem informasi pada website atau gate utama yang tidak dapat diakses, menyebabkan gangguan dalam layanan publik dan pengelolaan informasi yang kurang efektif. Penelitian ini bertujuan untuk mengevaluasi apakah penerapan Sistem Manajemen Keamanan Informasi (SMKI) pada Diskominfo Kota Mojokerto sudah sesuai dengan standar ISO 27001:2013. Metode penelitian mengacu pada kerangka kerja ISO 27001:2013, yang mencakup identifikasi risiko, penilaian keamanan, dan implementasi kontrol keamanan yang tepat. Hasil penelitian ini menghasilkan rekomendasi untuk pengembangan kebijakan, prosedur, formulir, dan instruksi kerja guna memperkuat keamanan sistem informasi yang ada. Harapan dari penelitian ini adalah meningkatkan kesadaran akan pentingnya keamanan informasi di Diskominfo Kota Mojokerto berdasarkan standar ISO 27001:2013 yang telah menjadi acuan selama penelitian. Upaya berkelanjutan dianjurkan untuk memantau dan mengevaluasi implementasi SMKI dengan memperhatikan perkembangan standar dan teknologi keamanan informasi yang relevan pada saat ini dan di masa yang akan datang.

Kata kunci: Diskominfo, Keamanan informasi, ISO/IEC 27001:2013

KATA PENGANTAR

Puji syukur selalu terpanjatkan kehadirat Allah S.W.T atas berkah dan hidayah-Nya sehingga penulis dapat menyelesaikan Laporan Tugas Akhir ini yang berjudul “Audit Keamanan Sistem Informasi Pada Dinas Komunikasi Dan Informatika Kota Mojokerto Berdasarkan Standar Iso 27001:2013”. Laporan Tugas Akhir ini merupakan salah satu syarat yang harus dipenuhi oleh setiap mahasiswa dalam menyelesaikan program studi strata satu di Universitas Dinamika Surabaya.

Penulisan laporan ini dapat dilaksanakan dengan baik berkat dukungan dari beberapa pihak. Oleh karena itu, pada kesempatan kali ini, saya ingin mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. Budi Jatmiko, M.Pd. selaku Rektor Universitas Dinamika.
2. Bapak Dr. Anjik Sukmaaji, S.Kom., M.Eng. selaku Dekan Fakultas Teknologi Informatika Universitas Dinamika.
3. Bapak Julianto Lemantara S.Kom. M.Eng selaku Ketua Program Studi S1 Sistem Informasi.
4. Bapak Slamet M,T. dan Bapak Rudi Santoso, S.Sos., M.M selaku dosen pembimbing yang telah memberikan bimbingan, motivasi, dan ilmu kepada penulis.
5. Bapak Haryanto Tanuwijaya S.Kom selaku dosen pembahas pada Tugas Akhir ini.
6. Keluarga Cenayank, Alifah, Adis, Bunda, Pace terutama Sasha dan Oya yang selalu mau menemani disaat susah.
7. Keluarga pasukan Huha, Caca dan Irvana yang selalu menyempatkan waktu untuk quality time bersama.
8. Jajaran *staff* akademik Universitas Dinamika Surabaya khususnya PPTA.

Serta kepada seluruh pihak yang telah membantu dalam penelitian serta dalam penyusunan laporan ini yang tidak dapat disebutkan satu persatu, semoga Allah S.W.T membalas seluruh kebaikan yang kalian lakukan kepada penulis sehingga laporan ini dapat terselesaikan. Penulis menyadari bahwa di dalam laporan ini masih banyak kesalahan dan kekurangan. Oleh karena itu saya memohon maaf dan selalu mengharapkan kritik dan saran yang membangun dari semua pihak. Semoga

laporan ini dapat bermanfaat bagi yang membutuhkan, atas perhatiannya terima kasih.

Surabaya, 10 Juli 2024

Penulis



UNIVERSITAS
Dinamika

DAFTAR ISI

	Halaman
ABSTRAK	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	4
1.4 Tujuan	4
1.5 Manfaat	5
BAB II LANDASAN TEORI	6
2.1 Penelitian Sebelumnya.....	6
2.2 Audit	6
2.3 Audit Sistem Informasi	7
2.3.1 Audit Keamanan Sistem Informasi	7
2.4 Sistem Informasi.....	8
2.5 Keamanan Sistem Informasi.....	8
2.7 Sistem Manajemen Keamanan Informasi (SMKI)	9
2.8 Standar Sistem Manajemen Keamanan Informasi IEC/ISO 27000.....	10
2.9 ISO 27001	11
2.9.1 ISO 27001:2013	11
2.9.2 Struktur ISO 27001:2013	12

2.10 Metode P-D-C-A	13
2.11 Penilaian Risiko (<i>Risk Assessment</i>)	13
2.12 SSE-CMM (<i>System Security Engineering Capability Maturity Model</i>).....	18
BAB III METODE PENELITIAN	21
3.1 Tahap Awal.....	22
3.1.1 Studi Literatur	22
3.1.2 Identifikasi dan Analisis Permasalahan.....	22
3.2 Tahap Pengembangan (Pelaksanaan Audit).....	23
3.2.1 Tahapan <i>Plan</i>	23
3.2.2 Tahapan <i>Do</i>	24
3.2.3 Tahapan <i>Check</i>	25
3.2.4 Tahapan <i>Act</i>	26
3.3 Tahap Akhir	26
BAB IV HASIL DAN PEMBAHASAN.....	28
4.1 Tahapan Awal	28
4.1.1 Studi Literatur	28
4.2.1 Identifikasi dan Analisis Masalah	28
4.2.2. Dokumen Permasalahan yang Teridentifikasi	30
4.2 Tahapan Pengembangan (Pelaksanaan Audit).....	30
4.1.1 Tahapan <i>Plan</i>	30
4.1.2 Tahapan <i>Do</i>	32
4.1.3 Tahapan <i>Check</i>	40
4.1.4 Tahapan <i>Act</i>	43
BAB V KESIMPULAN DAN SARAN.....	49
5.1 Kesimpulan.....	49
5.2 Saran.....	49

DAFTAR PUSTAKA	51
LAMPIRAN.....	53



UNIVERSITAS
Dinamika

DAFTAR GAMBAR

	Halaman
Gambar 2. 1 Tiga Pilar Keamanan Informasi (Arnason & Willet, 2008)	9
Gambar 3. 1 Metode Penelitian	21
Gambar 4. 1 Hasil Perencanaan Kebijakan.....	46
Gambar 4. 2 Hasil Perencanaan Prosedur	46
Gambar 4. 3 Hasil Perencanaan Kebijakan	47
Gambar 4. 4 Hasil Perencanaan Rekam Kerja	47



UNIVERSITAS
Dinamika

DAFTAR TABEL

	Halaman
Tabel 2. 1 Penilaian Aset Menurut Aspek Kerahasiaan (<i>Confidentiality</i>).....	14
Tabel 2. 2 Penilaian Aset Menurut Aspek Keutuhan (<i>Integrity</i>).....	14
Tabel 2. 3 Penilaian Aset Menurut Aspek Ketersediaan (<i>Availability</i>).....	15
Tabel 2. 4 Jenis dan Contoh Ancaman.....	15
Tabel 2. 5 Contoh Daftar Kelemahan.....	16
Tabel 2. 6 Nilai Rerata Probabilitas.....	16
Tabel 2. 7 Skala <i>Business Impact Analysis</i> (BIA).....	17
Tabel 2. 8 Matriks Level Risiko.....	18
Tabel 2. 9 <i>Capability</i> Level SSE-CMM.....	20
Tabel 3. 1 Tingkat Kemampuan SSE-CMM.....	25
Tabel 4. 1 Nilai Aset Dari Sisi Kerahasiaan (<i>Confidentiality</i>).....	32
Tabel 4. 2 Nilai Aset Dari Sisi Keutuhan (<i>Integrity</i>).....	32
Tabel 4. 3 Nilai Aset Dari Sisi Ketersediaan (<i>Availability</i>).....	32
Tabel 4. 4 Analisis Penilaian Aset.....	33
Tabel 4. 5 Identifikasi Kelemahan dan Ancaman Pada Aset.....	34
Tabel 4. 6 Tabel Nilai Rerata Probabilitas.....	34
Tabel 4. 7 Identifikasi Nilai Ancaman Pada Aset Data Aplikasi.....	36
Tabel 4. 8 Tabel Skala <i>Business Impact Analysis</i> (BIA).....	36
Tabel 4. 9 Pemberian Nilai <i>Business Impact Analysis</i> (BIA).....	37
Tabel 4. 10 Tabel Matriks Level Risiko.....	38
Tabel 4. 11 Hasil Nilai Dampak Bisnis Aset Diskominfo.....	38
Tabel 4. 12 Nilai Risiko Dan Level Risiko Aset.....	40
Tabel 4. 13 Level Tingkatan SSE-CMM.....	42
Tabel 4. 14 Penilaian Klausul Menggunakan SSE-CMM Klausul 9.....	42
Tabel 4. 15 Pemetaan Hasil Rekomendasi (Klausul 9: Pengendalian Hak Akses).....	44
Tabel 4. 16 Penyusunan Rangkaian SOP Pada Klausul 9.....	44

DAFTAR LAMPIRAN

	Halaman
Lampiran L1. 1 Surat Izin Penelitian	53
Lampiran L2. 1 Hasil Wawancara dan Observasi Ke-1	54
Lampiran L2. 2 Hasil Wawancara dan Observasi Ke-2.....	56
Lampiran L3. 1 Perbandingan Lima Standar Keamanan Informasi	58
Lampiran L3. 2 Klausul Pada ISO 27001:2013	60
Lampiran L4. 1 Struktur Jabatan Diskominfo Kota Mojokerto	63
Lampiran L4. 2 Detail Pegawai Diskominfo Kota Mojokerto.....	64
Lampiran L5.1 Proses Bisnis Diskominfo Kota Mojokerto	67
Lampiran L6. 1 Daftar Kejadian Insiden Keamanan Sistem Informasi	68
Lampiran L7. 1 Pemetaan Permasalahan dan Dampak	69
Lampiran L8. 1 Daftar Aset Utama Diskominfo Kota Mojokerto	70
Lampiran L8. 2 Daftar Aset Pendukung Diskominfo Kota Mojokerto	71
Lampiran L8. 3 Daftar Aset Kritis Diskominfo Kota Mojokerto	72
Lampiran L8. 4 Analisis Nilai Aset	73
Lampiran L8. 5 Identifikasi Kelemahan Dan Ancaman Pada Aset.....	74
Lampiran L8. 6 Nilai Ancaman Aset Data Aplikasi	75
Lampiran L8. 7 Nilai Ancaman Aset Data Informasi Publik.....	75
Lampiran L8. 8 Nilai Ancaman Aset <i>Windows Ultimate</i>	76
Lampiran L8. 9 Nilai Ancaman Aplikasi PPID	76
Lampiran L8. 10 Nilai Ancaman Aset Aplikasi <i>Website</i> Pemkot	77
Lampiran L8. 11 Nilai Ancaman Aset PC Unit	77
Lampiran L8. 12 Nilai Ancaman Aset Server.....	78
Lampiran L8. 13 Nilai Ancaman Aset Switch	78
Lampiran L8. 14 Nilai Ancaman Aset Router	79
Lampiran L8. 15 Nilai Ancaman Aset Firewall.....	79
Lampiran L8. 16 Nilai <i>Business Impact Analysis</i> Aset Diskominfo	80
Lampiran L8. 17 Hasil Penilaian Nilai Dampak Bisnis (<i>Impact</i>)	88
Lampiran L8. 18 Hasil Identifikasi Nilai Risiko Dan Level Risiko	88
Lampiran L8. 19 Pemetaan Klausul Pada ISO 27001:2013	89

Lampiran L8. 20 Tabel Pemilihan Klausul ISO 27001:2013	91
Lampiran L8. 21 Tabel Klausul 7 Keamanan Sumber Daya Manusia.....	93
Lampiran L8. 22 Tabel Klausul 9 Kontrol Akses	93
Lampiran L8. 23 Tabel Klausul 11 Keamanan Fisik Dan Lingkungan	94
Lampiran L8. 24 Penilaian Tingkat Kematangan Pada Klausul 7	94
Lampiran L8. 25 Grafik Tingkat Kematangan Level Klausul 7.....	97
Lampiran L8. 26 Penilaian Tingkat Kematangan Pada Klausul 9	97
Lampiran L8. 27 Grafik Tingkat Kematangan Level Klausul 9.....	100
Lampiran L8. 28 Penilaian Tingkat Kematangan Pada Klausul 11	101
Lampiran L8. 29 Grafik Tingkat Kematangan Level Klausul 11.....	105
Lampiran L9. 1 Hasil Penelusuran Bukti dan Gap.....	106
Lampiran L10.1 Pemetaan Rekomendasi Klausul ISO 27001:2013.....	117
Lampiran L11. 1 Pengelompokan Risiko.....	123
Lampiran L11. 2 Pengelompokan Kebijakan.....	124
Lampiran L12. 1 KB 01 - Klausul 7 Keamanan Sumber Daya Manusia	125
Lampiran L12. 2 KB 02 - Klausul 9 Pengaturan Hak Akses	127
Lampiran L12. 3 KB 03 - Klausul 11 Keamanan Fisik Dan Lingkungan.....	129
Lampiran L13. 1 PO 01 - Pelatihan dan Pengembangan SDM.....	131
Lampiran L13. 2 PO 02 - Prosedur Pengelolaan Hak Akses	136
Lampiran L13. 3 PO 03 - Prosedur Manajemen Kata Sandi.....	148
Lampiran L13. 4 PO 04 - Perawatan Perangkat Keras.....	160
Lampiran L14. 1 IK 01 - Pengelolaan Hak Akses.....	167
Lampiran L14. 2 IK 02 - Instruksi Kerja Manajemen Kata Sandi	169
Lampiran L14. 3 IK 03 - Pengaturan Ulang Kata Sandi	172
Lampiran L14. 4 IK 04 - Pengelolaan Perangkat Keras.....	173
Lampiran L14. 5 IK 05 - Pelatihan Pengembangan SDM.....	175
Lampiran L15. 1 FM 01 - Formulir Verifikasi Latar Belakang Pegawai.....	177
Lampiran L15. 2 FM 02 - <i>Non-Disclosure Agreement</i> (NDA)	179
Lampiran L15. 3 FM 03 - Formulir Pengelolaan Hak Akses.....	182
Lampiran L15. 4 FM 04 - Formulir Log Hak Akses Sistem.....	183

Lampiran L15. 5 FM 05 - Formulir Log Hak Akses Fisik.....	185
Lampiran L15. 6 FM 06 - Formulir Pelaporan Insiden Fisik.....	187
Lampiran L15. 7 FM 07 - Formulir Pemeliharaan Perangkat IT.....	188
Lampiran L15. 8 FM 08 - Formulir Pengaturan Ulang Kata Sandi.....	189
Lampiran L15. 9 FM 09 - Pemeliharaan Perangkat Keras.....	190
Lampiran L15. 10 FM 10 - Pengaduan Kerusakan Perangkat Keras.....	191
Lampiran L15. 11 FM 11 - Kehadiran Pelatihan Pegawai.....	192
Lampiran L15. 12 FM 12 - Formulir Evaluasi Pelatihan.....	193
Lampiran L15. 13 FM 13 - Formulir Perbaikan Sistem.....	195
Lampiran L16. 1 Kondisi Ruangan Bagian Aplikasi Dan Infrastruktur.....	196
Lampiran L16. 2 Kondisi Koridor Diskominfo Kota Mojokerto.....	197
Lampiran L16. 3 Kondisi Tangga Darurat Diskominfo Kota Mojokerto.....	198
Lampiran L16. 4 Kondisi Ruang Depan Diskominfo Kota Mojokerto.....	199
Lampiran L16. 5 Kondisi Ruang Pelayanan Diskominfo Kota Mojokerto.....	200
Lampiran L16. 6 Kondisi Pintu Utama Diskominfo Kota Mojokerto.....	201
Lampiran L16. 7 <i>Campaign</i> Keamanan Informasi.....	202
Lampiran L16. 8 Halaman Depan Buku Tamu Diskominfo Kota Mojokerto.....	203
Lampiran L16. 9 Isi Buku Tamu Diskominfo Kota Mojokerto.....	203
Lampiran L16. 10 Hasil Penentuan Level Kematangan Klausul 7.....	205
Lampiran L16. 11 Hasil Penentuan Level Kematangan Klausul 7.....	206
Lampiran L16. 12 Hasil Penentuan Level Kematangan Klausul 9.....	207
Lampiran L16. 13 Hasil Penentuan Level Kematangan Klausul 9.....	208
Lampiran L16. 14 Hasil Penentuan Level Kematangan Klausul 11.....	209
Lampiran L16. 15 Hasil Penentuan Level Kematangan Klausul 11.....	210
Lampiran L17. 1 Bukti Plagiasi.....	211
Lampiran L18. 1 Kartu Bimbingan.....	212
Lampiran L19. 1 Biodata Penulis.....	213

BAB I

PENDAHULUAN

1.1 Latar Belakang

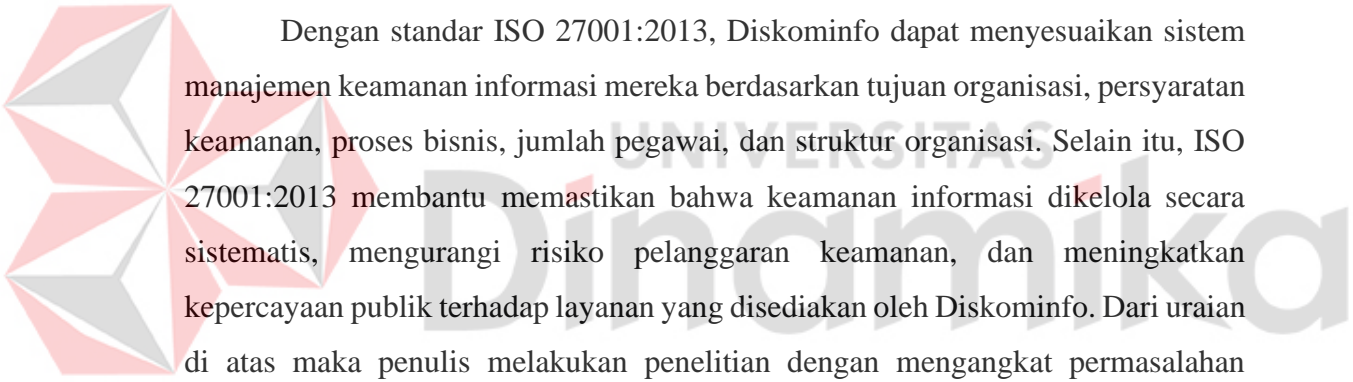
Dinas Komunikasi dan Informatika Kota Mojokerto merupakan salah satu instansi yang berada dalam lingkup pemerintahan Kota Mojokerto. Berdasarkan Peraturan Daerah Kota Mojokerto Nomor 8 Tahun 2016 Tentang Pembentukan Perangkat Daerah Kota Mojokerto, Dinas Komunikasi dan Informatika Kota Mojokerto merupakan Dinas tipe B yang menyelenggarakan urusan pemerintahan bidang komunikasi dan informatika, urusan pemerintahan bidang persandian dan urusan pemerintahan bidang statistik. Tujuan Dinas Kominfo sendiri yaitu meningkatkan kualitas Pelayanan Publik terutama yang berbasis Teknologi Informasi di Kota Mojokerto. Berdasarkan dokumen rencana strategis Dinas Komunikasi dan Informatika Kota Mojokerto tahun 2019-2023, Dinas Kominfo Kota Mojokerto memiliki fungsi untuk mengelola pelayanan aplikasi pemerintah dan layanan publik serta tata laksana *e-government* di lingkup Pemerintahan Kota Mojokerto. Selain itu, Dinas Kominfo Kota Mojokerto juga memiliki tugas untuk menyediakan infrastruktur teknologi informasi bagi dinas-dinas lain yang berada di wilayah Kota Mojokerto, dan pelaksanaan kerja sama program *e-government* dengan lembaga pemerintah dan atau lembaga swasta. Adapun kurang lebih 15 sistem informasi Organisasi Perangkat Daerah (OPD) yang berada dalam kendali Diskominfo Kota Mojokerto.

Banyaknya data ataupun aset informasi yang disimpan oleh Dinas Kominfo Kota Mojokerto membuat begitu pentingnya untuk menjaga dan memperhatikan keamanan sistem informasi baik dari sisi ancaman (*Threat*) dan kelemahan (*Vulnerable*) dalam satu bulan, Dinas Kominfo Kota Mojokerto menerima ratusan email spam yang mencoba mengakses sistem, mengganggu layanan publik, dan mengancam integritas data. Sementara untuk kelemahan (*Vulnerable*) yaitu kurangnya SDM yang mengikuti bimtek TIK dan adanya beberapa sarana dan prasarana yang rusak dan perlu diganti. Keamanan informasi juga dapat diartikan sebagai proteksi untuk informasi termasuk juga pada sistem dan perangkat keras yang menaungi dan menjalankan sistem informasi tersebut (Whitman & Herbert,

2014). Hal tersebut sangat erat kaitannya dengankualitas dan tingkat kepercayaan masyarakat pengguna layanan tersebut. Aspek tersebut harus sangat diawasi mengingat kinerja tata kelola sistem akan berdampak pada *Business Impact Analysis Is* (BIA) terlebih apabila mengenai masalah keamanan yang berhubungan dengan kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) sebuah data.

Dari hasil observasi dan juga wawancara ditemui kondisi yang saat ini masih menjadi kekurangan dalam penanganan teknologi informasi di antaranya dari sisi kerahasiaan (*Confidentiality*) dimana belum adanya kebijakan mengenai pengelolaan kata sandi untuk penggunaan sistem informasi yang ada pada Diskominfo sehingga data atau informasi menjadi terancam untuk diakses oleh orang tidak berwenang. Dari sisi keutuhan (*Integrity*) yaitu adanya *platform* OPD yang berasal dari pihak ketiga sehingga sering terjadinya perubahan data ataupun informasi tanpa sepengetahuan Diskominfo selaku penyedia SPBE (Sistem Informasi Berbasis Elektronik) di Kota Mojokerto. Dari sisi ketersediaan (*Availability*) yaitu masih sering terjadinya *server down* pada Diskominfo Kota Mojokerto terutama ketika terdapat acara besar dikarenakan kapasitas sumber daya seperti CPU, RAM, dan bandwidth yang terbatas, sehingga tidak mampu untuk memproses permintaan dalam jumlah besar secara bersamaan. Ketika sumber daya ini mencapai batas maksimal, server menjadi tidak responsif atau down. Selain itu pernah terjadinya insiden peretasan *website* Kota Mojokerto pada tahun 2016. Peretasan tersebut mengakibatkan perubahan tampilan *website* Pemkot Mojokerto dipenuhi dengan berbagai informasi perihal kritikan rekening gendut tiga pegawai di Bagian Umum Pemkot Mojokerto dan juga peretas mencantumkan nama wali kota serta sekretaris daerah sehingga dari peristiwa tersebut mengakibatkan *website* dari Pemkot Kota Mojokerto tidak dapat diakses dalam kurun waktu 24 jam (Zen, 2016). Adapun permasalahan mengenai pengelolaan teknologi informasi lainnya yang ditemui ialah adanya kendala pengintegrasian aplikasi yang ada di SKPD karena perbedaan *platform* program aplikasi yang dimiliki OPD dikarenakan Belum terpenuhinya kebutuhan *programmer*, Belum terintegrasinya *database* dan layanan *e-government* instansi pemerintah pusat dan daerah sehingga dari hasil pencapaian kinerja pelayanan Dinas Komunikasi dan Informatika Kota Mojokerto masih

ditemui kesenjangan antara target dan realisasi kinerja. Dengan demikian mengingat begitu pentingnya keamanan informasi maka diperlukannya kegiatan audit untuk mengetahui bagaimana kebijakan keamanan sistem informasi yang selama ini diterapkan oleh Dinas Kominfo Kota Mojokerto dan apakah dari kebijakan tersebut sudah sesuai dengan Standar SMKI ISO 27001: 2013. Dengan adanya audit sebuah organisasi juga dapat menerima serangkaian informasi yang dapat membantu organisasi tersebut mengelola risiko dan sumber daya TI yang lebih efisien sehingga diharapkan tujuan TI dan Tujuan bisnis dapat tercapai (Gantz, 2014). Sementara untuk menunjang proses bisnis yang lebih baik dari hasil temuan audit akan diberikannya sebuah rekomendasi meliputi Standar Operasional Prosedur (SOP), instruksi kerja dan rekaman kerja untuk memastikan bahwa dari hasil rekomendasi yang dihasilkan dapat diimplementasikan oleh Dinas Kominfo Kota Mojokerto.



Dengan standar ISO 27001:2013, Diskominfo dapat menyesuaikan sistem manajemen keamanan informasi mereka berdasarkan tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai, dan struktur organisasi. Selain itu, ISO 27001:2013 membantu memastikan bahwa keamanan informasi dikelola secara sistematis, mengurangi risiko pelanggaran keamanan, dan meningkatkan kepercayaan publik terhadap layanan yang disediakan oleh Diskominfo. Dari uraian di atas maka penulis melakukan penelitian dengan mengangkat permasalahan tersebut. Adapun judul yang digunakan pada penelitian ini yaitu “Audit Keamanan Sistem Informasi pada Dinas Komunikasi dan Informatika Kota Mojokerto berdasarkan Standar ISO 27001: 2013”

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas maka didapat rumusan masalah sebagai berikut:

1. Bagaimana tingkat keamanan sistem informasi pada Dinas Kominfo Kota Mojokerto berdasarkan hasil audit, dan apa saja temuan terkait kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) data?
2. Bagaimana upaya yang dapat dilakukan untuk mengatasi kendala keamanan sistem teknologi informasi di Dinas Kominfo Kota Mojokerto agar sesuai dengan standar keamanan informasi ISO 27001:2013?

3. Bagaimana cara efektif untuk mengatasi risiko yang dihadapi dalam pengelolaan keamanan informasi di Dinas Kominfo Kota Mojokerto agar sesuai standar ISO 27001:2013?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Penelitian mengacu berdasarkan standar ISO/IEC 27001:2013
2. Objek penelitian merupakan sistem informasi website portal pada bagian Aplikasi dan Infrastruktur Informasi Dinas Kominfo Kota Mojokerto
3. Data yang diperoleh untuk dianalisis diperoleh dari studi literatur dan studi lapangan berupa observasi, wawancara, dokumen Rencana Kerja tahun 2019-2022, Dokumen SOP.
4. Terdapat 3 Klausul ISO 27001:2013 yang digunakan pada penelitian ini yaitu Klausul 7 (Keamanan Sumber Daya Manusia), Klausul 9 (Manajemen Kontrol Akses) dan Klausul 11 (Keamanan Fisik dan Lingkungan).
5. Langkah-langkah pelaksanaan audit pada penelitian ini menggunakan siklus *Plan-Do-Check-Act* (PDCA) berdasarkan standar ISO/IEC 27001:2013.
6. Menggunakan skala pengukuran kematangan (*maturity level*) berdasarkan SSE-CMM (*System Security Engineering Capability Maturity Model*)

1.4 Tujuan

Tujuan dari penelitian ini antara lain:

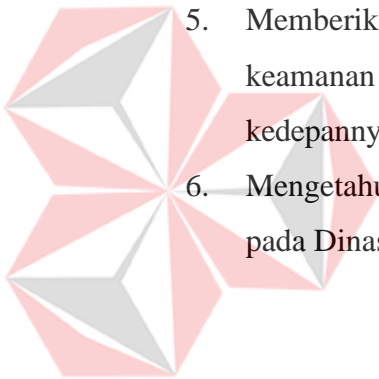
1. Untuk mengevaluasi tingkat keamanan sistem informasi pada Dinas Kominfo Kota Mojokerto dengan mengacu pada hasil audit, serta mengidentifikasi temuan terkait kerahasiaan, keutuhan, dan ketersediaan data.
2. Untuk merumuskan langkah-langkah perbaikan guna mengatasi kendala yang ada, sehingga sistem teknologi informasi dapat memenuhi standar keamanan informasi ISO 27001:2013.
3. Untuk mengidentifikasi risiko yang dihadapi dalam pengelolaan keamanan informasi di Dinas Kominfo Kota Mojokerto. Penelitian ini akan merumuskan cara-cara efektif untuk mengatasi risiko tersebut agar sesuai dengan standar

ISO 27001:2013, guna meningkatkan pengelolaan dan perlindungan data serta sistem informasi.

1.5 Manfaat

Adapun yang menjadi manfaat penelitian ini yaitu:

1. Mengetahui sistem manajemen keamanan sistem informasi berdasarkan standar ISO 27001:2013.
2. Membantu instansi dalam hal pengawasan manajemen keamanan sistem informasi yang berjalan.
3. Memahami kondisi dari instansi dari sisi sistem manajemen keamanan sistem informasi.
4. Meningkatkan sistem manajemen keamanan informasi untuk efektifitas sistem dan pelayanan Dinas Kominfo Kota Mojokerto kepada masyarakat.
5. Memberikan rekomendasi dan masukan sebagai acuan pengembangan keamanan sistem informasi Dinas Kominfo Kota Mojokerto untuk kedepannya.
6. Mengetahui tingkat kematangan keamanan sistem informasi (*Maturity Level*) pada Dinas Kominfo Kota Mojokerto.



BAB II

LANDASAN TEORI

2.1 Penelitian Sebelumnya

ISO 27001 dengan judul penelitian Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5 (Winarno & Amborowati, 2017), dimana tujuan penelitian ini adalah untuk membuat tata kelola keamanan informasi sesuai dengan persyaratan SMKI ISO 27001:2013 dan kerangka kerja keamanan informasi COBIT 5. Perbedaan penelitian yang penulis lakukan dibanding penelitian sebelumnya adalah penelitian ini memberikan saran dan rekomendasi berdasarkan permasalahan yang ditemui dari objek penelitian, sedangkan penelitian sebelumnya tidak memberikan saran dan rekomendasi.

Selanjutnya penelitian dengan judul Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA Dan ISO 27001 Pada Organisasi XYZ (Budiarto, 2017). Dengan tujuan mengidentifikasi gangguan keamanan yang kemungkinan terjadi pada perusahaan XYZ, kemudian akan memberikan saran-saran dan rekomendasi yang sesuai untuk menjaga keamanan pada perusahaan tersebut. Kelebihan penelitian yang penulis lakukan adalah penelitian ini menerapkan klausul khusus yang digunakan agar hasil audit dapat lebih spesifik, sedangkan yang penelitian sebelumnya tidak menyertakan berapa jumlah klausul yang digunakan

2.2 Audit

Audit merupakan sebuah proses pengumpulan serta pemeriksaan bukti mengenai informasi guna menentukan dan membuat laporan terkait tingkat kesesuaian antara informasi dan kriteria yang ditetapkan (Arens *et al.*, 2014). Dapat juga diartikan sebagai pemeriksaan.

Proses audit dilakukan secara mandiri, sistematis, dan terdokumentasi dengan baik guna memperoleh bukti audit tersebut. Kemudian, dievaluasi secara objektif untuk melihat sejauh mana kriteria audit terpenuhi. Adapun tujuan audit ialah untuk memeriksa kesesuaian kebijakan, prosedur, dan proses dengan standar

serta untuk menganalisis adanya kelemahan ataupun risiko awal suatu organisasi, dan menilai standar atau kinerja organisasi.

2.3 Audit Sistem Informasi

Menurut (Weber, 1999) Audit sistem informasi merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah dari sistem komputer yang ada sudah dapat mengamankan aset yang berhubungan dengan sistem informasi mencakup perangkat keras (*hardware*), perangkat lunak (*Software*), Manusia (*human*), *file*, data, dan perangkat pendukung lainnya, kemudian dapat memelihara integritas data, dan apakah sudah dapat mendorong tercapainya tujuan organisasi secara efektif menggunakan sumber daya yang ada secara efisien.

Sedangkan audit informasi yaitu kegiatan mengumpulkan dan menilai bukti untuk menentukan apakah sistem komputerisasi yang ada pada organisasi mampu mengamankan harta, memelihara kebenaran data, dan mampu untuk mencapai tujuan organisasi secara efektif dan penggunaan aset organisasi yang secara tepat menurut (Gondodiyoto, 2006).

2.3.1 Audit Keamanan Sistem Informasi

Audit Keamanan bertujuan untuk evaluasi sistematis dari keamanan informasi dengan cara mengukur beberapa kriteria yang diterapkan oleh perusahaan atau instansi. Sedangkan menurut (Ibrachim *et al.*, 2012) audit keamanan sistem informasi yaitu sebuah kegiatan dimana dilakukannya evaluasi untuk semua proses perlindungan keamanan yang telah diterapkan pada organisasi.

Audit ini mencakup peninjauan terhadap aspek teknis dan manajerial, memastikan bahwa semua komponen keamanan informasi berjalan sesuai dengan standar yang ditetapkan, dan dapat mengidentifikasi potensi kelemahan atau ancaman yang mungkin belum terdeteksi. Dengan demikian, audit keamanan berfungsi sebagai alat penting untuk mengevaluasi kesiapan organisasi dalam menghadapi risiko keamanan informasi serta untuk memberikan rekomendasi perbaikan yang sesuai.

2.4 Sistem Informasi

Sistem informasi adalah kumpulan dari perangkat keras (*hardware*) dan perangkat lunak (*Software*) yang terdapat pada komputer beserta manusia mengolah data menggunakan perangkat keras dan perangkat lunak tersebut, yang menjadi peranan penting dalam sistem informasi salah satunya yaitu data. Data yang akan dimasukkan dalam suatu sistem informasi dapat berupa formulir, prosedur, dan bentuk lainnya (Kristanto, 2003).

Menurut (O'Brien, 2016) Sistem Informasi memiliki beberapa komponen yang penting diantaranya yaitu teknologi informasi, manajemen, konsep dasar, aplikasi bisnis, proses pengembangan. Ada beberapa ciri mengenai sistem diantaranya mempunyai tujuan, mempunyai batasan, terbuka, terdiri dari beberapa susunan sub sistem yang saling berhubungan dan berkaitan (Nopriandi, 2018).

Sehingga dapat disimpulkan bahwa sistem informasi merupakan kumpulan dari elemen *hardware*, *software*, dan juga manusia yang saling membentuk kesatuan untuk mengintegrasikan, memproses, serta menyimpan data sehingga dapat terdistribusikan sebagai *output* informasi.

2.5 Keamanan Sistem Informasi

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*) dan memaksimalkan kinerja proses bisnis. Keamanan informasi merupakan perlindungan informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi atau perusakan yang tidak sah (Klaic, 2010) Menurut ISO 27001 keamanan informasi dapat melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan risiko pencurian data dan memaksimalkan kinerja sistem.



Gambar 2. 1 Tiga pilar keamanan informasi (Arnason & Willet, 2008)

Menurut ISO/IEC 27000:2013 terdapat tiga pilar dalam keamanan informasi yaitu kerahasiaan (*Confidentiality*), integritas atau keutuhan (*Integrity*) dan ketersediaan informasi (*Availability*) yang juga merupakan tujuan keamanan informasi. berikut beberapa aspek yang terdapat pada keamanan informasi (BSN, 2009):

- 1) *Availability* atau aspek ketersediaan yaitu aspek yang memastikan bahwa data akan selalu tersedia saat data tersebut dibutuhkan, menjamin pengguna yang memiliki wewenang dapat menggunakan informasi tersebut beserta perangkat terkait.
- 2) *Integrity* atau aspek integritas yaitu aspek yang memastikan bahwa data tidak dapat diubah tanpa adanya *authorized access* (izin akses) dari pihak yang berwenang, sehingga menjaga keakuratan dan keutuhan informasi.
- 3) *Confidentiality* yaitu aspek yang menjamin kerahasiaan data atau informasi, aspek ini memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang, dan memastikan kerahasiaan data yang dikirim, diterima, dan disimpan.

2.6 Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System (ISMS)* merupakan istilah yang sangat berkaitan terutama pada ISO/IEC 27001:2013 merujuk pada suatu sistem manajemen yang berafiliasi

dengan keamanan informasi. Konsep utama SMKI ini digunakan oleh suatu organisasi sebagai aspek untuk merancang, menerapkan, dan memelihara suatu rangkaian terpadu pada proses serta sistem agar secara efektif dapat mengelola keamanan informasi serta menjamin kerahasiaan, integritas, serta ketersediaan segala aset informasi sekaligus meminimalisir risiko keamanan informasi. (Firmansyah, 2018).

Tujuan dari SMKI yaitu untuk meminimalisir risiko yang ada dan menjamin kelangsungan proses bisnis sebuah organisasi dari ancaman dan membatasi dampak dari adanya pelanggaran keamanan. Dalam sebuah organisasi sangatlah penting untuk menerapkan Sistem Manajemen Keamanan Informasi guna untuk menjaga keamanan aset teknologi informasi yang dimiliki. Pada setiap penerapan Sistem Manajemen Keamanan Informasi juga sangat penting untuk mengacu pada sebuah standar nasional maupun internasional supaya kualitas pengamanan yang diberikan menjamin dan mampu untuk menanggulangi permasalahan yang dialami (Basyarahil *et al.*, 2017).

2.7 Standar Sistem Manajemen Keamanan Informasi IEC/ISO 27000

ISO atau *The International Organization for Standardization* merupakan badan yang memiliki kewenangan menetapkan segala standar internasional baik pada bidang industri maupun komersial dunia dengan tujuan untuk mengoptimalkan perdagangan antar negara.

Pihak ISO mengeluarkan *series* 27000 sebagai rangkaian standar yang berfokus pada manajemen keamanan informasi yang dapat digabungkan untuk menyediakan kerangka kerja yang diakui secara global. Seiring berkembangnya zaman dan berkembangnya teknologi, standar baru terus dikembangkan untuk mengatasi perubahan persyaratan SMKI di berbagai industri dan lingkungan.

Adapun perbedaan ISO 27001 dengan *framework* lainnya berdasarkan 11 kriteria standar keamanan sistem informasi yaitu dapat dilihat pada lampiran 3 (Tabel 3.1 Perbandingan 5 Standar Keamanan).

Dapat disimpulkan bahwa ISO/IEC 27001, ITIL, dan PCI DSS yang memenuhi semua 11 kriteria standar keamanan informasi, sedangkan untuk COBIT tidak memenuhi empat kriteria untuk *Communication and Operation Management, Information System Acquisition, Development and Maintenance, Human Resource*

Security dan Physical and Environment Security. Dan pada framework BS 7799 tidak memenuhi kriteria untuk *Information Security Incident Management*.

Pada penelitian ini penulis menggunakan standar ISO/IEC 27001 sebagai *framework* keamanan informasi, karena *framework* ini dapat digunakan di segala macam jenis instansi, berfokus untuk melindungi aset informasi dan membantu instansi mengetahui tingkat keamanan teknologi informasi yang diterapkan dan tahapan peningkatan yang penting untuk dilakukan pada bagian keamanan informasi.

2.8 ISO 27001

Sesuai dengan perannya pada seri 27000 yang berisi prinsip dasar mengenai ISMS dan sejumlah istilah penting untuk hubungan antar standar dalam keluarga ISMS yang dapat digunakan oleh semua jenis organisasi. Terdapat beberapa jenis standar ISO yang dikeluarkan, salah satunya adalah ISO 27001.

Salah satu seri yang telah diterbitkan oleh *The International Organization for Standardization* yaitu ISO 27001. Pada ISO seri ini berisi mengenai bagaimana spesifikasi persyaratan dalam Sistem Manajemen Keamanan Informasi (SMKI) harus dipenuhi. Seri ini bersifat *independen* terhadap produk teknologi informasi, dirancang untuk menjamin kontrol keamanan yang dipilih sebuah perusahaan dapat melindungi segala aset informasi yang dimiliki dari bahaya risiko dan memberikan tingkat keamanan bagi pihak perusahaan atau pihak yang terkait (KOMINFO Direktorat Keamanan Informasi, 2017).

Pada seri ini juga disediakan kerangka kerja dalam lingkup pengelolaan aset dan penggunaan teknologi informasi yang membantu organisasi untuk memastikan efektivitas keamanan teknologi informasi yang telah diterapkan (Basyarahil et al., 2017). Pada ISO/IEC 27001:2014 keamanan sistem informasi tidak hanya keamanan mengenai penggunaan antivirus, *firewall*, dan manajemen kata sandi saja namun juga pendekatan secara keseluruhan baik dari SDM, proses dan teknologi untuk menjamin berjalannya keamanan yang lebih efektif (Chazar, 2017).

2.8.1 ISO 27001:2013

ISO 27001:2013 merupakan versi terbaru dari seri ISO 27001 yang telah diterbitkan pada tahun 2013 oleh *The International Organization for*

Standardization. ISO 27001:2013 tetap dapat diadopsi oleh semua organisasi, apapun jenis maupun ukurannya sebagaimana versi terdahulu. Berbeda dengan versi 2005 yang mengadopsi model PDCA (*Plan-Do-Check-Act*), versi 2013 tidak secara spesifik menyatakan penggunaan model manajemen tertentu.

Namun demikian model PDCA tetap terlihat pada keseluruhan proses yang ada dalam SMKI yang diarahkan dalam ISO 27001:2013. ISO/IEC 27001:2013 telah ditetapkan oleh badan Standarisasi Nasional Nomor 61/KEP/BSN/4/2016 dan Peraturan Menteri Kominfo Nomor 4 tahun 2016 Pasal 7 (Zulianto et al., 2020). Penggunaan standar Internasional ini dapat berasal dari pihak internal maupun pihak eksternal perusahaan untuk melakukan penilaian keamanan sistem informasi (ISO, 2008).

Adapun manfaat dari adanya penerapan ISO 27001:2013 bagi sebuah organisasi diantaranya dapat meningkatkan kepercayaan publik terhadap segala informasi yang dikeluarkan dan diproses oleh perusahaan tersebut. Standar ISO 27001:2013 ini telah disesuaikan dengan acuan terhadap kebutuhan tujuan, sasaran, dan ruang lingkup untuk memudahkan organisasi dalam penerapan ISMS.

2.8.2 Struktur ISO 27001:2013

Terdapat dua bagian pada struktur ISO/IEC 27001 yaitu:

1. Annex A: Security Control

Annex A merupakan dokumen referensi yang dapat dijadikan sebagai pedoman untuk menentukan kontrol keamanan yang akan diterapkan di dalam Sistem Manajemen Keamanan Informasi.

2. Klausul: Mandatory Process

Klausul dapat dijadikan sebagai standar dalam menyusun kebijakan keamanan oleh perusahaan besar maupun kalangan pemerintahan dalam penerapan *IT Governance*. Klausul pada ISO 27001 berisi mengenai pasal-pasal kebijakan standar keamanan sistem informasi di dalam sebuah organisasi.

Pada seri ISO 27001:2013 memiliki 14 klausul, 35 kontrol objektif, dan 114 kontrol keamanan yang dapat diterapkan dalam membangun SMKI dengan detail yang dapat dilihat pada lampiran 3 (Tabel L3.2 Klausul pada ISO 27001:2013).

2.9 Metode P-D-C-A

Metode PDCA merupakan metode yang dipakai untuk implementasi SMKI. Berikut merupakan pemaparan mengenai metode PDCA atau bisa disebut dengan siklus SMKI (Sarno & Iffano, 2009) :

1. *Plan*

Pada tahap dilakukan untuk merencanakan dan merencanakan SMKI perusahaan. Adapun implementasi SMKI yang harus diterapkan agar sesuai dengan keinginan atau kebutuhan perusahaan yaitu; membangun komitmen, kontrol, kebijakan, prosedur, dan instruksi kerja

2. *Do*

Tahapan ini dilakukan pengimplementasian dan operasi dari kontrol, kebijakan, proses serta prosedur SMKI yang telah direncanakan sebelumnya pada tahap *plan*.

3. *Check*

Pada tahap check yaitu dilakukannya pemantauan pelaksanaan SMKI melalui kegiatan evaluasi atau bisa disebut sebagai audit SMKI. Tahapan ini juga dilakukan untuk mengetahui apakah SMKI yang telah diterapkan berjalan sesuai dengan keinginan instansi serta pemberian solusi perbaikan apabila SMKI yang ada pada saat itu kurang sesuai dengan harapan instansi.

4. *Act*

Tahapan ini merupakan serangkaian kegiatan untuk perbaikan, pengembangan SMKI, dan tindakan pencegahan berdasarkan temuan hasil audit pada tahapan *check*.

2.10 Penilaian Risiko (*Risk Assessment*)

Penilaian risiko dibutuhkan untuk mengukur atau menjabarkan secara kualitatif suatu risiko dengan tujuan manajer dapat memprioritaskan risiko yang sesuai dengan kriteria yang telah menyebabkan potensi kerugian bagi perusahaan serta untuk mendapatkan ilustrasi mengenai bagaimana, dimana, dan mengapa suatu kerugian mungkin terjadi (ISO, 2008).

Menurut (Sarno & Iffano, 2009) penilaian risiko merupakan tahapan awal untuk mengetahui ancaman (*threat*) yang berpotensi SMKI organisasi dan potensi kelemahan yang mungkin dimiliki oleh perusahaan.

2.10.1 Identifikasi Aset dan Menghitung Aset

Menurut (ISO, 2008) aset merupakan salah satu yang bernilai bagi perusahaan oleh karena itu dibutuhkannya perlindungan. Untuk identifikasi aset juga perlu diingat bahwa sistem informasi terdiri dari perangkat keras (*hardware*) dan perangkat lunak (*Software*). Arti identifikasi pada hal ini yaitu mengelompokkan aset kedalam beberapa kategori maupun golongan. Sehingga *Output* yang dihasilkan pada tahap ini yaitu daftar inventaris aset yang dimiliki oleh organisasi (Sarno & Iffano, 2009). Sedangkan menghitung nilai aset ialah menghitung nilai dari informasi yang dimiliki oleh perusahaan. Menghitung nilai aset dilakukan berdasarkan Kerahasiaan (*Confidentiality*), keutuhan (*Integrity*), serta ketersediaan (*Availability*).

Berikut pada tabel 2.1 merupakan contoh penilaian aset berdasarkan aspek kerahasiaan (*Confidentiality*)

Tabel 2. 1 Penilaian aset menurut aspek kerahasiaan (*Confidentiality*)

Aspek <i>Confidentiality</i>	Nilai <i>Confidentiality</i> (NC)
<i>Public</i>	0
<i>Internal use only</i>	1
<i>Private</i>	2
<i>Confidentiality</i>	3
<i>Secret</i>	4

Sumber : (Sarno & Iffano, 2009)

Pada Tabel 2.2 merupakan contoh dari penilaian aset berdasarkan aspek keutuhan (*Integrity*)

Tabel 2. 2 Penilaian aset menurut aspek keutuhan (*Integrity*)

Aspek <i>Integrity</i>	Nilai <i>Integrity</i> (NI)
<i>No Impact</i>	0
<i>Minor incident</i>	1
<i>General disturbance</i>	2
<i>Mayor disturbance</i>	3
<i>Unacceptable damage</i>	4

Sumber : (Sarno & Iffano, 2009)

Pada Tabel 2.3 merupakan contoh dari penilaian aset berdasarkan aspek ketersediaan (*availability*)

Tabel 2. 3 Penilaian aset menurut aspek ketersediaan (*Availability*)

Aspek <i>Availability</i>	Nilai <i>Availability</i> (NA)
<i>Low / No Availability</i>	0
<i>Office hour Availability</i>	1
<i>Strong Availability</i>	2
<i>High Availability</i>	3
<i>Very high Availability</i>	4

Sumber: (Sarno & Iffano, 2009)

Apabila telah ditentukan nilai dari setiap aset berdasarkan 3 aspek di atas maka selanjutnya yaitu menghitung nilai aspek dengan menggunakan rumus persamaan di bawah ini (Sarno & Iffano, 2009)

$$\text{Nilai Aset} = NC + NI + NV \dots\dots\dots (2.1)$$

Keterangan :

NC: Nilai *Confidence* yang telah disesuaikan dengan tabel

NI : Nilai *Integrity* yang telah disesuaikan dengan tabel

NV : Nilai *Availability* yang telah disesuaikan dengan tabel

2.10.2 Identifikasi ancaman (*Threat*) dan Kelemahan (*Vulnerability*) Aset

Menurut (IBISA, 2011) ancaman ialah kejadian yang dapat mengakibatkan suatu perusahaan mengalami kerugian. Kerugian yang dialami dapat berupa kerugian materi, uang, tenaga, reputasi nama baik, upaya hingga dapat mengakibatkan perusahaan itu mengalami kebangkrutan. Ancaman juga memiliki potensi membahayakan aset informasi, sistem, dan proses bisnis perusahaan. Menurut (ISO, 2008) ancaman harus diidentifikasi secara umum berdasarkan jenisnya. Berikut merupakan contoh ancaman yang dapat terjadi pada sebuah perusahaan

Tabel 2. 4 Jenis dan Contoh Ancaman

No	Jenis ancaman	Contoh ancaman
1.	Kerusakan fisik	Kerusakan karena air, kebakaran, korosi dan pembekuan, polusi, debu, kerusakan pada peralatan

No	Jenis ancaman	Contoh ancaman
2.	Peristiwa alam	Iklim cuaca, gempa bumi, gunung meletus, badai hujan petir, angin puting beliung, banjir.
3.	Kehilangan layanan	Hilangnya pasokan listrik, kegagalan sistem pasokan air
4.	Manusia	
	<i>Hacker dan cracker</i>	<i>Hacking</i> merupakan kegiatan meretas sistem untuk mencari bugs pada sistem yang akan dimasuki. <i>Crackers</i> ialah tindakan penyusupan ke dalam sistem untuk mengambil ataupun merusak informasi yang ada dalam sistem
	Terrorist	Blackmail, sistem penetrasi, penyerangan sistem, virus
	Karyawan	Kelalaian dalam <i>entry</i> data atau pemrograman

Sumber : (ISO, 2008)

Sedangkan yang dimaksud kelemahan merupakan kekurangan dari prosedur keamanan informasi, baik dalam tahap perencanaan, implementasi atau kontrol internal yang hanya dalam ruang lingkup perusahaan untuk penjagaan informasi yang dapat menimbulkan ancaman. Berikut merupakan contoh daftar kelemahan aset

Tabel 2. 5 Contoh daftar kelemahan

Kelemahan	Contoh
Gangguan sumber daya	Kerentanan terhadap voltase yang bervariasi.
Gangguan perangkat keras	Kerentanan terhadap kelembaban debu dan kotoran, Kurangnya pemeliharaan media penyimpanan, Penyimpanan yang tidak dilindungi, kurangnya perawatan di pembuangan penyalinan yang tidak terkendali.
Gangguan perangkat lunak	Desain antarmuka yang rumit, kurangnya pengujian perangkat lunak, Perangkat lunak yang didistribusikan secara luas.
Kerusakan data	Menerapkan program aplikasi yang terkena virus ataupun didistribusikan secara luas.
Kurang kesadaran pengguna	Kelalaian lupa <i>log out</i> ketika meninggalkan PC, kurangnya pelatihan keamanan, kurang kesadaran dalam hal keamanan
Jaringan	Sambungan kabel yang buruk, arsitektur jaringan yang tidak aman, koneksi jaringan publik yang tidak dilindungi.

Sumber : (Sarno & Iffano, 2009)

Kemudian untuk rerata probabilitas akan terjadi ancaman dan kelemahan dihasilkan dari klasifikasi kemungkinan kejadian dengan rentang nilai seperti pada tabel 2.6:

Tabel 2. 6 Nilai Rerata Probabilitas

Keterangan	Nilai Kemungkinan Kejadian
LOW	0.1 – 0.3
MEDIUM	0.4 – 0.6
HIGH	0.7 – 1.0

Sumber : (Sarno & Iffano, 2009)

Langkah berikutnya setelah mengidentifikasi ancaman dan kelemahan maka selanjutnya dapat dicari nilainya dengan menggunakan rumus persamaan sebagai berikut : (Sarno & Iffano, 2009)

$$\text{Nilai Ancaman (NT)} = \sum PO / \sum \text{Ancaman} \dots \dots \dots (2.2)$$

Keterangan :

\sum PO: Jumlah *probability Occurrence*

\sum Ancaman: Jumlah ancaman terhadap informasi

2.10.3 Analisis Evaluasi Risiko

Diperoleh pada tahap sebelumnya untuk mengetahui serta memahami sejauh mana level risiko yang dapat terjadi serta menganalisis apakah risiko tersebut dapat langsung diterima atau masih memerlukan pengelolaan supaya dampak risiko yang diterima masih dapat ditoleransi atau tidak (Sarno & Iffano, 2009). Terdapat beberapa tahapan pada analisis dan evaluasi risiko di antaranya:

1. Analisis dampak bisnis (*Business Impact Analysis*) / BIA

Analisis dampak yang ditujukan seberapa besar dampak atau pengaruh risiko terhadap proses bisnis perusahaan. Adapun dampak bisnis dilakukan dengan menentukan skala BIA seperti pada tabel 2.7:

Tabel 2. 7 Skala Business Impact Analysis (BIA)

Batas Toleransi gangguan	Keterangan	Nilai skala
< 1 minggu	<i>Not critical</i>	0 -20
1 hari - 2 hari	<i>Minor critical</i>	21 – 40
<1 hari	<i>Mayor critical</i>	41 – 60
< 12 jam	<i>High critical</i>	61 – 80
<1 jam	<i>Very High critical</i>	81 - 100

Sumber: (Sarno & Iffano, 2009)

2. Identifikasi level risiko (*risk level*)

Level risiko merupakan tingkat risiko yang muncul apabila dihubungkan dengan dampak dan probabilitas ancaman yang mungkin timbul (Sarno & Iffano, 2009). Tahapan ini memiliki ketentuan yang diterima perusahaan yang mengacu

pada hubungan probabilitas ancaman yang mungkin terjadi dengan dampak yang mungkin ada. Adapun tabel acuan identifikasi level risiko seperti pada tabel 2.8:

Tabel 2. 8 Matriks Level Risiko

Probabilitas ancaman	Dampak Bisnis (Impact)				
	Not Critical (20)	Low Critical (40)	Medium Critical (60)	High Critical (80)	Very High critical (100)
Low (0.1)	Low $20 \times 0.1 = 2$	Low $40 \times 0.1 = 4$	Low $60 \times 0.1 = 6$	Low $80 \times 0.1 = 8$	Low $100 \times 0.1 = 100$
Medium (0.5)	Low $20 \times 0.5 = 10$	Medium $40 \times 0.5 = 20$	Medium $60 \times 0.5 = 30$	Medium $80 \times 0.5 = 40$	Medium $100 \times 0.5 = 50$
High (1.0)	Medium $20 \times 1.0 = 20$	Medium $40 \times 1.0 = 40$	High $60 \times 1.0 = 60$	High $80 \times 1.0 = 80$	High $100 \times 1.0 = 100$

Sumber : (Sarno & Iffano, 2009)

Selanjutnya merupakan tahap menentukan apakah risiko yang muncul langsung dapat diterima atau dikelola. Nilai risiko merupakan gambaran dari seberapa besar akibat yang akan diterima oleh perusahaan apabila ancaman yang menyebabkan kegagalan keamanan informasi terjadi (Sarno & Iffano, 2009). Berikut merupakan rumus persamaan untuk melakukan penilaian risiko :

$$\text{Nilai Risiko} = \text{NA} \times \text{BIA} \times \text{NT} \dots\dots\dots(2.3)$$

Keterangan :

NA : Nilai Aset

BIA : Analisis Dampak Bisnis

NT : Nilai Ancaman

Kemudian apabila telah melakukan penilaian risiko maka selanjutnya ialah menghubungkan dengan matriks risiko yang ada pada tahapan sebelumnya untuk menentukan apakah risiko akan mungkin terjadi langsung atau dapat diterima ataupun apakah diperlukannya penanganan terlebih dahulu.

2.11 SSE-CMM (System Security Engineering Capability Maturity Model)

SSE-CMM merupakan referensi model untuk meningkatkan dan menilai kemampuan rekayasa terkait dengan domain keamanan teknologi informasi.

Tujuan dari SSE-CMM ialah untuk memajukan rekayasa keamanan yang lebih terdefinisi, dan terukur. SSE-CMM ini telah dikembangkan untuk mendukung praktik keamanan dengan tujuan meningkatkan kualitas serta layanan rekayasa keamanan. Menurut (University, 2003) terdapat 5 tingkat dalam SSE-CCM yaitu di antaranya :

1. Level 1 *Performed Informally*

Dimana praktik dasar umumnya harus dilakukan. Pada level ini kinerja praktik dasar belum sepenuhnya direncanakan. Kinerja tergantung pada pengetahuan individu serta perusahaan. Hasil kerja pada level ini memberikan hasil untuk kinerja perusahaan.

2. Level 2 *Planned and Tracked*

Kinerja sesuai dengan prosedur yang sudah diverifikasi. Pada tingkatan ini berfokus pada definisi, perencanaan dan masalah kinerja. Hasil kinerja sesuai dengan standar yang telah ditetapkan serta sesuai dengan persyaratan. Perbedaan antara level 1 yaitu proses kinerja sudah lebih terencana dan dikelola.

3. Level 3 *Well defined*

Pada level ini sudah berfokus pada penyesuaian disiplin dari proses yang ditetapkan di tingkat perusahaan. Pada tingkatan ini menggunakan persetujuan sesuai dengan standar yang ada dan proses tersebut telah didokumentasikan. Perbedaan dengan level 2 yaitu pada tingkatan ini proses kinerja ini direncanakan dan dikelola dengan proses standar perusahaan

4. Level 4 *Quantitatively Controlled*

Pada tingkatan ini berfokus pada pengukuran yang berkaitan dengan tujuan bisnis perusahaan. Perbedaan dengan kinerja level 3 yaitu, proses kinerja telah didefinisikan dipahami dan dikendalikan secara kuantitatif.

5. Level 5 *Continuously Improving*

Pada level 5 ini dilakukan proses perbaikan secara menyeluruh dari proses yang telah didefinisikan. Perbedaan dengan level 4 yaitu proses yang didefinisikan dan yang telah sesuai dengan standar menjalani perbaikan terus-menerus dan

dilakukannya peningkatan berdasarkan pemahaman kuantitatif dampak perubahan proses.

Tabel 2. 9 *Capability Level SSE-CMM*

Keterangan	Level
<i>Performed Informally</i>	1
<i>Planned and Tracked</i>	2
<i>Well Defined</i>	3
<i>Quantitatively Controlled</i>	4
<i>Continuously Improving</i>	5

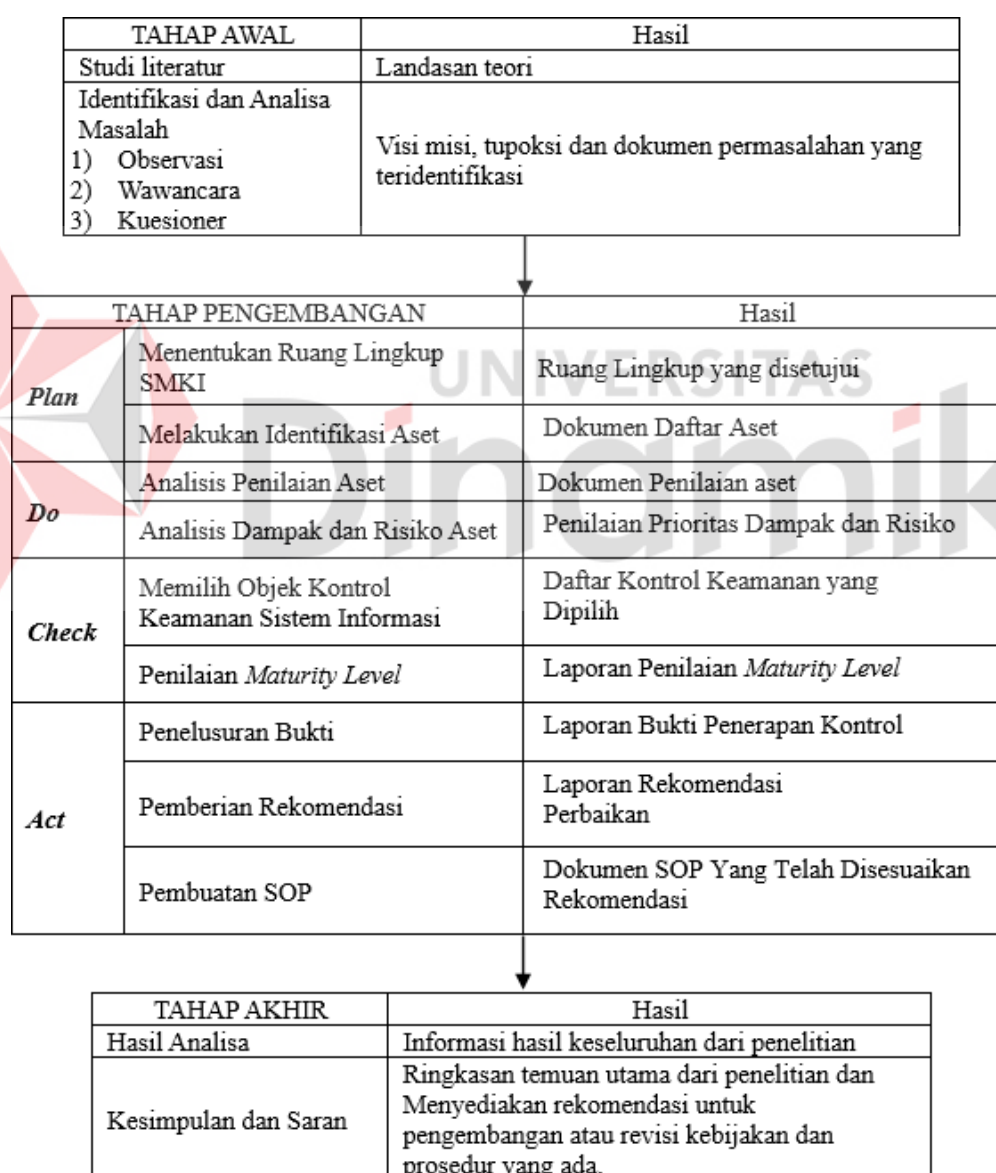
Sumber : (University, 2003)



UNIVERSITAS
Dinamika

BAB III METODE PENELITIAN

Adapun metode dalam penelitian yang dilakukan pada Dinas Kominfo Kota Mojokerto penulis menggunakan langkah-langkah pelaksanaan audit keamanan sistem informasi yang mengacu pada siklus P-D-C-A ISO 27001:2013 seperti pada diagram 3.1 :



Gambar 3. 1 Metode Penelitian

3.1 Tahap Awal

Pada tahap awal, dimulai dengan studi literatur untuk membangun landasan teori yang kuat sebagai dasar penelitian. Langkah selanjutnya adalah mengidentifikasi dan menganalisis permasalahan yang ada di Diskominfo Kota Mojokerto. Proses ini dilakukan melalui berbagai metode seperti observasi, wawancara, dan penyebaran kuesioner. Hasil dari identifikasi ini mencakup pemahaman terhadap visi, misi, tupoksi (tugas pokok dan fungsi), serta dokumen permasalahan yang berhasil diidentifikasi.

3.1.1 Studi Literatur

Tahapan Studi literatur dilakukan dengan Studi literatur dilakukan dengan membaca dan memahami informasi dari sumber-sumber seperti buku fisik, e-book, jurnal penelitian, dan skripsi terkait audit keamanan sistem informasi dan ISO/IEC 27001. Selain itu, penulis mempelajari kebijakan dari Dinas Komunikasi dan Informatika Kota Mojokerto, termasuk Rancangan Kerja, Pelaturan Walikota, dan SOP yang diterapkan untuk memahami kondisi proses bisnis dan sistem informasi saat ini.

3.1.2 Identifikasi dan Analisis Permasalahan

Langkah awal dalam analisis di Diskominfo Kota Mojokerto adalah mengidentifikasi permasalahan yang ada. Identifikasi ini dilakukan melalui wawancara dan observasi yang mengevaluasi kondisi terkini di instansi tersebut. Proses ini dimulai dengan mengungkap permasalahan yang ada, dilanjutkan dengan pengumpulan data dan referensi yang relevan untuk mendukung penelitian. Data yang dikumpulkan mencakup daftar risiko keamanan informasi, yang berguna untuk memahami potensi risiko, frekuensi kemunculannya, serta peluang terulangnya risiko di lingkungan Diskominfo Kota Mojokerto. Tahapan ini dilaksanakan dengan 2 tahapan yaitu observasi dan wawancara langsung dengan kepala Aplikasi dan Infrastruktur Informasi.

1) Observasi

Observasi dilakukan dengan pengamatan langsung proses sistem keamanan informasi yang berlangsung pada di Kantor Dinas Komunikasi dan Informatika yang terletak di gedung GMSC Lantai 3, Jl. Gajah Mada No.149, Mergelo, Balongsari, Kec. Magersari, Kota Mojokerto, Jawa Timur 61314. Didapatkan data berupa tugas pokok dan fungsi, Visi Misi serta struktur organisasi pada Dinas Kominfo Kota Mojokerto.

2) Wawancara

Untuk mengetahui penerapan sistem keamanan informasi serta permasalahan yang kerap kali maka penulis melakukan sesi tanya jawab dengan beberapa staf ahli dari Dinas Kominfo kota Mojokerto.

3.2 Tahap Pengembangan (Pelaksanaan Audit)

Tahap Pengembangan (Pelaksanaan Audit) dalam penelitian keamanan informasi menggunakan siklus PDCA (*Plan-Do-Check-Act*) perencanaan audit, pelaksanaan di lapangan untuk pengumpulan data, evaluasi hasil untuk identifikasi kepatuhan dan perbaikan, serta implementasi tindakan untuk meningkatkan keamanan informasi di Kantor Dinas Komunikasi dan Informatika Kota Mojokerto.

3.2.1 Tahapan *Plan*

1. Menentukan ruang lingkup SMKI

Tahapan ini melibatkan identifikasi area, proses bisnis dan aset yang akan dilindungi. Organisasi harus mempertimbangkan faktor internal dan eksternal, seperti kebutuhan bisnis, persyaratan hukum, serta risiko keamanan informasi yang dihadapi. Hasil dari tahap ini yaitu berupa batasan mengenai area fungsional yang akan diaudit.

Penetapan batasan ini membantu memastikan bahwa audit dilakukan secara optimal dan dengan efikasi tinggi, dengan fokus pada aspek-aspek yang paling mempengaruhi kepatuhan dan kinerja keamanan informasi pada *website* portal kota Mojokerto.

2. Identifikasi Aset Ruang lingkup SMKI

Proses identifikasi aset dimulai dengan mengumpulkan data dan informasi dari berbagai sumber, termasuk wawancara dengan staf, peninjauan dokumentasi, serta observasi langsung terhadap infrastruktur teknologi informasi yang digunakan. Setiap aset yang diidentifikasi kemudian dikategorikan berdasarkan jenis dan kepentingannya terhadap operasional organisasi.

3.2.2 Tahapan *Do*

1. Melakukan Identifikasi Nilai Aset

Tahapan pertama yang dilakukan ialah melakukan identifikasi pada ancaman yang mungkin terjadi pada Aset Dinas Kominfo Kota Mojokerto, adapun tahapan melakukan identifikasi risiko yaitu:

- A. Melakukan identifikasi terhadap ancaman dan kelemahan aset yang dapat mengganggu proses bisnis dengan cara menghitung nilai dari ancaman dan kelemahan yang ditemukan pada aset Dinas Kominfo kota Mojokerto.
- B. Melakukan perhitungan Nilai Ancaman berdasarkan kemungkinan terjadinya ancaman dan kelemahan dari masing masing aset dengan menggunakan skala nilai rerata probabilitas beserta levelnya.

2. Analisis dan Evaluasi Dampak Risiko

Tahap berikutnya yaitu melakukan analisis dan evaluasi dampak dan risiko sesuai dengan hasil identifikasi pada tahap sebelumnya. Analisis serta evaluasi dampak digunakan untuk menentukan apakah risiko yang terjadi kepada aset yang dimiliki oleh Dinas Kominfo kota Mojokerto langsung diterima atau masih harus dilakukan pengelolaan supaya risiko dapat diterima dengan dampak yang ditoleransi. Adapun langkah untuk analisis dan evaluasi risiko yaitu:

- A. Melakukan analisis berdasarkan dampak dan risiko bisnis yang ditimbulkan (*Business Impact Analysis*), pada tahap analisis ini dilakukan dengan menentukan nilai berdasarkan skala nilai BIA.
- B. Melakukan identifikasi level risiko (*risk level*) untuk menilai tingkat risiko yang terjadi apabila digabungkan dengan dampak bisnis dan probabilitas ancaman yang mungkin terjadi. Pada tahap ini identifikasi nilai berpedoman pada matriks level risiko.

3.2.3 Tahapan *Check*

1. Memilih Objek Kontrol Keamanan Informasi

Dalam tahapan ini, dilakukan pemilihan kontrol objektif dan kontrol keamanan berdasarkan hasil identifikasi aset, nilai risiko, serta analisis risiko yang telah ditentukan sebelumnya. Proses ini mencakup penyusunan tabel identifikasi aset, tabel nilai risiko, tabel identifikasi nilai risiko, serta tabel pemilihan kontrol. Setelah itu, dipilih penanganan risiko yang paling tepat, diikuti dengan penerapan kontrol objektif dan kontrol keamanan yang sesuai untuk memastikan mitigasi risiko yang efektif..

2. Penilaian Maturity Level menggunakan metode SSE-CCM

Pada tahapan menentukan Maturity Level, penulis menggunakan model SSE-CCM (*System Security Engineering Capability Maturity Model*). Langkah-langkah yang dikerjakan pada penilaian maturity level di antaranya:

A. Pembuatan pernyataan

Setelah ditetapkan objek kontrol dan kontrol keamanan yang akan digunakan dari hasil pengukuran risiko, kemudian penulis membuat pernyataan yang mengacu pada kontrol keamanan dari setiap objektif kontrol yang dipilih untuk diterapkan pada Dinas Kominfo Kota Mojokerto. Pernyataan yang dibuat disesuaikan dengan standar ISO 27001: 2013 yang berisi panduan implementasi dari setiap klausul yang dipilih.

B. Penentuan tingkat kemampuan

Penulis menggunakan tabel SSE-CMM sebagai acuan menilai level kemampuan pada pernyataan.

Tabel 3. 1 Tingkat kemampuan SSE-CMM

Deskripsi	Tingkat Kemampuan
<i>Performed Informally</i> (Dilakukan Informal)	1
<i>Planned and tracked</i> (Direncanakan dan dilacak)	2
<i>Well Defined</i> (Didefinisikan dengan baik)	3
<i>Quantitatively controlled</i> (Dikendalikan secara kuantitatif)	4

Deskripsi	Tingkat Kemampuan
<i>Continuously improving</i> (Ditingkatkan terus-menerus)	5

Sumber : (University, 2003)

3.2.4 Tahapan Act

1. Penelusuran Bukti

Pada tahapan ini dilakukan penelusuran bukti sesuai dengan penilaian pada maturity level yang telah dilakukan pada fase tahapan *check*. Hal tersebut dilakukan untuk menyesuaikan kondisi sebenarnya dari keamanan informasi pada Dinas Kominfo Kota Mojokerto dan untuk mendapatkan hasil apakah terdapat gap antara kondisi saat ini dengan implementasi kontrol keamanan yang ada pada ISO 27001: 2013.

2. Pemberian Rekomendasi

Tahapan akhir ini dilakukan dengan memberikan hasil rekomendasi berdasarkan gap yang ditemui pada tahap penelusuran bukti. Pada fase ini juga akan diberikan masukan perbaikan dan pengembangan SMKI serta panduan implementasi dari tiap kontrol keamanan pada pihak manajerial Dinas Kominfo Kota Mojokerto yang mengacu pada ISO 27001: 2013.

3. Pembuatan *Standard Operational Procedure* (SOP)

Pada tahap ini akan dilakukan pembuatan SOP berdasarkan pemilihan klausul dan rekomendasi yang telah dihasilkan dari audit. Pada tahap ini juga akan dihasilkan dokumen berupa instruksi kerja dan rekaman kerja untuk memastikan bahwa setiap prosedur telah diterapkan.

3.3 Tahap Akhir

Pada tahapan akhir ini penulis akan menyimpulkan rekomendasi yang telah dihasilkan berdasarkan permasalahan dan gap yang ada serta memberikan saran untuk membantu organisasi tersebut.

1. Hasil Analisis

Pada tahap ini, dijelaskan hasil kerja dari tugas akhir yang diperoleh dari penelitian yang telah dilakukan dengan metode pelaksanaan yang direncanakan. Hasil analisis mencakup rekomendasi perbaikan keamanan informasi berdasarkan temuan penelitian yang ada.

2. Kesimpulan dan saran

Pada tahap ini, kesimpulan dari penelitian dan pembahasan yang telah dilakukan akan dijelaskan secara ringkas, mencakup penilaian umum terhadap keamanan informasi efektivitas kontrol yang ada, serta kesenjangan yang perlu diatasi. Selain itu, diberikan saran untuk pengembangan lebih lanjut, diharapkan dapat membantu organisasi dalam meningkatkan sistem keamanan informasi dan mengurangi risiko yang ada di masa depan.



UNIVERSITAS
Dinamika

BAB IV

HASIL DAN PEMBAHASAN

Pada bab IV ini dijelaskan hasil dari penelitian Audit Keamanan Sistem Informasi pada Dinas Komunikasi dan Informatika Kota Mojokerto berdasarkan standar ISO 27001:2013. Hasil yang didapat diperoleh dari metode dari tahapan awal, tahap pengembangan dan tahapan akhir.

4.1 Tahapan Awal

4.1.1 Studi Literatur

Dalam penyusunan penelitian, perlu diterapkan teknik yang sistematis agar mempermudah pelaksanaan setiap langkah yang diambil pada tahap penyusunan. Sesuai dengan tahapan yang diuraikan dalam metodologi penelitian, tahap awal yang dilakukan adalah studi literatur, dengan mencari referensi berupa buku di perpustakaan serta jurnal yang relevan dengan topik penelitian. Studi literatur yang digunakan dalam penyusunan laporan ini meliputi:

1. Konsep keamanan informasi yang diterapkan untuk menyusun dokumen aset, mengelola keamanan informasi, dan menetapkan kontrol objektif serta kontrol keamanan.
2. Konsep pengelolaan risiko keamanan informasi yang digunakan dalam penyusunan pengelolaan risiko terkait keamanan informasi.
3. Sistem manajemen keamanan informasi yang berperan dalam penyusunan langkah-langkah untuk menentukan kontrol objektif dan kontrol keamanan.

4.2.1 Identifikasi dan Analisis Masalah

A. Wawancara

Tujuan dari wawancara ini adalah untuk memperoleh informasi dan data yang diperlukan terkait topik penelitian. Wawancara ini dilaksanakan dengan Bapak Zakky Nilelm Sanjifa, kepala bagian Aplikasi dan Infrastruktur Informasi. Berikut adalah uraian hasil wawancara tersebut:

1) Visi dan Misi Diskominfo Kota Mojokerto

Hasil wawancara yang membahas visi dan misi organisasi, yang dilakukan dengan Bapak Zakky Nilelm Sanjifa sebagai Aplikasi dan Infrastruktur Informasi, telah dicatat secara rinci. Informasi lengkap mengenai hal tersebut dapat ditemukan pada lampiran 4.

2) Struktur organisasi dan tugas pokok Diskominfo Kota Mojokerto

Detail mengenai struktur organisasi, serta tugas pokok dan fungsi dari setiap bagian di Diskominfo Kota Mojokerto, disajikan secara rinci dalam lampiran 4. Lampiran tersebut memberikan penjelasan mendalam mengenai pembagian tugas dan peran masing-masing bagian dalam struktur organisasi pada Diskominfo Kota Mojokerto.

3) Proses bisnis dan kebijakan pelayanan

Kebijakan pelayanan ini mencakup proses layanan yang diterapkan dalam operasional bidang Aplikasi dan Infrastruktur Informasi. Penjelasan rinci mengenai proses bisnis yang diterapkan dan kebijakan pelayanan tersebut dapat ditemukan dalam lampiran 5.

4) Daftar kejadian terkait keamanan informasi pada Diskominfo Kota Mojokerto

Daftar kejadian ini merangkum semua peristiwa yang telah terjadi di Diskominfo Kota Mojokerto, termasuk setiap insiden dan tindakan yang telah diambil untuk menanganinya. Dokumen ini mencatat setiap kejadian secara kronologis serta langkah-langkah yang telah diimplementasikan untuk mengatasi atau menyelesaikannya. Informasi terperinci mengenai daftar kejadian tersebut dapat ditemukan pada lampiran 6.

B. Observasi

Pada tahap observasi, auditor mengumpulkan data yang relevan melalui berbagai metode, selain wawancara dengan staf yaitu dilakukannya pemeriksaan dokumentasi seperti renstra, dan pengamatan langsung terhadap proses kerja. Data yang dikumpulkan mencakup informasi tentang pemeliharaan sistem, pengendalian akses, serta pengelolaan insiden dan risiko. Pengumpulan data ini bertujuan untuk mendapatkan data yang rinci mengenai permasalahan dan kendala yang sering

dihadapi oleh Diskominfo Kota Mojokerto. Untuk daftar kejadian mengenai keamanan informasi dapat dilihat lebih rinci pada lampiran 7.

4.1.2. Dokumen Permasalahan yang Teridentifikasi

Berdasarkan hasil observasi dan wawancara, ditemukan beberapa kekurangan dalam pengelolaan teknologi informasi di Diskominfo Kota Mojokerto. Dari aspek kerahasiaan (*Confidentiality*), belum ada kebijakan yang mengatur pengelolaan kata sandi untuk sistem informasi, sehingga data dan informasi berisiko diakses oleh pihak yang tidak berwenang. Dari aspek keutuhan (*Integrity*), adanya platform OPD dari pihak ketiga menyebabkan perubahan data dan informasi tanpa sepengetahuan Diskominfo sebagai penyedia SPBE (Sistem Informasi Berbasis Elektronik). Dari aspek ketersediaan (*Availability*), sering terjadi gangguan server, terutama saat acara besar, akibat kapasitas terbatas pada CPU, RAM, dan bandwidth, yang mengakibatkan server menjadi tidak responsif atau down ketika menghadapi permintaan yang tinggi.

4.2 Tahapan Pengembangan (Pelaksanaan Audit)

Tahap pengembangan dalam penelitian ini mengikuti pendekatan PDCA. Pada fase *Plan*, dilakukan perencanaan dan identifikasi masalah melalui pembuatan dokumen aset, penentuan ruang lingkup, dan kebijakan SMKI. Di fase *Do*, data dikumpulkan, audit dilakukan, dan analisis diterapkan melalui dokumen pengelolaan risiko serta kontrol objektif dan keamanan. Selanjutnya, pada fase *Check*, hasil evaluasi dibandingkan dengan standar ISO 27001:2013 untuk mengidentifikasi kesenjangan.

Terakhir, pada fase *Act*, rekomendasi diterapkan, manajemen diinformasikan, dan pemantauan berkala dilakukan. Pendekatan ini memastikan bahwa penelitian dilakukan secara sistematis dan berkelanjutan.

4.1.1 Tahapan *Plan*

Pada tahapan ini akan dilakukan pengumpulan informasi aset yang dimiliki oleh Diskominfo Kota Mojokerto sebelum dilakukannya penilaian aset pada tahapan *Do*. Selain itu pada tahapan ini dilakukan identifikasi serta menentukan ruang lingkup SMKI.

A. Menentukan Ruang Lingkup SMKI

Ruang lingkup SMKI di Diskominfo Kota Mojokerto ditetapkan melalui wawancara dengan Bapak Zakky Nilem Sanjifa, Kepala Bidang Aplikasi dan Infrastruktur. Bidang ini bertanggung jawab atas pengembangan, pemeliharaan, dan keamanan infrastruktur TI serta aplikasi yang digunakan. Komitmen organisasi adalah melindungi informasi sesuai dengan standar ISO 27001:2013. Ruang lingkungnya mencakup:

- a) Bagian Aplikasi dan Infrastruktur
- b) Aset TI, termasuk perangkat keras, perangkat lunak, dan data.

B. Identifikasi Aset Pada Ruang lingkup SMKI

Tahapan ini merupakan tahapan dimana auditor akan melakukan identifikasi dan pencatatan terhadap aset aset yang dimiliki oleh bagian Aplikasi dan Infrastruktur Informatika Diskominfo Kota Mojokerto.

1. Aset Utama

Aset utama merupakan aset yang digunakan untuk proses bisnis utama dari kegiatan dan pada ruang lingkup instansi. Berikut aset utama yang dimiliki oleh bagian Aplikasi dan Infrastruktur Informatika Diskominfo Kota Mojokerto. Untuk penjelasan lebih detail mengenai aset utama dapat dilihat pada lampiran 8 (Tabel L8.1 Daftar Aset Utama).

2. Aset Pendukung

Aset pendukung merupakan aset yang digunakan sebagai fasilitas alat bantu atau pendukung dalam proses bisnis. Berikut Aset pendukung yang dimiliki oleh bagian Aplikasi dan Infrastruktur Informatika Diskominfo Kota Mojokerto dapat dilihat pada lampiran 8 (Tabel L8.2 Daftar Aset Pendukung).

3. Aset Kritis

Dari daftar aset yang dimiliki oleh Bagian Aplikasi dan Infrastruktur Aplikasi maka langkah selanjutnya yaitu menentukan aset kritis dari Diskominfo Kota Mojokerto. Aset kritis ialah aset yang sangat vital bagi kelangsungan proses bisnis atau keselamatan entitas tersebut. Hasil dari observasi aset kritis Diskominfo Kota Mojokerto dapat lebih dilihat pada lampiran 8 (Tabel L8.3 Tabel Aset Kritis).

4.1.2 Tahapan *Do*

Pada tahapan *Do* dilakukan identifikasi dan evaluasi risiko yang berkaitan dengan aset yang dimiliki oleh bagian Aplikasi dan Infrastruktur Informasi Diskominfo Kota Mojokerto.

1. Analisis Penilaian Aset

Dari hasil penentuan aset kritis kemudian akan dilakukan penilaian nilai aset dengan menghitung nilai berdasarkan Kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*), dan Ketersediaan (*Availability*) berdasarkan wawancara dan observasi.

Tabel-tabel berikut digunakan untuk menentukan nilai aset dari perspektif kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Penilaian ini membantu dalam mengidentifikasi seberapa penting setiap aspek keamanan informasi bagi aset tersebut, yang selanjutnya digunakan untuk menghitung total nilai aset dan menentukan prioritas pengelolaannya.

Tabel 4. 1 Nilai aset dari sisi kerahasiaan (*Confidentiality*)

Aspek <i>Confidentiality</i>	Nilai <i>Confidentiality</i> (NC)
<i>Public</i>	0
<i>Internal use only</i>	1
<i>Private</i>	2
<i>Confidentiality</i>	3
<i>Secret</i>	4

Tabel 4. 2 Nilai aset dari sisi keutuhan (*Integrity*)

Aspek <i>Integrity</i>	Nilai <i>Integrity</i> (NI)
<i>No Impact</i>	0
<i>Minor incident</i>	1
<i>General disturbance</i>	2
<i>Mayor disturbance</i>	3
<i>Unacceptable damage</i>	4

Tabel 4. 3 Nilai aset dari sisi ketersediaan (*Availability*)

Aspek <i>Availability</i>	Nilai <i>Availability</i> (NA)
<i>Low / No Availability</i>	0
<i>Office hour Availability</i>	1
<i>Strong Availability</i>	2
<i>High Availability</i>	3
<i>Very high Availability</i>	4

Setelah nilai-nilai ini ditentukan, nilai total aset (NV) dihitung menggunakan rumus:

$$\text{Nilai Aset} = NC + NI + NV \dots\dots\dots (4.1)$$

Keterangan :

NC: Nilai *Confidence*

NI : Nilai *Integrity*

NV : Nilai *Availability*

Contoh Penerapan kepemilikan aset Data Aplikasi yang dinilai (sebagaimana dapat dilihat tabel 4.4 berikut)

- **Kerahasiaan (NC):** *Confidential* (3)
- **Integritas (NI):** *Major Disturbance* (2)
- **Ketersediaan (NA):** *High Availability* (2)

Langkah-langkah untuk menghitung Nilai Aset adalah:

- 1) Menggunakan rumus: Nilai Aset=NC+NI+NA
- 2) Nilai Aset=3+2+2=7
- 3) Dalam contoh ini, maka total nilai aset yang didapat adalah 7.

Tabel 4. 4 Analisis penilaian aset

Nama Aset	Nilai <i>Confidentiality</i> (NC)	Nilai <i>Integrity</i> (NI)	Nilai <i>Availability</i> (NA)	Nilai Aset
Data Aplikasi	3	2	2	7
Data informasi publik	2	3	3	8

Untuk hasil analisis aset Diskominfo Kota Mojokerto yang lebih detail, didapat dari hasil kuesioner dan wawancara dengan bidang staf aplikasi dan informasi dapat dilihat pada lampiran 8 (Tabel L8.4 Analisis Penilaian Aset).

A. Identifikasi Kelemahan dan Ancaman Aset

Tahapan selanjutnya adalah mengidentifikasi kelemahan dan ancaman pada masing-masing aset yang dimiliki oleh Bagian Aplikasi dan Infrastruktur Informasi

Diskominfo Kota Mojokerto. Langkah ini bertujuan untuk memahami risiko yang dihadapi dan merumuskan langkah mitigasi yang tepat. Sebagaimana dapat dilihat pada tabel 4.5

Tabel 4. 5 Identifikasi kelemahan dan ancaman pada aset

Nama Aset	Kelemahan (<i>Vulnerable</i>)	Ancaman (<i>Threat</i>)
Data Aplikasi	<ul style="list-style-type: none"> • <i>Software bug</i> • kerusakan pada perangkat <i>hardware</i> 	<ul style="list-style-type: none"> • Pencurian data • Hilangnya data
Data informasi publik	<ul style="list-style-type: none"> • <i>Software bug</i> • kerusakan pada perangkat <i>hardware</i> 	<ul style="list-style-type: none"> • Pencurian data • Hilangnya data

Untuk keterangan lebih lengkap mengenai kelemahan dan ancaman aset dapat ditemukan pada Lampiran 8 (Tabel L8.5 Identifikasi Kelemahan dan Ancaman pada Aset).

Setelah mengidentifikasi kelemahan dan ancaman pada aset, langkah selanjutnya yaitu mengklasifikasi setiap kelemahan dan ancaman sesuai dengan skala rentang nilai probabilitas.

Dengan mengklasifikasikan kelemahan dan ancaman menggunakan tabel nilai probabilitas, Diskominfo Kota Mojokerto dapat menetapkan prioritas yang tepat dan menerapkan langkah-langkah pengendalian yang efektif untuk meningkatkan keamanan sistem informasi mereka.

Tabel 4. 6 Tabel Nilai Rerata Probabilitas

Keterangan	Nilai Kemungkinan Kejadian
<i>LOW</i>	0.1 – 0.3
<i>MEDIUM</i>	0.4 – 0.6
<i>HIGH</i>	0.7 – 1.0

Sumber : (Sarno & Iffano, 2009)

Langkah berikutnya setelah mengidentifikasi ancaman dan kelemahan yaitu dapat dicari nilainya dengan menggunakan rumus persamaan sebagai berikut : (Sarno & Iffano, 2009)

$$\text{Nilai Ancaman (NT)} = \sum PO / \sum \text{Ancaman} \dots\dots\dots (4.2)$$

Keterangan:

Σ PO: Jumlah *Probability Occurrence* (Probabilitas Kejadian) dari ancaman yang teridentifikasi.

Σ Ancaman: Jumlah ancaman terhadap informasi

Contoh Penerapan:

Terdapat lima ancaman yang telah diidentifikasi dengan probabilitas kejadian pada aset Data Aplikasi sebagai berikut:

1. **Gangguan pada perangkat keras:** Probabilitas Kejadian = 0.3
2. **Software bug:** Probabilitas Kejadian = 0.2
3. **Human error:** Probabilitas Kejadian = 0.4
4. **Serangan virus:** Probabilitas Kejadian = 0.3
5. **penyalahgunaan hak akses:** Probabilitas Kejadian = 0.3

Langkah-langkah untuk menghitung Nilai Ancaman (NT) adalah:

- 1) **Hitung Jumlah Probabilitas Kejadian:**

$$\Sigma PO = 0.3 + 0.2 + 0.4 + 0.3 + 0.3 = 1.5$$

- 2) **Hitung Jumlah Ancaman:**

$$\Sigma \text{Ancaman} = 5 \text{ (Karena ada 5 ancaman)}$$

- 3) **Hitung Nilai Ancaman (NT):**

$$\text{Nilai Ancaman (NT)} = 1.5 / 5 = 0.3$$

- 4) **Interpretasi Nilai:**

Berdasarkan tabel nilai probabilitas, **0.3** termasuk dalam kategori **LOW**.

Dengan langkah-langkah ini, dapat ditentukan nilai tingkat ancaman yang dihadapi dan menentukan tindakan pengelolaan yang sesuai berdasarkan hasil perhitungan.

Untuk hasil identifikasi nilai ancaman pada aset Diskominfo Kota Mojokerto yang telah didapat dari hasil kuesioner dan wawancara dengan bidang staff aplikasi dan informasi dapat dilihat pada tabel 4.7

Tabel 4. 7 Identifikasi nilai ancaman pada aset Data Aplikasi

NO	Kejadian	Kategori	jenis probabilitas	rerata probabilitas
1	Gangguan pada perangkat keras	Kelemahan	<i>Low</i>	0,3
2	<i>Software bug</i>	Kelemahan	<i>Low</i>	0,2
3	<i>Human error</i>	Kelemahan	<i>Medium</i>	0,4
4	Serangan virus	Ancaman	<i>Low</i>	0,3
5	penyalahgunaan hak akses	Ancaman	<i>Low</i>	0,3
Jumlah kejadian = 5		Jumlah rerata probabilitas		1,5
NA = jumlah rerata probabilitas/ jumlah kejadian				0,3 (LOW)

Hasil penilaian yang lebih rinci mengenai identifikasi ancaman dan kelemahan aset Diskominfo Kota Mojokerto dapat ditemukan pada Lampiran 8, dari Tabel L8.6 (Nilai Ancaman Aset Data Aplikasi) hingga Tabel L8.15 (Nilai Ancaman Aset Firewall).

2. Analisis Dampak dan Risiko Aset

Setelah melakukan langkah analisis dari setiap kelemahan dan ancaman pada aset maka tahapan berikutnya yaitu melakukan observasi dan wawancara untuk menganalisis dampak bisnis, langkah ini bertujuan untuk menentukan seberapa berpengaruhnya ancaman atau kelemahan yang terjadi terhadap keberlangsungan proses bisnis pada bagian Aplikasi dan Infrastruktur Informasi Diskominfo Kota Mojokerto berdasarkan skala *Business Impact Analysis* (BIA) dengan menggunakan nilai skala berikut:

Tabel 4. 8 Tabel Skala *Business Impact Analysis* (BIA)

Batas Toleransi gangguan	Keterangan	Nilai skala
< 1 minggu	<i>Not critical</i>	0 - 20
1 hari - 2 hari	<i>Minor critical</i>	21 - 40
<1 hari	<i>Mayor critical</i>	41 - 60
< 12 jam	<i>High critical</i>	61 - 80
<1 jam	<i>Very High critical</i>	81 - 100

Berikut merupakan pemberian nilai *Business Impact Analysis* (BIA) melalui observasi dan wawancara dengan staff aplikasi dan infrastruktur Diskominfo Kota Mojokerto berdasarkan tabel skala pada setiap aset yang dimiliki

Tabel 4. 9 Penilaian Level Business Impact Analysis (BIA)

NO	NAMA ASET	NILAI BIA	ANALISIS DAMPAK DAN RISIKO	KETERANGAN
1.	Data aplikasi	70	<p>Dampak: Jika data aplikasi diakses oleh pihak yang tidak berwenang, dapat terjadi kebocoran informasi sensitif yang dapat merusak reputasi organisasi atau melanggar privasi.</p> <p>Risiko: Peretasan, kebocoran data, atau kesalahan konfigurasi yang mengakibatkan akses tidak</p>	<i>High critical</i>
2.	Data informasi publik	85	<p>Dampak: Jika data publik diubah, dapat menyebabkan informasi yang salah atau menyesatkan yang dapat mempengaruhi reputasi organisasi dan kepercayaan publik.</p> <p>Risiko: Manipulasi data oleh pihak tidak berwenang atau kesalahan pembaruan data.</p>	<i>High critical</i>

Untuk hasil penerapan nilai BIA yang lebih detail pada aset Diskominfo Kota Mojokerto dapat dilihat pada lampiran 8 (Tabel L8.16. Analisis Dampak dan Risiko aset Diskominfo Kota Mojokerto)

A. Nilai Dampak Bisnis Pada Aset

Tahap berikutnya setelah menentukan nilai BIA dari masing masing aset adalah menentukan nilai Dampak bisnis. Nilai dampak bisnis yang dihasilkan yaitu berasal dari hasil perhitungan Nilai Ancaman yang telah diidentifikasi sebelumnya dengan Identifikasi Nilai BIA.

Matriks Level Risiko menghubungkan probabilitas ancaman dengan dampak bisnis untuk mengkategorikan risiko. Nilai risiko dihitung dengan mengalikan probabilitas kejadian ancaman dengan dampak bisnis yang dihasilkan. Hasilnya membantu dalam menilai dan memprioritaskan risiko berdasarkan dampak yang mungkin terjadi pada aset. Dengan menggunakan tabel ini, Diskominfo dapat mengidentifikasi dan mengelola risiko secara efektif sesuai dengan tingkat risiko yang dihitung.

Tabel 4. 10 Tabel Matriks Level Risiko

Probabilitas ancaman	Dampak Bisnis (Impact)				
	Not Critical (20)	Low Critical (40)	Medium Critical (60)	High Critical (80)	Very High critical (100)
Low (0.1)	Low $20 \times 0.1 = 2$	Low $40 \times 0.1 = 4$	Low $60 \times 0.1 = 6$	Low $80 \times 0.1 = 8$	Low $100 \times 0.1 = 10$
Medium (0.5)	Low $20 \times 0.5 = 10$	Medium $40 \times 0.5 = 20$	Medium $60 \times 0.5 = 30$	Medium $80 \times 0.5 = 40$	Medium $100 \times 0.5 = 50$
High (1.0)	Medium $20 \times 1.0 = 20$	Medium $40 \times 1.0 = 40$	High $60 \times 1.0 = 60$	High $80 \times 1.0 = 80$	High $100 \times 1.0 = 100$

Sumber : (Sarno & Iffano, 2009)

Contoh Perhitungan dan langkah-langkah Perhitungan Level Risiko:

A. Identifikasi Probabilitas dan Dampak:

Terdapat ancaman Data Aplikasi yang memiliki probabilitas **Medium** (0.2) dan nilai BIA-nya (70)

B. Hitung Nilai Dampak Bisnis (impact):

- 1) Nilai Dampak = Nilai Ancaman \times Nilai BIA
- 2) Menggunakan contoh di atas: Nilai Dampak = $0.2 \times 70 = 14$
- 3) Berdasarkan nilai impact yang dihitung, dapat menentukan kategori risiko sesuai dengan tabel yaitu *Medium*.

Maka nilai dampak bisnis pada aset Diskominfo telah dievaluasi dan dirangkum dalam Tabel 4.11. Tabel ini menunjukkan penilaian aset terkait nilai ancaman, dampak bisnis, dan risiko, membantu menentukan prioritas pengelolaan dan perlindungan aset untuk keamanan sistem informasi Diskominfo Kota Mojokerto.:

Tabel 4. 11 Hasil Nilai Dampak Bisnis aset Diskominfo

NO	NAMA ASET	Nilai Ancaman	Nilai BIA	Dampak Bisnis (impact)	Keterangan
1	Data aplikasi	0,2	70	14	<i>Medium</i>
2	Data informasi publik	0,23	85	19,55	<i>Medium</i>

Untuk hasil lebih detail mengenai nilai dampak bisnis aset pada Diskominfo Kota Mojokerto dapat dilihat pada lampiran 8 (Tabel L8.17 Hasil penilaian dampak bisnis(*impact*)).

B. Menentukan Nilai Risiko dan Level Risiko Aset

Langkah berikutnya adalah menentukan nilai dan level risiko untuk setiap aset, menggunakan matriks level risiko. Tujuannya adalah mengidentifikasi risiko yang dapat diterima dan yang memerlukan pengelolaan lebih lanjut oleh Bagian Aplikasi dan Infrastruktur Informatika Diskominfo Kota Mojokerto. Berikut merupakan rumus persamaan untuk melakukan penilaian risiko:

$$\text{Nilai Risiko} = \text{NA} \times \text{BIA} \times \text{NT} \dots\dots\dots(4.3)$$

Keterangan :

NA : Nilai Aset

BIA : Analisis Dampak Bisnis

NT : Nilai Ancaman

Contoh Perhitungan dan langkah-langkah Perhitungan Nilai Risiko Data Aplikasi:

A. Identifikasi Probabilitas dan Dampak:

Terdapat ancaman Data Aplikasi yang memiliki nilai probabilitas **Medium** (0.5) dan dampaknya **High Critical** (80).

B. Hitung Nilai Risiko:

- 1) Nilai Risiko = Nilai Aset × BIA × Nilai Ancaman
- 2) Menggunakan contoh di atas: Nilai Risiko=7×70×0.3=98
- 3) Berdasarkan nilai risiko yang dihitung diperoleh nilai risiko pada Data Aplikasi yaitu 98, dapat menentukan kategori risiko sesuai dengan tabel yaitu *High*.

Berikut ini adalah penilaian *Business Impact Analysis* (BIA) yang diperoleh melalui observasi dan wawancara dengan staf aplikasi dan infrastruktur Diskominfo Kota Mojokerto berdasarkan skala pada setiap aset yang dimiliki:

Tabel 4. 12 Nilai Risiko dan Level Risiko aset

NO	NAMA ASET	Nilai Aset	Nilai BIA	Nilai Ancaman	Nilai Risiko	Level Risiko
1	Data Aplikasi	7	70	0,2	98	High
2	Data informasi publik	8	85	0,23	156,4	High

Untuk hasil lebih detail mengenai nilai dampak bisnis aset pada Diskominfo Kota Mojokerto dapat dilihat pada lampiran 8 (Tabel L8.18. Hasil identifikasi nilai risiko dan level risiko)

4.1.3 Tahapan *Check*

Pada Pada tahap check, auditor mengidentifikasi masalah sesuai dengan klausul ISO 27001:2013 yang dipilih. Proses ini mencakup verifikasi penerapan kebijakan, prosedur, dan kontrol keamanan informasi, serta memastikan semuanya berjalan sesuai standar berdasarkan bukti, wawancara, dan observasi lapangan untuk menilai kepatuhan dan efektivitas sistem manajemen keamanan informasi.

A. Pemilihan Kontrol Objektif Berdasarkan ISO 27001:2013

Pada tahap pemilihan kontrol sesuai ISO 27001:2013, identifikasi dan pemilihan kontrol keamanan dilakukan untuk mengatasi masalah pada website portal Diskominfo. Kontrol yang dipilih bertujuan untuk mengurangi risiko dan memastikan keamanan informasi, mencakup kerahasiaan, integritas, dan ketersediaan. Rincian kontrol terdapat pada Lampiran 8 (Tabel L8.19 Pemetaan Klausul pada ISO 27001:2013).

B. Memilih Klausul ISO 27001:2013

Berdasarkan hasil temuan dari identifikasi aset, risiko, ancaman, serta penilaian dampak terhadap bisnis (BIA) terdapat Aset dengan nilai risiko tinggi seperti Data Aplikasi, Data Informasi Publik, dan Aplikasi PPID menunjukkan bahwa ancaman terhadap kerahasiaan dan integritas informasi sangat signifikan. Tingginya nilai risiko pada aset-aset ini (seperti Aplikasi Website Pemkot dengan nilai risiko 216 dan Server dengan nilai risiko 345,95) menunjukkan bahwa pengendalian akses yang ketat sangat diperlukan untuk melindungi data dari akses tidak sah. Klausul 9 mengatur kebijakan dan prosedur kontrol akses yang penting untuk memastikan hanya pengguna yang berwenang yang dapat mengakses

informasi sensitif, memitigasi risiko terhadap kerahasiaan dan integritas data yang memiliki nilai risiko tinggi.

Adanya temuan audit mengungkapkan bahwa aset-aset seperti Data Aplikasi, Aplikasi PPID, dan Data Informasi Publik menghadapi risiko tinggi, terutama disebabkan oleh ancaman internal seperti kesalahan manusia dan kurangnya pelatihan keamanan informasi. Ketidakterlaksanaan pelatihan keamanan informasi SDM di Diskominfo Kota Mojokerto semakin menyoroti perlunya perlindungan yang lebih baik terhadap sumber daya manusia. Oleh karena itu, Klausul 7 dari ISO 27001:2013 menjadi sangat relevan karena mengatur tentang proses pelatihan, peningkatan kesadaran, dan pemeliharaan kompetensi SDM untuk memastikan bahwa personel yang menangani data dan sistem informasi memiliki pengetahuan dan keterampilan yang memadai untuk melindungi informasi dari ancaman internal dan mengurangi risiko yang ada.

Temuan terkait Aset dengan nilai risiko tinggi seperti Server (nilai risiko 345,95) dan Switch (nilai risiko 115,2) menunjukkan kebutuhan mendesak untuk menjaga infrastruktur fisik dan lingkungan agar tetap aman dan berfungsi dengan baik. Klausul 11 mencakup pemeliharaan dan perlindungan lingkungan fisik, yang penting untuk melindungi perangkat keras dari kerusakan dan ancaman fisik yang dapat mengganggu ketersediaan dan integritas data.

Hasil temuan ini, dapat dirinci lebih lanjut di Lampiran 8 (Tabel L8.20), yang menguraikan pemilihan klausul ISO 27001:2013 yang sesuai dengan hasil evaluasi tersebut.

Dengan temuan audit menunjukkan bahwa Klausul 7, 9, dan 11 merupakan area yang paling mendesak serta memerlukan tindakan segera untuk memastikan keamanan dan integritas sistem informasi perlu perhatian khusus karena langsung menangani kekurangan seperti kelemahan keamanan SDM, risiko akses tidak sah, dan kerusakan fisik pada infrastruktur TI.

C. Penilaian SSE-CMM

SSE-CMM adalah model referensi untuk meningkatkan dan menilai kapabilitas dalam domain keamanan teknologi informasi. Dengan tujuan memajukan praktik keamanan yang lebih terdefinisi dan terukur, serta mencakup praktik keamanan

untuk meningkatkan kualitas dan layanan dalam keamanan informasi. Terdapat lima tingkat dalam SSE-CMM:

Tabel 4. 13 Level tingkatan SSE-CMM

Deskripsi	Tingkat Kemampuan
<i>Performed Informally</i> (Dilakukan Informal)	1
<i>Planned and tracked</i> (Direncanakan dan dilacak)	2
<i>Well Defined</i> (Didefinisikan dengan baik)	3
<i>Quantitatively controlled</i> (Dikendalikan secara kuantitatif)	4
<i>Continuously improving</i> (Ditingkatkan terus-menerus)	5

(University, 2003).

Berikut adalah proses penilaian Klausul 9 mengenai Kontrol Akses yang dilakukan melalui evaluasi menggunakan metode SSE-CMM, dengan kuesioner dan wawancara bersama staf aplikasi dan infrastruktur di Diskominfo Kota Mojokerto:

Tabel 4. 14 Penilaian klausul menggunakan SSE-CMM Klausul 9

Klausul 9 Kontrol Akses										
A.9.1.1 Kebijakan kontrol akses										
NO	Pernyataan	Bobot	1	2	3	4	5	Nilai	Rerata	
1	Adanya pendokumentasian kontrol hak akses	1				✓		4		
2	Adanya pemeriksaan secara berkala terhadap kontrol akses	1				✓		4		
Total bobot		2	Tingkat kemampuan					8	4	

Dengan total bobot 2 dan skor kumulatif 8, tingkat kemampuan keseluruhan untuk kebijakan kontrol akses di Diskominfo Kota Mojokerto adalah terkendali secara kuantitatif, dengan skor rata-rata 4. Ini menunjukkan bahwa meskipun terdapat langkah-langkah yang diterapkan, masih ada ruang untuk peningkatan

dalam pendokumentasian dan proses pemeriksaan berkala untuk meningkatkan keamanan dan kepatuhan terhadap standar ISO 27001:2013.

Langkah ini membantu organisasi menilai dan meningkatkan kapabilitas keamanan mereka hingga mencapai tingkat yang diinginkan. Tahap penilaian SSE-CMM dapat dilihat pada lampiran 8 (Tabel L8.21 hingga Tabel L8.23).

4.1.4 Tahapan *Act*

Tahapan "*Act*" dalam PDCA adalah tahap akhir yang fokus pada perbaikan berdasarkan hasil "*Check*." Setelah mengevaluasi efektivitas, perubahan yang diperlukan diidentifikasi dan diterapkan, lalu didokumentasikan sebagai standar operasional baru dengan komunikasi efektif kepada tim dan pemangku kepentingan.

A. Penelusuran Bukti dan Gap

Pada Pada tahap ini, dilakukan penelusuran terhadap bukti-bukti implementasi dan identifikasi gap atau kekurangan dalam sistem manajemen keamanan informasi melalui observasi dan wawancara.

Tabel 4.16 Hasil Penelusuran Bukti dan Gap (Klausul 9: Kontrol Akses)

Klausul 9 Kontrol Akses				
Deskripsi Tugas	Dilaksanakan		Bukti	Gap
	Ya	Tidak		
Pemilik aset menentukan aturan hak akses yang tepat	✓		Data OPD disimpan di server DISKOMINFO Kota Mojokerto dengan kebijakan akses yang mengatur data mana yang dapat diakses atau tidak.	
Adanya aturan kontrol akses yang bersifat fisik dan logis		✓		Menetapkan kebijakan akses fisik dan logis untuk melindungi data, memastikan hanya pihak berwenang yang dapat mengakses sistem.

Untuk hasil lebih detail mengenai hasil penelusuran bukti dan gap pada Diskominfo Kota Mojokerto dapat dilihat pada lampiran 9 (Tabel L9.1 Hasil Penelusuran Bukti dan Gap).

B. Pemetaan Permasalahan dan Pemberian Rekomendasi

Setelah dianalisis bukti dan gap pada setiap klausul, termasuk kontrol keamanan dan kontrol objektif, maka pada tahap ini setiap permasalahan akan diberi rekomendasi usulan baik berupa SOP maupun kebijakan baru untuk memaksimalkan kinerja organisasi dan meminimalisir risiko terjadinya dampak keamanan sistem informasi.

Tabel 4. 15 Pemetaan hasil rekomendasi (Klausul 9: Pengendalian Hak Akses)

Kontrol ISO	Kontrol Objektif	Petunjuk Pelaksanaan	Keamanan yang diterapkan	Hasil Rekomendasi
Klausul 9 Pengendalian Hak Akses	Kebijakan untuk mengontrol hak akses	pembatasan akses data atau layanan	Instansi membedakan hak akses untuk masing-masing pegawai sesuai dengan unit kerja dan fungsinya	Membuat aturan yang jelas dan tertulis mengenai hak akses terhadap asset sistem informasi

Untuk penjelasan lebih detail mengenai rekomendasi pada Diskominfo Kota Mojokerto dapat dilihat pada lampiran 10 (Tabel L10.1 Pemetaan Rekomendasi Berdasarkan Klausul ISO 27001:2013).

C. Perencanaan Pembuatan Prosedur

Pada tahap ini auditor akan menyusun Standar Operational Prosedur (SOP) mulai dari kebijakan, prosedur, instruksi kerja, dan lembar kerja.

1.) Penyusunan SOP

Setelah melakukan pemetaan rekomendasi, maka selanjutnya akan didefinisikan ke beberapa prosedur. Berikut adalah pemetaan kebijakan dengan dokumen prosedur, instruksi kerja, dan formulir yang dihasilkan.

Tabel 4. 16 Penyusunan rangkaian SOP Pada Klausul 9

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB-02 Kontrol Hak Akses	PO – 02 Prosedur Pengelolaan Hak Akses	IK – 01 Pengelolaan Hak Akses	FM-03 Pengelolaan Hak Akses

Keterangan:

KB: Kebijakan

PO: Prosedur

IK: Instruksi Kerja

FM: Formulir.

Berdasarkan hasil pemetaan risiko ISO 27001:2013, didapatkan 3 kebijakan, 4 prosedur, 5 instruksi kerja, dan 13 rekam kerja berupa formulir. Kebijakan dan prosedur tersebut disusun berdasarkan rekomendasi pengendalian risiko dan risiko yang terjadi. Penjelasan dan pembentukan prosedur dapat dilihat pada lampiran 11 (Tabel L11.2 Pengelompokan kebijakan dengan prosedur, instruksi kerja, dan formulir).

2.) Hasil Penyusunan Kebijakan

Hasil dari penyusunan kebijakan ini berguna sebagai pendukung pelaksanaan SOP yang juga membutuhkan dokumen-dokumen pendukung seperti rekam kerja. Berikut merupakan tabel perencanaan kebijakan. Untuk detailnya dapat dilihat pada lampiran 12.

DINAS KOMUNIKASI DAN INFORMATIKA KOTA MOJOKERTO



DINAS KOMUNIKASI & INFORMATIKA
KOTA MOJOKERTO

KB - 01

No. Rilis :

No. Revisi :

Kebijakan Pengendalian Hak Akses

Tanggal Terbit

1 . Tujuan: Kebijakan berikut ini dibuat untuk menjamin persyaratan pengendalian hak akses terhadap informasi dan fasilitas informasi yang dimiliki agar dapat didefinisikan dengan cepat

A. Kebijakan

1. Pengelolaan hak akses sistem informasi
 2. Hak akses pada setiap sistem informasi yang terkait dengan informasi instansi harus dibedakan sesuai peran dan fungsi dari masing – masing pengguna
-

B. Dokumen terkait

PO – 01 Prosedur Pengelolaan Hak Akses

Gambar 4. 1 Hasil perencanaan kebijakan

3.) Hasil Perencanaan Prosedur


Tahap ini bertujuan untuk mendukung pelaksanaan SOP yang dimana membutuhkan dokumen-dokumen pendukung yaitu instruksi kerja yang digunakan sebagai acuan pada setiap langkah-langkah yang dilakukan. Untuk hasil dari perencanaan prosedur dapat dilihat pada lampiran 13.

 DINAS KOMUNIKASI & INFORMATIKA KOTA MOJOKERTO	<u>Nomor SOP</u>	<u>PO – 01</u>	
	Tgl. Pembuatan		
Disahkan Oleh :			
Nama SOP : PERENCANAAN HAK AKSES			
DESKRIPSI SOP	KLASIFIKASI	DAN	DAFTAR
Prosedur pengelolaan hak akses merupakan prosedur untuk penggunaan hak akses terhadap sistem informasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun dari luar instansi.	PELAKSANAAN	DAFTAR PELAKSANAAN	
		<ol style="list-style-type: none"> 1. Pengguna sistem (staff pegawai) 2. Kepala seksi 3. Kepala persandian dan keamanan informasi 	

Gambar 4. 2 Hasil perencanaan prosedur

4.) Hasil Perencanaan Instruksi Kerja

Hasil dari penyusunan instruksi kerja ini bertujuan untuk mendukung pelaksanaan SOP yang dimana membutuhkan dokumen instruksi kerja yang berguna untuk mendokumentasikan aktivitas. Untuk hasil perencanaan instruksi kerja dapat dilihat pada lampiran 14.


 DINAS KOMUNIKASI & INFORMATIKA KOTA MOJOKERTO	<u>LK-01</u>
	Instruksi Kerja Pemberian Hak Akses
Tanggal Terbit:	
1. PELAKSANA	

2. RINCIAN INSTRUKSI KERJA		
Pegawai mengajukan permintaan pemberian hak akses baru melalui email		
No.	Tanggal Revisi	Uraian Revisi

Gambar 4. 3 Hasil perencanaan kebijakan

5.) Hasil Perencanaan Rekam Kerja

Hasil dari penyusunan prosedur ini bertujuan untuk mendukung pelaksanaan SOP yang dimana membutuhkan dokumen rekam kerja yang berguna untuk mendokumentasikan aktivitas yang mendukung SOP. Untuk hasil dari perencanaan instruksi kerja dapat dilihat pada lampiran 15.



**DINAS KOMUNIKASI & INFORMATIKA
KOTA MOJOKERTO**

Dinas Komunikasi dan Informatika Kota Mojokerto

FM – 01	NO.RILIS	: 00
	NO. REVISI	: 00
FORMULIR PENGELOLAAN HAK AKSES	TANGGAL TERBIT	: 00
	HALAMAN	: 01

FORMULIR PENGHAPUSAN HAK AKSES

IDENTITAS PEGAWAI:

Nama Pegawai _____

NIP _____

Jabatan _____

Email _____

No.Hp _____

Permintaan Hak Akses : _____

Disetujui Oleh: _____ Diketahui Oleh: _____

(ttt)

(ttt)

Gambar 4. 4 Hasil perencanaan rekam kerja

4.5 Tahap Akhir

Hasil dari tahapan ini adalah rekomendasi untuk peningkatan kinerja organisasi dan pengurangan risiko gangguan keamanan sistem informasi.

A. Hasil Analisis

Berdasarkan proses audit, dari analisis awal hingga kesimpulan, ditemukan bahwa Dinas Komunikasi dan Informatika Kota Mojokerto perlu melakukan perubahan dan penambahan sistem untuk meningkatkan kinerja organisasi. Tahapan analisis dimulai dengan identifikasi dan peninjauan kondisi awal keamanan informasi, diikuti dengan analisis proses bisnis untuk mengkaji kelemahan dan potensi risiko. Selanjutnya, pengumpulan bukti dilakukan melalui wawancara dan observasi langsung untuk mengevaluasi implementasi kebijakan dan prosedur keamanan informasi. Kesimpulan dari audit ini menunjukkan perlunya perubahan dalam bentuk *Standar Operasional Prosedur (SOP)* dan prosedur kerja agar kinerja organisasi lebih optimal dan tidak mengganggu proses bisnis lainnya.

Penelitian ini menghasilkan rekomendasi yang lebih rinci berupa 3 kebijakan baru yang mencakup panduan keamanan informasi secara umum, manajemen risiko, dan tanggap darurat. Selain itu, disusun 4 prosedur kerja yang meliputi prosedur pengelolaan akses, pelaporan insiden keamanan, manajemen perubahan, dan audit internal. Untuk mendukung pelaksanaan prosedur kerja, dibuat 5 instruksi kerja yang memberikan langkah-langkah operasional detail terkait backup data, pengelolaan perangkat keras, kontrol akses fisik, penanganan data sensitif, dan pelatihan keamanan informasi. Selain itu, terdapat 13 rekam kerja yang mencatat pelaksanaan harian dari kebijakan dan prosedur tersebut, seperti log akses, laporan insiden, catatan audit, dan daftar perangkat keras dan perangkat lunak yang digunakan. Semua rekomendasi ini telah disesuaikan dengan klausul ISO 27001:2013 untuk memastikan kepatuhan terhadap standar internasional dalam manajemen keamanan informasi.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Hasil penelitian dari pengerjaan tugas akhir sesuai dengan metode pelaksanaan yang telah direncanakan memberikan kesimpulan sebagai berikut:

1. Hasil pengukuran *maturity level* SSE-CMM menunjukkan bahwa klausul 7 keamanan sumber daya manusia di Diskominfo Kota Mojokerto, dengan *nilai maturity level* 3,9, berada di level *Defined*, yang artinya proses ini sudah terstruktur dengan baik namun masih memerlukan peningkatan. Klausul 9 mengenai kontrol hak akses, dengan nilai *maturity level* 4,42, berada di level *Quantitatively Managed*, yang menunjukkan bahwa proses ini dikelola secara kuantitatif dan efektif. Sementara itu, klausul 11 keamanan fisik dan lingkungan, dengan *nilai maturity level* 4,8, berada di level *Optimizing*, mencerminkan kematangan tinggi dan komitmen terhadap perbaikan berkelanjutan.
2. Hasil penelitian ini menghasilkan 3 kebijakan, 4 prosedur, 5 instruksi kerja, dan 13 formulir untuk memperkuat keamanan informasi dan memastikan kepatuhan Diskominfo Kota Mojokerto terhadap standar ISO 27001:2013 dengan tujuan menciptakan sistem yang teratur dan mudah diikuti sehingga pengelolaan keamanan informasi menjadi lebih efektif dan efisien serta penguatan langkah-langkah penanganan risiko guna memastikan tingkat keamanan informasi yang optimal di masa depan.

5.2 Saran

Dinas Kominfo Kota Mojokerto disarankan untuk memperluas perhatian pada 11 Klausul ISO 27001:2013 lainnya. Penerapan keseluruhan klausul ini akan mendukung peningkatan efisiensi sistem keamanan informasi dan memastikan bahwa kebijakan yang diterapkan sejalan dengan visi dan misi Diskominfo untuk menyediakan layanan informasi yang aman dan terpercaya.

Selain itu, disarankan untuk menambahkan analisis dampak biaya kerugian, memperbaharui SOP sesuai perkembangan teknologi, dan melibatkan evaluasi serta

implementasi langsung dalam proses bisnis untuk memastikan efisiensi dan adaptasi yang berkelanjutan.



UNIVERSITAS
Dinamika

DAFTAR PUSTAKA

- Arens, A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2014). *Auditing and Assurance Services: An Integrated Approach*. Pearson Education Limited.
- Arnason, S. T., & Willet, K. (2008). *How To Achieve 27001 Certification: An Example of Applied Compliance Management* (Boca Raton). Auerbach Publications.
- Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C. (2017). Evaluasi Manajemen Keamanan Informasi pada DPTSI ITS Surabaya. *Jurnal Teknik Its*, 6(1), 122–128. <https://www.neliti.com/publications/193043/evaluasi-manajemen-keamanan-informasi-menggunakan-indeks-keamanan-informasi-kami>
- BSN. (2009). *Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan*.
- Budiarto, R. (2017). MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI MENGGUNAKAN METODE FMEA DAN ISO 27001 PADA ORGANISASI XYZ. *Journal of Computer Engineering, System and Science*.
- Chazar, C. (2017). Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005. *Jurnal Informasi*, VII(2), 48–57.
- Firmansyah, M. B. (2018). Manajemen Keamanan Informasi di Perpustakaan Menggunakan. *Media Pustakawan*, 25(1), 46–53.
- Gantz, S. D. (2014). *The Basics of IT Audit. Purposes, Processes, and Practical Information*.
- Gondodiyoto, S. (2006). *Audit Sistem Informasi*.
- IBISA. (2011). *Keamanan Sistem Informasi* (ANDI (ed.)).
- Ibrachim, N., Wiryana, I. M., Hadiyono, A., Wati, S., Andriansyah, M., Musawir, A., Wibowo, B. E., Tjenreng, M. I. B., Meidyasari, W. A., & Widyatmoko, K. (2012). *Bakuan Audit Keamanan Informasi Kemenpora. Bakuan Audit Keamanan Informasi Kemenpora*, 98 + xii.
- ISO. (2008). “International Standard ISO/IEC 27005 Information Technology. Security techniques”.” *Information Security Risk Management*.
- ISO. (2013). “International Standard ISO/IEC 27001 Information Technology - Security Techniques”. *Information Security Management Systems - Requirements*.
- Klaic, A. (2010). *Overview of the state and trends in the contemporary information*

security policy and information security management methodologies.

KOMINFO Direktorat Keamanan Informasi. (2017). *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)*. September, 1–74.

Kristanto, A. (2003). *Perancangan Sistem Informasi dan Aplikasinya*. Gava Media.

Nopriandi, H. (2018). Perancangan Sistem Informasi Registrasi Mahasiswa. *Jurnal Teknologi Dan Open Source*, 1(1), 73–79. <https://doi.org/10.36378/jtos.v1i1.1>

O'Brien, J. A. (2016). *Analisa Sistem Informasi. Ed 1*. Andy.

Sarno, R., & Iffano. (2009). *Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*. ITS Press.

Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECS-IJENS*, 11(5), 23–29.

University, C. M. (2003). *systems Security Engineering Capability Maturity Model SSE-CMM Version 3.0*. Carnegie Mellon University.

Weber, R. (1999). *Information Systems Control And Audit*.

Whitman, M., & Herbert, M. . (2014). *Management of Information Security*. Cengage Learning.

Winarno, W. W., & Amborowati, A. (2017). Tata Kelola Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5. –*Sentra Penelitian Engineering Dan Edukasi*.

Zen, A. (2016). *Ini yang Ditulis Peretas Website Pemkot Mojokerto*. Okezone. <https://news.okezone.com/read/2016/06/01/519/1403463/ini-yang-ditulis-peretas-website-pemkot-mojokerto>

Zulianto, A., Maulana, A., & Wahyudi, H. (2020). Audit Keamanan Sistem Informasi Manajemen Akademik Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013 (Studi Kasus STMIK Mardira Indonesia). *Jurnal Computech & Bisnis*, 14(1), 40–46.