

**ANALISIS MANAJEMEN INSIDEN KEAMANAN INFORMASI
MENGUNAKAN STANDAR ISO 27002:2013 (STUDI KASUS: DINAS
KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR)**

SKRIPSI



Oleh :

ANNISA DWI PUSPITARINI

NPM. 19081010003

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2023**

**ANALISIS MANAJEMEN INSIDEN KEAMANAN INFORMASI
MENGUNAKAN STANDAR ISO 27002:2013 (STUDI KASUS: DINAS
KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR)**

SKRIPSI

Diajukan Untuk Memenuhi Sebagai Persyaratan Dalam Menempuh Gelar Sarjana Komputer
Program Studi Informatika



Oleh :

ANNISA DWI PUSPITARINI

NPM. 19081010003

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2023

LEMBAR PENGESAHAN SKRIPSI

**Judul : ANALISIS MANAJEMEN INSIDEN KEAMANAN INFORMASI
MENGUNAKAN STANDAR ISO 27002:2013 (STUDI KASUS:
DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA
TIMUR)**

**Oleh : ANNISA DWI PUSPITARINI
NPM : 19081010003**

Telah Diseminarkan Dalam Ujian Skripsi Pada :


Hari Jumat, Tanggal 17 Maret 2023

Mengetahui

Dosen Pembimbing

Dosen Penguji

1.


Budi Nugroho, S.Kom., M.Kom
NIP. 19800907 2021211 005

1.


Eva Yulia Puspaningrum, S.Kom., M.Kom
NIP. 19890705 2021212 002

2.


M. Muharrom Al Haromainy, S.Kom., M.Kom
NIP. 19950601 2022031 006

2.


Firza Prima Aditiawan, S.Kom., MTI
NIP. 19860523 2021211 003

Menyetujui

**Dekan
Fakultas Ilmu Komputer**

**Koordinator Program Studi
Informatika**


Dr. Ir. Novirina Hendrasarie, MT.
NIP. 19681126 199403 2 001


Fetty Tri Anggrahny, S.Kom., M.Kom
NIP. 19820211 2021212 005

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Informatika UPN “Veteran” Jawa Timur, yang bertandatangan dibawah ini:

Nama : Annisa Dwi Puspitarini

NPM : 19081010003

Menyatakan bahwa Judul Skripsi / Tugas Akhir yang Saya ajukan dan akan dikerjakan, yang berjudul:

“ANALISIS MANAJEMEN INSIDEN KEAMANAN INFORMASI MENGGUNAKAN STANDAR ISO 27002:2013 (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR)”

Bukan merupakan plagiat dari Skripsi / Tugas Akhir / Penelitian orang lain dan juga bukan merupakan produk dan atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi / Tugas Akhir ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN “Veteran” Jawa Timur maupun institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 17 Maret 2023
Hormat Saya,



Annisa Dwi Puspitarini
NPM. 19081010003

**ANALISIS MANAJEMEN INSIDEN KEAMANAN INFORMASI
MENGUNAKAN STANDAR ISO 27002:2013 (STUDI KASUS: DINAS
KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR)**

Nama Mahasiswa : Annisa Dwi Puspitarini

NPM : 19081010003

Program Studi : Informatika

Dosen Pembimbing : Budi Nugroho, S.Kom. M.Kom.

Muhammad Muharrom Al Haromainy, S.Kom. M.Kom.

Abstrak

Manajemen insiden keamanan informasi perlu dilakukan oleh instansi pemerintahan untuk menjamin pengamanan kerahasiaan data, integritas informasi, dan ketersediaan informasi. Berkembangnya teknologi menjadikan instansi pemerintahan juga melakukan pelayanan dengan memanfaatkan teknologi digital dan berusaha untuk menerapkan *e-government* yang menjadikan resiko insiden keamanan informasi semakin meningkat.

Beberapa penelitian terdahulu telah dilakukan untuk meningkatkan manajemen insiden keamanan informasi pada berbagai instansi pemerintahan yang bergerak di bidang teknologi dan informasi. Kerangka kerja atau *framework* yang digunakan dalam melakukan audit tersebut beragam dengan tingkat standar yang berbeda, seperti COBIT, ISO 27001, ISO 27002, dan Indeks KAMI. Standar COBIT dan ISO 27001 banyak digunakan dalam penelitian audit teknologi informasi karena berstandar internasional, sedangkan Indeks KAMI merupakan alat ukur berstandar nasional untuk mempersiapkan suatu instansi melakukan manajemen keamanan.

ISO 27002 dinilai sangat efektif dalam menganalisis insiden keamanan informasi karena merupakan pengembangan dan penyempurnaan dari standar ISO 27001 yang berfokus pada penerapan, pemeliharaan, dan perbaikan manajemen keamanan informasi untuk meningkatkan kualitas sistem keamanan dan mengurangi resiko terjadinya pencurian data. Pada penelitian ini dilakukan analisis manajemen insiden keamanan informasi menggunakan standar ISO 27002:2013 dengan fokus kontrol Klausul 16 yaitu Manajemen Insiden Keamanan Informasi. Hasil penelitian yang didapat adalah penerapan manajemen insiden keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada level 4 dengan pemberian rekomendasi yang berfokus pada kontrol dengan nilai kematangan rendah yaitu kontrol 16.1.1, 16.1.2, 16.1.3, dan 16.1.4. Selain itu juga diberikan rekomendasi perbaikan atas aset-aset teknologi informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur yang memiliki tingkat resiko tinggi beserta perancangan sistem untuk meningkatkan keamanan informasi menggunakan *honeypot*.

Kata kunci: *Manajemen Insiden Keamanan Informasi, COBIT, ISO 27001, ISO 27002, Indeks KAMI*

KATA PENGANTAR

Alhamdulillah, puji syukur kehadiran Allah SWT, yang telah melimpahkan rahmat, hidayah serta karunia-Nya, sehingga penulis dapat menyelesaikan Skripsi dengan judul : “Analisis Manajemen Insiden Keamanan Informasi Menggunakan ISO 27002:2013 (Studi Kasus: Dinas Komunikasi dan Informatika Provinsi Jawa Timur)”, sebagai salah satu syarat untuk menyelesaikan pendidikan Sarjana (S1) pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.

Penulis menyadari bahwa penulisan skripsi ini masih jauh dari sempurna karena keterbatasan kemampuan dan pengetahuan yang dimiliki penulis. Oleh karena itu, penulis sangat mengharapkan masukan, kritik, dan saran yang dapat membangun dan berharap semoga laporan Skripsi ini dapat memberikan manfaat bagi pembaca, penulis dengan penelitian terkait, serta bagi penggunaanya untuk perkembangan ilmu pengetahuan.

Surabaya, 17 Maret 2023

Annisa Dwi Puspitarini

UCAPAN TERIMA KASIH

Dalam penyelesaian studi dan penulisan Skripsi ini, penulis banyak memperoleh bantuan baik pengajaran, bimbingan dan arahan dari berbagai pihak baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa dalam proses penulisan Skripsi ini banyak mengalami kendala, namun berkat bantuan, bimbingan, dukungan, doa dari orang tua saya, terutama ibu saya yang selalu mendampingi, kerjasama dari berbagai pihak, dan juga berkah dari Allah SWT yang selalu menyertai sehingga kendala-kendala yang dihadapi tersebut dapat teratasi. Untuk itu penulis menyampaikan rasa hormat dan terima kasih kepada:

1. Ibu Dr. Ir. Novirina Hendrasarie, MT selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
2. Ibu Fetty Tri Anggraeny, S.Kom, M.Kom selaku Koordinator Program Studi Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Bapak Budi Nugroho, S.Kom, M.Kom, selaku Dosen Pembimbing Pertama yang selalu memberi banyak masukan dan memberikan solusi ketika terdapat permasalahan dalam pengerjaan skripsi dan pembuatan laporan skripsi hingga selesai.
4. Bapak Muhammad Muharrom Al Haromainy, S.Kom. M.Kom selaku Dosen Pembimbing Kedua yang telah banyak memberi referensi dan masukan yang sangat berharga dalam menyelesaikan skripsi ini hingga selesai
5. Bapak Agung Mustika, S. Kom, M. Kom selaku koordinator skripsi Jurusan Informatika yang membantu proses administrasi dan keberlangsungan sidang proposal dan lisan.
6. Ibu Eva Yulia Puspaningrum, S.Kom., M.Kom dan Bapak Firza Prima Aditiawan, S.Kom., MTI selaku Dosen Penguji yang telah memberikan banyak saran dan masukan untuk perbaikan dan kesempurnaan penulisan skripsi ini hingga selesai.
7. Bapak Taufiq Ramadhan, ST. selaku narasumber yang membantu proses pengambilan data dan pengisian kuisisioner terkait insiden keamanan teknologi informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

8. Saudara Erik Prasetyo Nugroho yang telah menemani dan mendengarkan lika liku proses pengerjaan skripsi hingga selesai.
9. Teman-teman jurusan Informatika, serta semua pihak yang telah membantu proses perkuliahan di Informatika yang tidak bisa penulis sebutkan satu persatu

Terima kasih untuk semua pihak yang telah membantu, membimbing dan memberikan motivasi pengerjaan skripsi ini. Semoga Allah SWT selalu memberikan rahmat dan hidayah-Nya kepada kita semua, *Aamiin Yaa Rabbal'Aalamiin*.

DAFTAR ISI

DAFTAR ISI.....	vii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xiii
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	4
1.3. Batasan Masalah.....	5
1.4. Tujuan Penelitian.....	5
1.5. Manfaat Penelitian.....	6
BAB 2 TINJAUAN PUSTAKA	7
2.1. Penelitian Terdahulu.....	7
2.2. Landasan Teori	13
2.2.1. Keamanan Informasi	13
2.2.2. Sistem Informasi.....	14
2.2.3. Audit.....	14
2.2.4. Sistem Manajemen Keamanan Informasi (SMKI)	15
2.2.5. (Internasional Organisation for Standardization ISO)/(Internasional Electrotechnical Commission) IEC.....	15
2.2.6. ISO/IEC 27002:2013	16
2.2.7. Uji Kematangan.....	24
2.2.8. Analisis Gap	25
2.2.9. Honeypot	26

2.3.	Gambaran Umum Dinas Komunikasi dan Informatika Provinsi Jawa Timur	27
2.3.1.	Profil Dinas Komunikasi dan Informatika Provinsi Jawa Timur	27
2.3.2.	Tugas dan Fungsi Dinas Komunikasi dan Informatika Provinsi Jawa Timur.....	28
2.3.3.	Visi dan Misi Dinas Komunikasi dan Informatika Provinsi Jawa Timur	29
2.3.4.	Struktur Organisasi.....	29
BAB 3 METODOLOGI.....		31
3.1.	Metodologi Penelitian	31
3.2.	Perencanaan.....	31
3.3.	Persiapan	33
3.4.	Pelaksanaan	35
3.5.	Metode Pengumpulan Data	35
3.6.	Metode Analisis Manajemen Keamanan Informasi	36
3.7.	Metode Analisis Dampak Sistem Strategis	37
3.8.	Hasil	39
BAB 4 HASIL DAN PEMBAHASAN.....		40
4.1.	Pemilihan <i>Control Objective</i> dan Klausul Keamnan Informasi..	40
4.1.1.	Hasil Pemilihan <i>Control Objective</i> dan Klausul ISO 27002:2013.....	40
4.2.	Proses <i>Assessment</i> Penerapan Insiden Keamanan Informasi Berdasarkan ISO 27002:2013.....	42
4.2.1.	Penentuan <i>Auditee</i>	42

4.2.2.	Pelaksanaan <i>Assessment</i> Penerapan	43
4.3.	Analisis <i>Maturity Level</i> dan GAP	51
4.3.1.	<i>Assessment Maturity Level</i>	51
4.3.2.	Perhitungan <i>Maturity Level</i>	63
4.3.3.	Analisis Gap	65
4.4.	Analisis Dampak Sistem Strategis	67
4.4.1.	Identifikasi Aset	67
4.4.2.	Identifikasi Kelemahan dan Ancaman	68
4.4.3.	Identifikasi Resiko	70
4.4.4.	Identifikasi Dampak Sistem Strategis	71
4.4.5.	Hasil Analisis Dampak Sistem Strategis	71
4.5.	Rekomendasi Perbaikan	76
4.5.1.	Rekomendasi Perbaikan terhadap <i>Control Objective</i> Manajemen Insiden Keamanan Informasi berdasarkan ISO 27002:2013	76
4.5.2.	Rekomendasi Perbaikan Dampak Sistem Strategis pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur	82
4.6.	Perancangan Sistem	85
4.6.1.	Rancangan <i>Honeypot</i>	87
4.6.2.	Perancangan Perangkat Keras	88
4.6.3.	<i>Flowchart</i> Diagram Perancangan Sistem	89
4.6.4.	<i>Use Case</i> Diagram Perancangan Sistem	90
4.6.5.	<i>Sequence</i> Diagram Perancangan Sistem	91
4.6.6.	<i>Entity Relationship Diagram</i> Perancangan Sistem	93

4.6.7.	<i>Conceptual Data Model (CDM) Diagram Perancangan</i>	
	Sistem	94
BAB 5	PENUTUP.....	96
5.1.	Kesimpulan.....	96
5.2.	Saran.....	97
DAFTAR	PUSTAKA	98
LAMPIRAN	103

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu Tentang Analisis Keamanan Informasi Menggunakan Kerangka Kerja ISO 27002	8
Tabel 2.2 Struktur Kendali Keamanan ISO/IEC 27002:2013	17
Tabel 2.3 Rentang Nilai Kematangan Keamanan Informasi	24
Tabel 3.1 Klausul dan Kontrol objektif yang Digunakan	33
Tabel 3.2 Jadwal Penelitian	34
Tabel 4.1 Hasil Pemilihan <i>Control Objective</i> dan Klausul ISO 27002:2013	41
Tabel 4.2 Penentuan <i>Auditee</i>	43
Tabel 4.3 Hasil <i>Assessment</i> Penerapan Panduan ISO 27002:2013 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.....	44
Tabel 4.4 Hasil <i>Assessment Maturity Level</i> Manajemen Insiden Keamanan Informasi berdasarkan ISO 27002:2013.....	53
Tabel 4.5 Hasil Perhitungan <i>Maturity Level</i>	64
Tabel 4.6 Analisis GAP	66
Tabel 4.7 Hasil Identifikasi Aset	68
Tabel 4.8 Identifikasi Kelemahan	70
Tabel 4.9 Identifikasi Ancaman.....	70
Tabel 4.10 Identifikasi Resiko	71
Tabel 4.11 Identifikasi Dampak Sistem Strategis.....	72
Tabel 4.12 Hasil Analisis Dampak Sistem Strategis	73
Tabel 4.13 Rekomendasi Perbaikan Kontrol 16.1.1	78
Tabel 4.14 Rekomendasi Perbaikan Kontrol 16.1.2	80
Tabel 4.15 Rekomendasi Perbaikan Kontrol 16.1.3	81

Tabel 4.16 Rekomendasi Perbaikan Kontrol 16.1.4	82
Tabel 4.17 Rekomendasi Perbaikan Dampak Sistem Strategis pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur	83

DAFTAR GAMBAR

Gambar 2.1 Dinas Komunikasi dan Informatika Provinsi Jawa Timur.....	27
Gambar 2.2 Struktur Organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur	29
Gambar 3.1 Kerangka Kerja Penelitian	31
Gambar 4.1 Grafik Hasil <i>Maturity Level</i>	65
Gambar 4.2 Grafik Hasil Analisis Gap	67
Gambar 4.3 Rancangan Sistem Honeypot	88
Gambar 4.4 Flowchart Diagram Perancangan Sistem	90
Gambar 4.5 Use Case Diagram Perancangan Sistem.....	91
Gambar 4.6 Sequence Diagram Perancangan Sistem	93
Gambar 4.7 Entity Relationship Diagram (ERD) Perancangan Database Sistem	95
Gambar 4.8 Conceptual Data Model (CDM) Diagram Perancangan Database Sistem.....	96