

**ANALISA KESADARAN KEAMANAN INFORMASI
CUSTOMER SERVICES DENGAN METODE
FAILURE MODE AND EFFECT ANALYSIS
FRAMEWORK ISO/IEC 27001:2013**

SKRIPSI



Disusun oleh:

**Amru Rizal Fakhriansyah Susilo
17.83.0091**

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

**ANALISA KESADARAN KEAMANAN INFORMASI
CUSTOMER SERVICES DENGAN METODE
FAILURE MODE AND EFFECT ANALYSIS
FRAMEWORK ISO/IEC 27001:2013**

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Amru Rizal Fakhriansyah Susilo
17.83.0091

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISA KESADARAN KEAMANAN INFORMASI
CUSTOMER SERVICES DENGAN METODE
FAILURE MODE AND EFFECT ANALYSIS
FRAMEWORK ISO/IEC 27001:2013**

yang dipersiapkan dan disusun oleh

Amru Rizal Fakhriansyah Susilo

17.83.0091

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 Januari 2021

Dosen Pembimbing,


Dony Ariyus, M.Kom

NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

**ANALISA KESADARAN KEAMANAN INFORMASI
CUSTOMER SERVICES DENGAN METODE
FAILURE MODE AND EFFECT ANALYSIS
FRAMEWORK ISO/IEC 27001:2013**

yang dipersiapkan dan disusun oleh

Amru Rizal Fakhriansyah Susilo

17.83.0091

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Februari 2021

Nama Penguji	Susunan Dewan Penguji	Tanda Tangan
<u>Dony Ariyus, M.kom</u> NIK. 190302128		
<u>Melwin Syafrizal, S.Kom., M.Eng</u> NIK. 190302105		
<u>Joko Dwi Santoso, M.Kom</u> NIK. 190302181		

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Februari 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Amru Rizal Fakhriansyah Susilo
NIM : 17.83.0091

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISA KESADARAN KEAMANAN INFORMASI CUSTOMER SERVICES DENGAN METODE FAILURE MODE AND EFFECT ANALYSIS FRAMEWORK ISO/IEC 27001:2013

Dosen Pembimbing : Dony Ariyus, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 Februari 2021

Yang Menyatakan,



Amru Rizal Fakhriansyah Susilo

HALAMAN MOTTO

Jangan pergi mengikuti kemana jalan akan berujung. Buat jalanmu sendiri dan tinggalkanlah jejak. (Ralph Waldo Emerson)



HALAMAN PERSEMBAHAN

Sujud syukur kepada Allah, Tuhan Yang Maha Agung dan Maha Tinggi. Atas kehendakmu saya bisa menjadi pribadi yang berpikir, berilmu, beriman dan bersabar. Semoga keberhasilan ini menjadi satu langkah awal untuk masa depanku, dalam meraih cita-cita saya. Dengan ini saya persembahkan karya ini untuk, ayah saya Bagus Susilo dan ibu saya Martinah. Terima kasih atas kasih sayang yang berlimpah dari mulai saya lahir, hingga saya sudah sebesar ini. Terima kasih juga atas limpahan doa yang tak berkesudahan. Serta dua adik saya Nizma Nabila Syafa Susilo dan Qory Qonita Aqila Susilo yang menjadi motivasi saya dalam mengerjakan skripsi ini

Terima kasih yang tak terhingga untuk dosen pembimbing saya, bapak Dony Ariyus, M.Kom, yang dengan sabar membantu dan membimbing saya dalam mengerjakan skripsi ini. Terima kasih juga untuk semua pihak yang mendukung keberhasilan skripsi saya yang tidak bisa saya sebutkan satu per satu. Ucapan terima kasih ini saya persembahkan juga untuk seluruh teman-teman saya di Fakultas Ilmu Komputer prodi Teknik Komputer. Terima kasih untuk memori yang kita rajut setiap harinya, atas tawa yang setiap hari kita miliki, dan atas solidaritas yang luar biasa.

Dan untuk seseorang yang selalu mendukung saya (inisial ACS), terimakasih telah menemani saya dalam 3 tahun terakhir, terimakasih atas waktu yang telah diberikan, menjadi tempat cerita ketika saya jauh dari rumah, terimakasih telah menemani dan selalu mendukung saya. Semoga kita bisa selalu bersama untuk menjadi pribadi yang lebih baik dan selalu dalam lindungan Allah SWT. Untuk semua pihak yang telah membantu saya yang tidak bisa saya sebutkan satu persatu, terima kasih atas semuanya. Semoga Tuhan senantiasa membalas setiap kebaikan kalian. Serta kehidupan kalian semua juga dimudahkan dan diberkahi selalu oleh Allah SWT.

KATA PENGANTAR

Puji syukur kehadiran Allah SWT, atas limpahan Rahmat dan Karunia-Nya, sehingga penulis dapat merampungkan skripsi dengan judul: Analisa Kesadaran Keamanan Informasi Customer Services Dengan Metode Failure Mode And Effect Analysis Framework ISO/IEC 27001:2013. Penghargaan dan terima kasih yang setulus-tulusnya kepada Ayah saya Bagus Susilo dan Ibu saya tercinta Martinah yang telah mencurahkan segenap cinta dan kasih sayang serta perhatian moril maupun materil. Semoga Allah SWT selalu melimpahkan Rahmat, Kesehatan, Karunia dan keberkahan di dunia dan di akhirat atas budi baik yang telah diberikan kepada penulis.

Penghargaan dan terima kasih penulis berikan kepada Bapak Dony Ariyus, M.Kom selaku Dosen Pembimbing yang telah membantu penulisan skripsi ini. Serta ucapan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Rektor Universitas Amikom Yogyakarta
2. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta
3. Bapak Dony Ariyus, M.Kom yang juga selaku Ketua Program Studi Teknik Komputer Universitas Universitas Amikom Yogyakarta
4. Sahabat-sahabat grup Softex (Redo Maland, Ipung Ardiansyah, Ero wahyu, Ahmad Ristanto, Ferry Dwi dan Andika Adnan) dan rekan-rekan mahasiswa khususnya program studi S1 Teknik Komputer.

Akhir kata penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Semoga dalam tulisan ini ada manfaat yang dapat diambil.

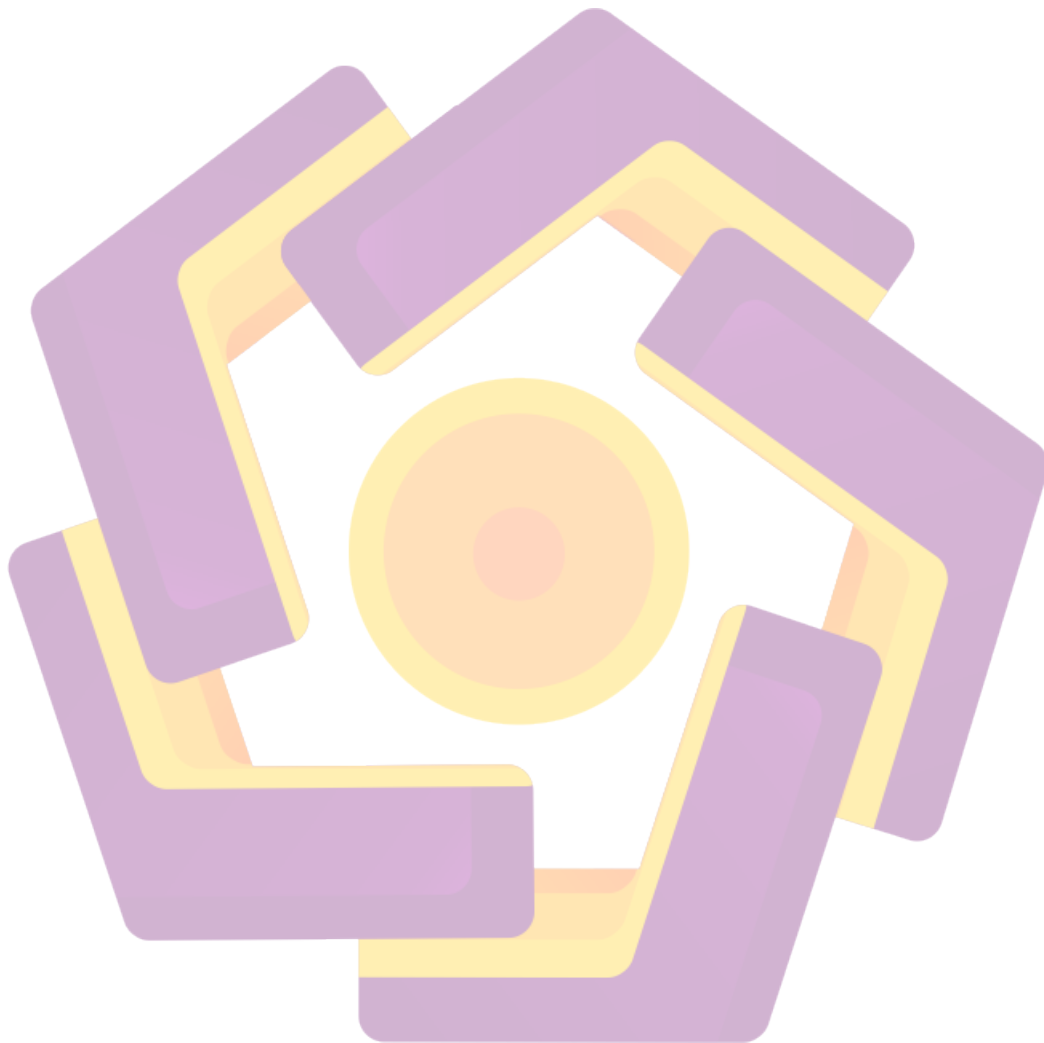
Yogyakarta, 26 Januari 2021

Penulis

DAFTAR ISI

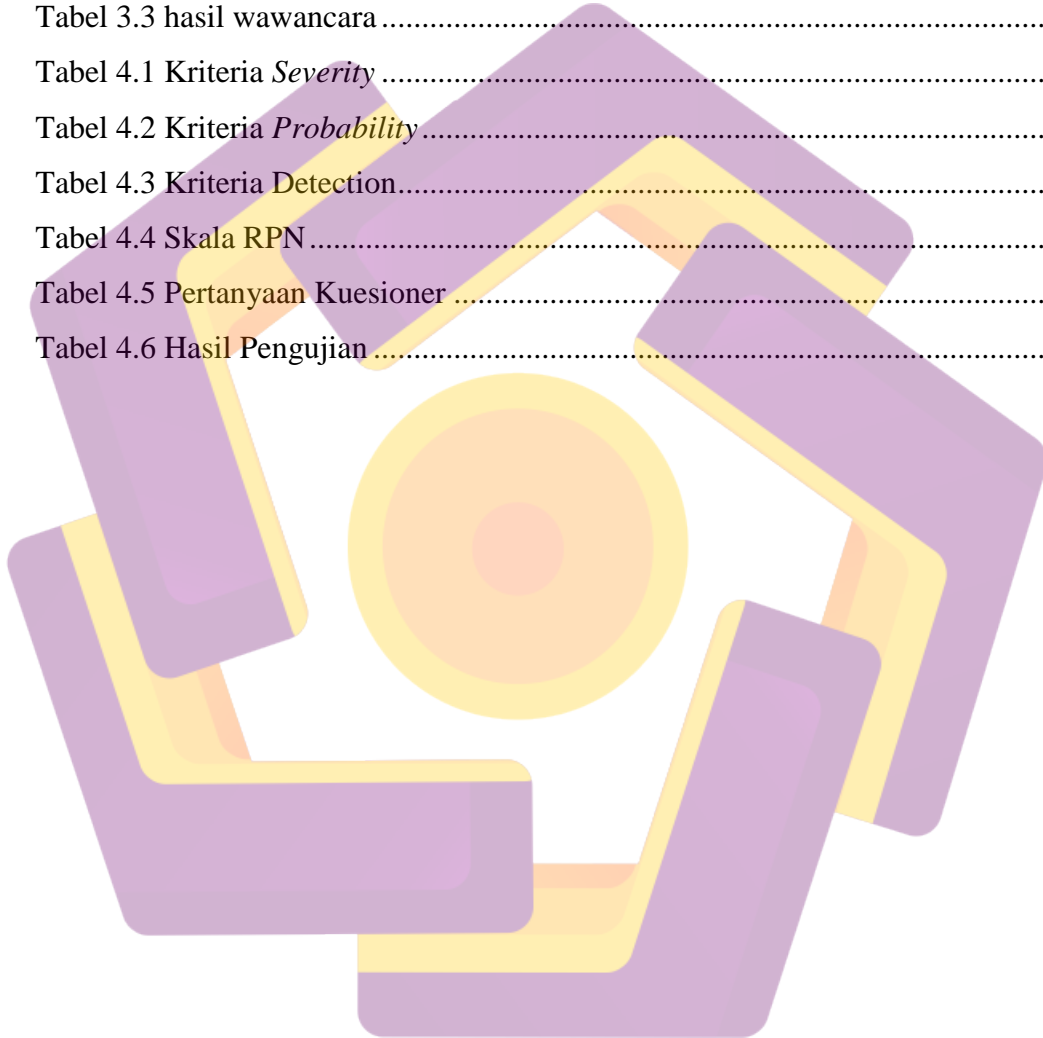
HALAMAN JUDUL.....	2
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	v
HALAMAN MOTTO	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
INTISARI.....	xiii
<i>ABSTRACT</i>	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1 Tinjauan Pustaka	5
2.2 Social Engineering	6
2.3 Cyber Security Awareness pada masa Pandemi	11
2.4 ISO/IEC 27001:2013	13
2.5 Failure Mode and Effect Analysis	14
BAB III METODOLOGI PENELITIAN	18
3.1 Deskripsi Singkat Obyek	18
3.2 Analisis Permasalahan	18
3.3 Solusi Yang Diusulkan	19
3.4 Alat dan Bahan Penelitian.....	19
3.5 Metode Penelitian	20
3.6 Metode Analisis	24
3.7 Metode Perancangan	24
BAB IV PEMBAHASAN	31
4.1 Perancangan	31
4.2 Implementasi sistem.....	37
4.3 Pengujian Sistem.....	39

BAB V PENUTUP.....	41
5.1 Kesimpulan	41
5.2 Saran	41
DAFTAR PUSTAKA	43



DAFTAR TABEL

Tabel 2.1 Controls List: The 14 Control Sets of Annex A	13
Tabel 2.2 Tingkat nilai RPN	17
Tabel 3.1 Masalah Pada Obyek Penelitian.....	19
Tabel 3.2 Daftar Solusi	19
Tabel 3.3 hasil wawancara	22
Tabel 4.1 Kriteria <i>Severity</i>	34
Tabel 4.2 Kriteria <i>Probability</i>	35
Tabel 4.3 Kriteria <i>Detection</i>	36
Tabel 4.4 Skala RPN	36
Tabel 4.5 Pertanyaan Kuesioner	37
Tabel 4.6 Hasil Pengujian	39



DAFTAR GAMBAR

Gambar 2.1 Social Engineering Clasification	6
Gambar 2.2 Social Engineering Berbasis Komputer	7
Gambar 2.3 Phising Attack Clasification	7
Gambar 2.4 Human Based	9
Gambar 2.5 Dimensi Security Awareness	12
Gambar 2.6 Severity of Effect Ranking	15
Gambar 2.7 Probability Rankings	15
Gambar 2.8 Detection Rankings	16
Gambar 3.1 PC yang digunakan Customer Services	20
Gambar 3.2 Ruang customer services	21
Gambar 3.3 Telepon Kantor	21
Gambar 3.4 Bukti wawancara	22
Gambar 3.5 Perancangan Risk Management	25
Gambar 3.6 Proses Identifikasi Risiko	26
Gambar 3.7 Proses Analisa Risiko	27
Gambar 3.8 Proses Evaluasi Risiko	28
Gambar 3.9 Analisa Respon Terhadap Risiko	28
Gambar 3.10 Proses Kontrol Dan Monitoring Risiko	29
Gambar 4.1 Perancangan Risk Management Sistem	32

INTISARI

Peningkatan serangan rekayasa sosial di masa pandemi menjadi salah satu masalah utama bagi individu, kelompok maupun perusahaan. Kesadaran keamanan informasi merupakan sebuah hal yang sangat penting dan menjadi salah satu pondasi utama dalam membangun sistem keamanan yang kuat. Terdapat tiga komponen utama dalam membangun sistem keamanan informasi, yaitu teknologi, proses dan manusia. Dengan kemajuan teknologi yang semakin canggih akan memberikan sebuah kenyamanan dan kepercayaan bagi setiap pengguna, namun secanggih apapun teknologi yang digunakan tetap memiliki celah kemanan, yaitu pada sektor 'manusia'.

Pada masa pandemi Covid-19, peningkatan penggunaan media sosial meningkat tajam. Kesadaran keamanan informasi menjadi hal wajib bagi setiap individu dalam mengimplementasikan sistem kesadaran keamanan pada masa pandemi. Dengan meningkatnya penggunaan media komunikasi berbasis internet, menimbulkan sebuah ancaman dalam keamanan informasi. Perusahaan juga menerapkan *Work From Home* (WFH) bagi pegawainya dalam melakukan pekerjaan. Secara tidak langsung perusahaan memberikan sebuah ruang yang dapat di manfaatkan pelaku kejahatan dimana perusahaan tidak dapat memantau secara langsung setiap *device* yang digunakan pegawai dalam melakukan pekerjaannya.

Penelitian ini akan menganalisa analisa kesadaran keamanan informasi menggunakan metode *Failure Mode And Effect Analysis* dengan Framework ISO/IEC 27001:2013. Hasil dari penelitian ini akan menunjukkan tingkat *security awareness* dalam upaya pencegahan serangan siber yang marak terjadi di masa pandemi, serta memberikan saran dan masukan untuk meningkatkan kesadaran keamanan informasi sesuai dengan standar ISO 27001:2013.

Kata kunci: Kesadaran Keamanan Informasi, Failure Mode Effect and Analysis (FMEA), SNI ISO/IEC 27001:2013

ABSTRACT

The increase in social engineering attacks during a pandemic is one of the main problems for individuals, groups and companies. Information security awareness is very important and becomes one of the main foundations in building a strong security system. There are three main components in building an information security system, namely technology, processes, and people. With advances in technology that are increasingly sophisticated will provide comfort and confidence for every user, but no matter how sophisticated the technology is used, it still has a security gap, namely in the “human” sector.

During the Covid-19 pandemic, the use of social media increased sharply. Information security awareness is mandatory for every individual in implementing a security awareness system during a pandemic. With the increasing use of internet-based communication media, it poses a threat to information security. The company also implements Work From Home (WFH) for employees in doing work. Indirectly, the company provides a space that can be used by criminals where the company cannot directly monitor every device used by employees in doing their work.

This study will analyze the analysis of information security awareness using the Failure Mode And Effect Analysis using Framework ISO / IEC 27001: 2013 Standards. The results of this study will show the level of security awareness in efforts to prevent cyber attacks that are rife during a pandemic, as well as provide suggestions and input to increase information security awareness in accordance with ISO 27001: 2013 standards.

Keyword: *information security awareness, Failure Mode Effect and Analysis (FMEA), SNI ISO / IEC 27001: 2013*