

**ANALISA KESADARAN KEAMANAN INFORMASI PADA
PETUGAS VAKSIN MENGGUNAKAN METODE
OCTAVE-S DAN FMEA BERDASARKAN
ISO/IEC 27001:2013**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

Fitriana Budhi Permatasari

18.83.0210

Kepada

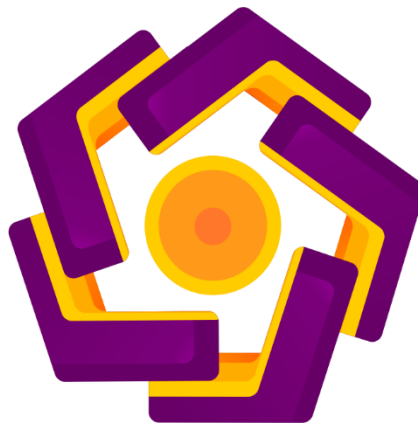
**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2022

**ANALISA KESADARAN KEAMANAN INFORMASI PADA
PETUGAS VAKSIN MENGGUNAKAN METODE
OCTAVE-S DAN FMEA BERDASARKAN
ISO/IEC 27001:2013**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

Fitriana Budhi Permatasari

18.83.0210

Kepada

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

2022

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISA KESADARAN KEAMANAN INFORMASI PADA
PETUGAS VAKSIN MENGGUNAKAN METODE
OCTAVE-S DAN FMEA BERDASARKAN
ISO/IEC 27001:2013**

yang disusun dan diajukan oleh

Fitriana Budhi Permatasari

18.83.0210

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Juni 2022

Dosen Pembimbing,

Dony Ariyus, M.Kom

NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

**ANALISA KESADARAN KEAMANAN INFORMASI PADA
PETUGAS VAKSIN MENGGUNAKAN METODE
OCTAVE-S DAN FMEA BERDASARKAN
ISO/IEC 27001:2013**

yang disusun dan diajukan oleh

Fitriana Budhi Permatasari

18.83.0210

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 Juli 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Joko Dwi Santoso, M.Kom
NIK. 190302181

Muhammad Kopravi, S.Kom., M.Eng
NIK. 190302454

Dony Ariyus, M.Kom
NIK. 190302128

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : **Fitriana Budhi Permatasari**
NIM : **18.83.0210**

Menyatakan bahwa Skripsi dengan judul berikut:

**ANALISA KESADARAN KEMAMAN INFORMASI PADA PETUGAS VAKSIN
MENGUNAKAN METODE OCTAVE-S DAN FMEA BERDASARKAN 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, 25 Juli 2022

Yang Menyatakan,



Fitriana Budhi Permatasari

HALAMAN PERSEMBAHAN

Dengan segala puji dan syukur kepada Tuhan yang Maha Esa dan atas dukungan dan doa dari orang-orang tercinta, alhamdulillah skripsi ini dapat terselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia saya khaturkan rasa syukur dan terimakasih saya kepada :

1. Allah SWT, Tuhan Yang Maha Esa karena hanya atas izin dan karunianya, maka skripsi ini dapat dibuat dan selesai pada waktunya.
2. Orang tua, yang selalu memberi dukungan serta doa. Untuk Ibu yang tidak pernah lelah dalam memberikan semangat agar bisa segera menyelesaikan skripsi ini dan untuk Bapak yang telah banyak memberikan begitu banyak pengorbanan yang tidak bisa terbalaskan. Terimakasih banyak saya ucapkan untuk keduanya.
3. Dosen Pembimbing skripsi bapak Dony Ariyus, M.Kom. Selaku dosen pembimbing, saya mengucapkan sangat berterimakasih atas bimbingannya selama ini yang telah memberikan motivasi, masukan, kritik dan saran yang membangun agar menjadi lebih baik lagi untuk kedepannya.
4. Rekan – rekan kelas 18 Teknik Komputer 02, yang telah memberikan saya motivasi, dukungan, semangat Semoga kita menjadi orang-orang yang bermanfaat dan dikenang menjadi pribadi yang baik.
5. Keluarga besar Himpunan Teknik Komputer, yang telah memberikan pengalaman yang begitu banyak dalam segala aspek.

Terimakasih yang sebesar besarnya kepada semua pihak yang telah memberikan masukan, dukungan serta motivasi dalam proses pembuatan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi pihak yang membutuhkan dan berguna untuk kemajuan ilmu pengetahuan dimasa yang akan datang.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur penulis panjatkan kehadirat ALLAH SWT, yang telah melimpahkan Rahmat dan Karunianya sehingga penulis dapat menyelesaikan skripsi ini sebagai salah satu syarat kelulusan Program Strata 1 Program Studi Teknik Komputer, Universitas AMIKOM Yogyakarta dan untuk memperoleh gelar Sarjana Komputer (S.Kom).

Dengan selesainya skripsi yang berjudul ***“Analisa Kesadaran Keamanan Informasi Pada PETUGAS Vaksin Menggunakan Metode OCTAVE-S dan FMEA berdasarkan ISO/IEC 27001:2013”***, dengan ini penulis mengucapkan terima kasih kepada :

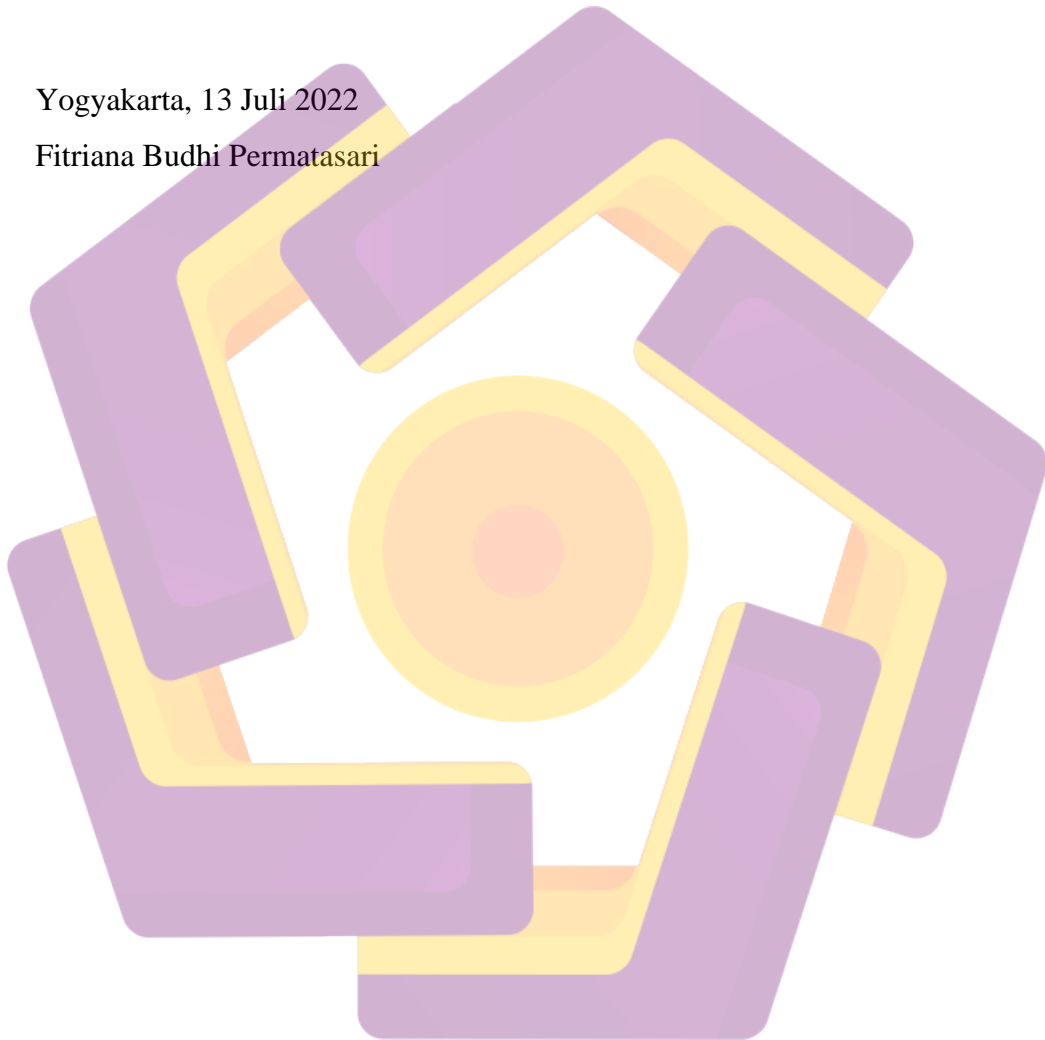
1. Allah SWT atas berkah, rahmat, hidayah, serta karunianya yang telah diberikan kepada penulis sehingga dapat menyelesaikan skripsi ini dengan maksimal.
2. Kepada kedua orang tua yang selalu memberikan motivasi, dukungan baik moral maupun materi.
3. Prof. Dr. M. Suyanto, MM selaku rektor Universitas AMIKOM Yogyakarta.
4. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer dan Ketua Program Studi S1 Sistem Informasi.
5. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta dan selaku dosen pembimbing yang selalu memberikan arahan, saran dan motivasi agar penulis bisa menyelesaikan skripsi ini dengan baik dan benar.
6. Keluarga besar kelas S1 Teknik Komputer 02 angkatan 2018.
7. Keluarga besar Himpunan Teknik Komputer Angkatan 2017-2019
8. Serta semua pihak yang telah membantu dalam proses penyusunan skripsi ini yang tidak dapat disebutkan satu persatu.

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

Wassalamualaikum Warahmatullahi Wabarakatuh

Yogyakarta, 13 Juli 2022

Fitriana Budhi Permatasari



DAFTAR ISI

HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN.....	iii
SKRIPSI.....	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiii
DAFTAR LAMBANG DAN SINGKATAN	xiv
DAFTAR ISTILAH	xv
INTISARI	xvi
ABSTRACT.....	xvii
BAB I PAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan masalah.....	3
1.3 Tujuan Penelitian	3
1.4 Batasan Masalah	4
1.5 Manfaat Penelitian	4
BAB II TINJAUAN PUSTAKA	5
2.1 Literature Review	5
2.2 Landasan Teori	9
2.2.1 Social Engineering	9
2.2.2 Security Awareness.....	15
2.2.3 OCTAVE-S	18
2.2.4 FMEA	18
2.2.5 ISO/IEC 27001:2013	19
BAB III METODOLOGI PENELITIAN	20
3.1 Profil Objek.....	20

3.1.1	Profil Dinas Kesehatan	20
3.1.2	Profil Dinas Komunikasi dan Informatika.....	21
3.2	Analisis Permasalahan	23
3.3	Alat dan Bahan Penelitian.....	24
3.4	Metode Penelitian	24
3.3	Flowchart Penelitian	30
BAB IV	HASIL DAN PEMBAHASAN	35
4.1	Implementasi.....	35
4.1.1	Pengumpulan Data.....	35
4.1.2	Analisa Data.....	48
4.1.3	Identifikasi Risiko.....	50
4.1.4	Penilaian.....	54
4.1.5	Mitigasi	56
BAB V	KESIMPULAN DAN SARAN	60
5.1	Kesimpulan	60
5.2	Saran	61
	DAFTAR PUSTAKA	62
	LAMPIRAN.....	65

DAFTAR TABEL

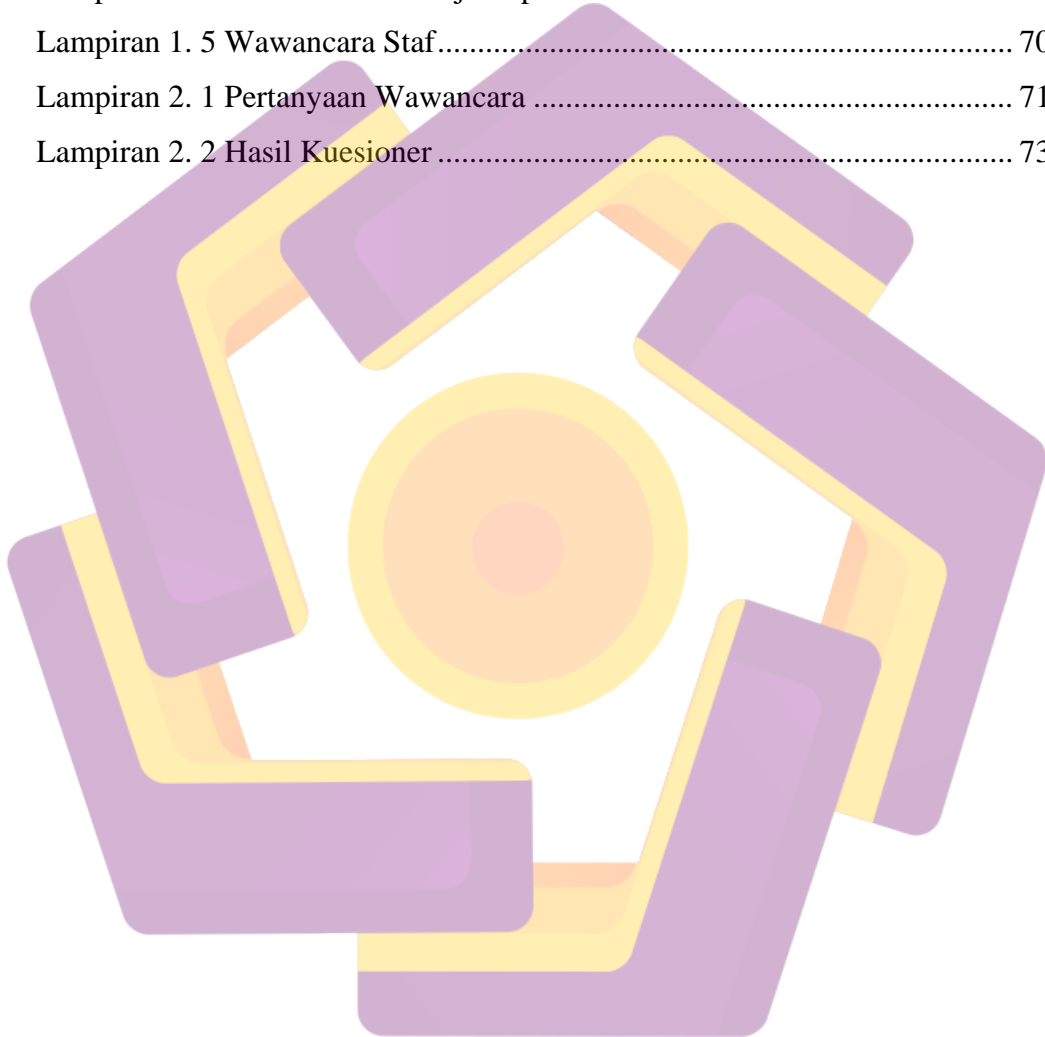
Tabel 2. 1 Penelitian Terkait	6
Tabel 3. 1 Kriteria Penilaian Severity	26
Tabel 3. 2 Kriteria Penilaian Probability	27
Tabel 3. 3 Kriteria Penilaian Detection.....	28
Tabel 3. 4 Tingkat Nilai RPN	29
Tabel 3. 5 Control list ISO/IEC 27001:2013	29
Tabel 4. 1 Daftar hasil Wawancara.....	38
Tabel 4. 2 Daftar Aset Kritis.....	44
Tabel 4. 3 Kebutuhan Keamanan Aset Kritis	45
Tabel 4. 4 Identifikasi Ancaman Aset Kritis.....	47
Tabel 4. 5 Identifikasi Komponen Kunci.....	48
Tabel 4. 6 Evaluasi Komponen.....	49
Tabel 4. 7 Identifikasi Potential Cause	50
Tabel 4. 8 Identifikasi Risiko.....	52
Tabel 4. 9 Penilaian Risiko	54
Tabel 4. 10 Mitigasi Risiko.....	56

DAFTAR GAMBAR

Gambar 1 1 Data jumlah phishing menurut laporan dari APWG	2
Gambar 2. 1 Social Engineering	9
Gambar 2. 2 Social Engineering Attack Computer Based.....	10
Gambar 2. 3 Social Engineering Attack Computer Based.....	12
Gambar 2. 4 Jenis-Jenis Phishing	13
Gambar 2. 5 Security Awareness.....	16
Gambar 2. 6 Dimensi Security Awareness	17
Gambar 3.1 Struktur Organisasi DINKES.....	21
Gambar 3.2 Struktur Organisasi DISKOMINFO	23
Gambar 3. 3 Metode OCTAVE-S.....	24
Gambar 3. 4 Rumus menghitung RPN	28
Gambar 3. 5 Flowchart Penelitian.....	30
Gambar 3. 6 Pengumpulan Data	31
Gambar 3. 7 Analisa Data.....	32
Gambar 3. 8 Identifikasi Risiko	33
Gambar 3. 9 Penilaian.....	33
Gambar 3. 10 Menghitung nilai RPN	54
Gambar 4.1 Device yang digunakan petugas admin.....	35
Gambar 4.2 Website yang digunakan petugas admin	35
Gambar 4.3 Petugas admin observasi	36
Gambar 4.4 Petugas admin registrasi.....	36
Gambar 4.5 Bekas yang sudah selesai diinput.....	37

DAFTAR LAMPIRAN

Lampiran 1. 1 Tabel Pertanyaan Wawancara	66
Lampiran 1. 2 Wawancara Manajer Senior	69
Lampiran 1. 3 Wawancara Manajer Senior	69
Lampiran 1. 4 Wawancara Manajer Operational	69
Lampiran 1. 5 Wawancara Staf	70
Lampiran 2. 1 Pertanyaan Wawancara	71
Lampiran 2. 2 Hasil Kuesioner	73



DAFTAR LAMBANG DAN SINGKATAN



APWG	: Phishing Activity Trends Report Analisis
KTP	: Kartu Tanda Penduduk
OKTAVE-S	: Operationally Critical Threat, Asset, And Vulnerability Evaluation
FMEA	: Failure Mode And Effect Analysis
ATM	: Anjungan Tunai Mandiri
VOIP	: Voice Over Internet Protocol
SMS	: Short Message Service
BSSN	: Badan Siber Dan Sandi Negara
RPN	: Tingkat Prioritas Risiko
ISMS	: Informasi Security Management System
SMKI	: Sistem Manajemen Keamanan Informasi
SOP	: Standard Operating Procedure
DRP	: Disaster Recovery Plan
NIK	: Nomor Induk Kependudukan
DISKOMINFO	: Dinas Komunikasi Dan Informatika
SMM	: Sistem Manajemen Mutu

DAFTAR ISTILAH

- Cybercrime : Sebuah kejahatan virtual yang memanfaatkan perangkat computer yang terhubung dengan jaringan internet.
- Hacker : Seseorang yang mempunyai kemampuan untuk menerobos sistem keamanan computer dengan tujuan untuk mengetes system keamanan hingga melakukan tindak kriminal
- Malware : Perangkat lunak yang bertujuan untuk merusak system computer, jaringan atau server tanpa diketahui oleh pemiliknya.
- Ransomware : Serangan malware yang menggunakan metode enkripsi untuk menyimpan dan menyembunyikan informasi korban

INTISARI

Perkembangan serangan rekayasa sosial merupakan masalah yang sering terjadi pada sebuah organisasi atau perusahaan. Karena seringkali ancaman ini diabaikan padahal serangan ini dapat dieksploitasi setiap saat untuk mengambil kesempatan dari kelemahan pada sisi pengguna sistem itu sendiri yaitu manusia. Menurut hasil laporan APWG jumlah *phising* Juni 2021 sebanyak 222.127 merupakan laporan bulan terburuk sepanjang sejarah pelaporan.

Sehingga kesadaran kita akan keamanan informasi perlu untuk ditingkatkan agar kita bisa tau apa yang harus dilakukan untuk menjaga informasi penting baik milik kita pribadi maupun orang lain. Pada penelitian ini akan melakukan analisa kesadaran keamanan informasi pada petugas vaksin yang akan dilakukan dengan menggunakan metode OCTAVE-S dan metode FMEA berdasarkan standar ISO/IEC 27001:2013. Metode OCTAVE-S digunakan untuk menganalisa risiko dengan sumber data yang didapat melalui metode wawancara bersama dengan tiga narasumber yaitu manajer senior, manajer operasional, staf Sedangkan metode FMEA digunakan untuk menghitung tingkat kesadaran keamanan informasi pada petugas vaksin pengolahan data dilapangan. Pada penelitian ini berfokus pada serangan rekayasa sosial. Langkah mitigasi juga peneliti berikan yang berdasarkan dengan ISO/IEC 27001:2013.

Hasil penelitian ini didapatkan 16 penyebab potensial dan 10 risiko yang mungkin akan terjadi. 16 potential cause tergolong menjadi 3 rendah, 3 sedang, 5 tinggi dan 5 sangat tinggi. Sehingga didapatkan kesimpulan bahwa kesadaran petugas vaksin akan keamanan informasi masih tergolong rendah.

Kata kunci: Rekayasa sosial, Kesadaran Keamanan, Operationally Critical Threat, Asset, and Vulnerability Evaluation, Failure Mode and Effect Analysis, ISO/IEC 27001:2013

Abstract

The development of social engineering attacks is a problem that often occurs in an organization or company. Because this threat is often ignored even though this attack can be exploited at any time to take advantage of weaknesses on the user side of the system itself, namely humans. According to the results of the APWG report, the number of phishing phishes in June 2021 was 222,127, which was the worst month in the history of reporting.

So that our awareness of information security needs to be increased so that we can know what to do to protect important information both ours and others. In this study, an analysis of information security awareness among vaccine officers will be carried out using the OCTAVE-S method and the FMEA method based on the ISO/IEC 27001:2013 standard. The OCTAVE-S method is used to analyze risk with data sources obtained through interviews with three sources, namely Senior Managers, Operational Managers and Staff. While the FMEA method is used to calculate the level of information security awareness of vaccine officers in data processing in the field. This research focuses on social engineering attacks. Mitigation steps are also given by researchers based on ISO/IEC 27001:2013.

The results of this study obtained 16 potential causes and 10 risks that might occur. The 16 potential causes are classified as 3 low, 3 medium, 5 high and 5 very high. So it can be concluded that awareness of vaccine officers on information security is still relatively low.

Keyword: *Social Engineering, Security Awareness, Operationally Critical Threat, Asset, and Vulnerability Evaluation, Failure Mode and Effect Analysis, ISO/IEC 27001:2013*