

**Analisis Resiko dan Strategi Mitigasi dalam Mengatasi Serangan Siber pada
Perusahaan Teknologi Informasi Menggunakan Framework OCTAVE**

TESIS

Untuk memenuhi sebagian persyaratan memperoleh gelar
Magister Teknologi Informasi

Disusun Oleh :

Ikbal Danu Setiawan

227064518015



**PROGRAM STUDI MAGISTER TEKNOLOGI INFORMASI
FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS NASIONAL
JAKARTA
2024**

HALAMAN PENGESAHAN

TESIS

ANALISIS RESIKO DAN STRATEGI MITIGASI DALAM MENGATASI
SERANGAN SIBER PADA PERUSAHAAN TEKNOLOGI INFORMASI
MENGUNAKAN FRAMEWORK OCTAVE



Ikbal Danu Setiwan

227064518015

Dosen Pembimbing



Dr. Septi Andryana, S.Kom., MMSI

NIDN. 0317097209

PERNYATAAN KEASLIAN TESIS

Saya menyatakan dengan sesungguhnya bahwa Tesis dengan judul :

Analisis Resiko dan Strategi Mitigasi dalam Mengatasi Serangan Siber pada Perusahaan Teknologi Informasi Menggunakan Framework OCTAVE

Yang dibuat untuk melengkapi salah satu persyaratan menjadi Magister Komputer pada Program Studi Magister Teknologi Informasi, Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional, sebagaimana yang saya ketahui adalah bukan merupakan tiruan atau publikasi dari Tesis yang pernah diajukan atau dipakai untuk mendapatkan gelar di lingkungan Universitas Nasional maupun perguruan tinggi atau instansi lainnya, kecuali pada bagian – bagian tertentu yang menjadi sumber informasi atau acuan yang dicantumkan sebagaimana mestinya.



Jakarta, 9 September 2024



Ikbal Danu Setiawan

227064518015

LEMBAR PERSETUJUAN REVIEW AKHIR

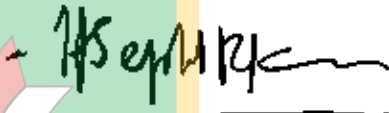
Tesis dengan judul :

ANALISIS RESIKO DAN STRATEGI MITIGASI DALAM MENGATASI SERANGAN SIBER PADA PERUSAHAAN TEKNOLOGI INFORMASI MENGUNAKAN FRAMEWORK OCTAVE

Dibuat untuk melengkapi salah satu persyaratan menjadi Magister Komputer pada Program Studi Magister Teknologi Informasi Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional. Tesis ini diujikan pada Sidang Akhir Semester Genap 2023-2024 pada tanggal 24 Agustus Tahun 2024



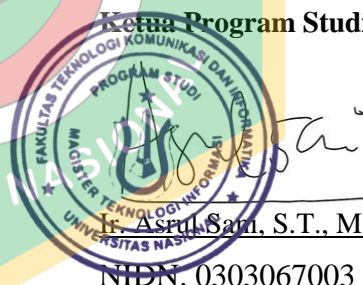
Dosen Pembimbing



Dr. Septi Andryana, S.Kom., MMSI

NIDN. 0317097209

Ketua Program Studi



Dr. Asrul Sami, S.T., M.Kom., Ph.D

NIDN. 0303067003

LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI

Nama : Ikkal Danu Setiawan
NPM : 227064518015
Fakultas/Akademi : Fakultas Teknologi Komunikasi dan Informatika
Program Studi : Teknologi Informasi
Tanggal Sidang : 24 Agustus 2024

JUDUL DALAM BAHASA INDONESIA :

Analisis Resiko dan Strategi Mitigasi dalam Mengatasi Serangan Siber pada Perusahaan Teknologi Informasi Menggunakan Framework OCTAVE

JUDUL DALAM BAHASA INGGRIS :

Risk Analysis and Mitigation Strategies for Addressing Cyber Attacks in Information Technology Companies Using the OCTAVE Framework

TANDA TANGAN DAN TANGGAL

Pembimbing 1	Ka. Prodi	Mahasiswa
TGL :	TGL :	TGL : 14 - 9 - 2024
	 	

LEMBAR PENGESAHAN

**JUDUL : ANALISIS RESIKO DAN MITIGASI DALAM MENGATASI SERANGAN SIBER PADA
PERUSAHAAN TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK OCTAVE**

Diajukan untuk memenuhi sebagai persyaratan
Memperoleh gelar Magister Komputer

Disusun Oleh :

Ikkal Danu Setiawan
227064518015

Tesis ini telah diuji dan dinyatakan lulus pada,
24 Agustus 2024

Telah diperiksa dan disetujui oleh:

Dosen Pembimbing



(Dr. Septi Andryana, S.Kom., MMSI)
NIDN. 0317097209

Ketua Program Studi
Magister Teknologi Informasi



(Ir. Asrul Sani, S.T., M.Kom., Ph.D)
NIDN. 0303067003

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan benar. Bilamana di kemudian hari ditemukan bahwa karya tulis ini menyalahi peraturan yang ada berkaitan etika dan kaidah penulisan karya ilmiah yang berlaku, maka saya bersedia dituntut dengan ketentuan berlaku

Yang menyatakan,

Nama : Ikkal Danu Setiawan

NPM : 227064518015

Tanggal : 9 September 2024

Mengetahui

Pembimbing I : **Dr. Septi Andryana, S.Kom., MMSI (NIDN. 0317097209)**



KATA PENGANTAR

Alhamdulillah, puji syukur kami panjatkan ke hadirat Allah Subhanahu wa Ta'ala yang telah memberikan petunjuk dan pertolongannya sehingga Panduan Tesis ini bisa diselesaikan dengan baik. Panduan ini disusun dalam rangka untuk memberikan arahan yang jelas dan terukur bagi seluruh pemangku kepentingan Tesis di lingkungan FTKI Program Studi S2 Teknologi Informasi.

Puji dan syukur saya panjatkan kepada Allah Swt. atas ridanya saya dapat menyelesaikan penyusunan Tesis ini. Adapun judul Tesis yang saya ajukan adalah "Analisis Resiko dan Strategi Mitigasi dalam Mengatasi Serangan Siber pada Perusahaan Teknologi Informasi Menggunakan Framework OCTAVE"

Tesis ini diajukan untuk memenuhi syarat kelulusan di Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional. Tidak dapat disangkal bahwa butuh usaha yang keras dalam penyelesaian pengerjaan skripsi ini. Namun, karya ini tidak akan selesai tanpa orang-orang tercinta di sekeliling saya yang mendukung dan membantu. Terima kasih saya sampaikan kepada:

1. Bapa dan Mama selaku orangtua penulis yang telah banyak memberi dukungan
2. Dr. Agung Triayudi, S.Kom., M.Kom. selaku Dekan dan Ketua Program Studi S2 Teknologi Informasi, Universitas Nasional beserta jajarannya yang telah mendedikasikan ilmunya kepada penulis sehingga penulis dapat menyelesaikan Tesis ini
3. Dr. Septi Andryana, S.Kom., MMSI selaku Dosen pembimbing yang telah memberikan bimbingan dan berbagai pengalaman kepada penulis.
4. Segenap Dosen Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional yang telah mendidik dan memberikan ilmu selama kuliah dan seluruh staf yang selalu sabar melayani segala administrasi selama proses penelitian ini.

Semoga segala kebaikan dan pertolongan semuanya mendapat berkah dari Allah Swt. dan akhirnya saya menyadari bahwa Tesis ini masih jauh dari kata sempurna, karena keterbatasan ilmu yang saya miliki. Untuk itu saya dengan kerendahan hati mengharapkan saran dan kritik yang sifatnya membangun dari semua pihak demi membangun laporan penelitian ini.

Jakarta, 9 September 2024

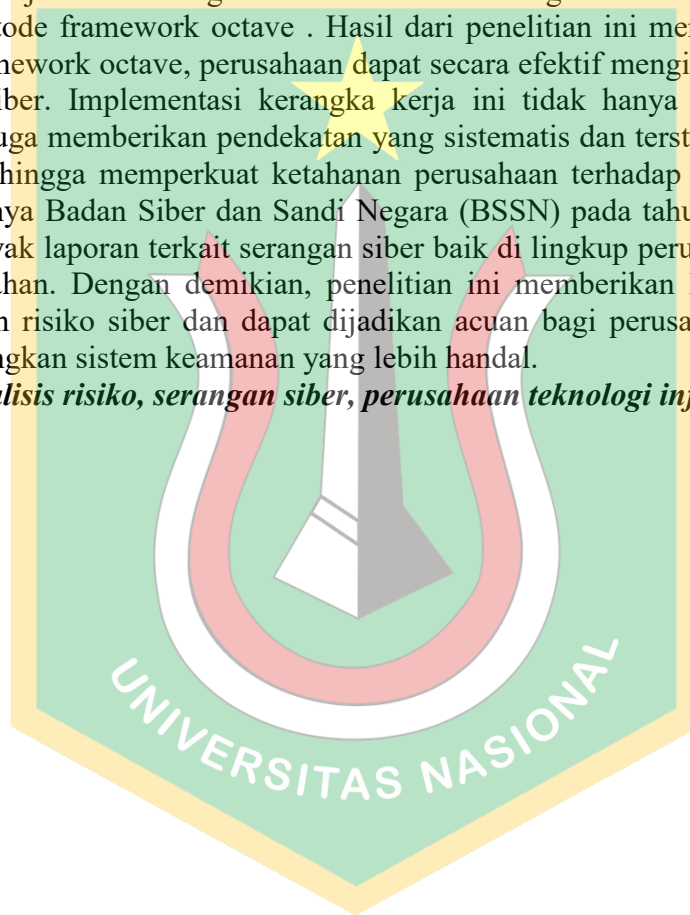


Ikbal Danu Setiawan
NPM : 227064518015

ABSTRAK

Dalam era digital yang semakin maju, perusahaan teknologi informasi menjadi target utama serangan siber yang terus berkembang dalam kompleksitas dan intensitas. Untuk mengatasi ancaman ini, analisis risiko merupakan langkah krusial yang harus diambil untuk mengidentifikasi, mengevaluasi, dan mengurangi risiko yang terkait dengan serangan siber. Penelitian ini bertujuan untuk menganalisis risiko serangan siber pada perusahaan teknologi informasi menggunakan framework octave. Framework octave menyediakan pedoman sistematis dan terstruktur untuk manajemen risiko yang dapat diterapkan pada berbagai jenis risiko, termasuk risiko siber. Berdasarkan hasil analisis risiko, prioritas diberikan kepada risiko yang memiliki tingkat keparahan tinggi untuk mendapatkan tindakan mitigasi yang tepat. Strategi mitigasi risiko yang diusulkan meliputi implementasi teknologi keamanan, pengembangan kebijakan dan prosedur keamanan, serta peningkatan kesadaran dan pelatihan karyawan tentang praktik keamanan siber. Selain itu, penelitian ini menekankan pentingnya pemantauan berkelanjutan dan evaluasi periodik terhadap efektivitas strategi mitigasi yang diterapkan. Dalam upaya melawan kejahatan serangan siber dan melindungi keamanan digital penulisan ini menggunakan metode framework octave . Hasil dari penelitian ini menunjukkan bahwa dengan menggunakan framework octave, perusahaan dapat secara efektif mengidentifikasi dan mengelola risiko serangan siber. Implementasi kerangka kerja ini tidak hanya meningkatkan keamanan informasi, tetapi juga memberikan pendekatan yang sistematis dan terstruktur dalam menghadapi ancaman siber, sehingga memperkuat ketahanan perusahaan terhadap serangan di masa depan. Setelah terbentuknya Badan Siber dan Sandi Negara (BSSN) pada tahun 2017, BSSN Indonesia mendapatkan banyak laporan terkait serangan siber baik di lingkup perusahaan swasta maupun di lingkup pemerintahan. Dengan demikian, penelitian ini memberikan kontribusi penting dalam bidang manajemen risiko siber dan dapat dijadikan acuan bagi perusahaan teknologi informasi dalam mengembangkan sistem keamanan yang lebih handal.

Kata Kunci : *Analisis risiko, serangan siber, perusahaan teknologi informasi, octave, keamanan siber.*



ABSTRACT

In an increasingly advanced digital age, information technology companies are becoming the main target of cyberattacks that are growing in complexity and intensity. To address these threats, risk analysis is a crucial step to identify, evaluate, and mitigate the risks associated with cyber attacks. This study aims to analyze the risk of cyberattacks on information technology companies using the octave framework. The octave framework provides systematic and structured guidelines for risk management that can be applied to various types of risks, including cyber risks. Based on the results of the risk analysis, priority is given to risks of high severity to obtain appropriate mitigation measures. The proposed risk mitigation strategies include the implementation of security technologies, development of security policies and procedures, as well as raising employee awareness and training on cybersecurity practices. In addition, the study emphasizes the importance of continuous monitoring and periodic evaluation of the effectiveness of the mitigation strategies implemented. In an effort to combat cybercrime and protect digital security this writing uses the octave framework method. The results of this study show that by using the octave framework, companies can effectively identify and manage the risk of cyberattacks. Implementation of this framework not only improves information security, but also provides a systematic and structured approach to cyber threats, thereby strengthening the company's resilience to future attacks. After the establishment of the National Cyber and Password Agency (BSSN) in 2017, BSSN Indonesia received numerous reports related to cyber attacks both in the private corporate and government spheres. Thus, the research has made important contributions in the field of cyber risk management and can serve as a benchmark for information technology companies in developing more reliable security systems.

Keywords: *Risk analysis, cyber attacks, information technology companies, octave, cybersecurity*



DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS.....	2
KATA PENGANTAR.....	3
ABSTRAK.....	4
DAFTAR GAMBAR.....	6
DAFTAR TABEL.....	7
BAB 1 PENDAHULUAN.....	8
1.1 Latar belakang.....	8
1.2 Rumusan masalah.....	10
1.3 Batasan masalah.....	11
1.4 Tujuan Penelitian.....	11
1.5 Manfaat.....	11
1.6 Sistematika pembahasan.....	12
BAB 2 TINJAUAN PUSTAKA.....	12
2.1 Pengertian Risiko Siber dan Ancaman Siber.....	13
2.2 Metode Analisis Risiko Siber.....	13
2.3 Implementasi Teknologi Keamanan.....	13
2.4 Kebijakan dan Prosedur Keamanan.....	13
2.5 Pentingnya Pelatihan dan Kesadaran Karyawan.....	14
2.6 Evaluasi dan Peningkatan Berkelanjutan.....	14
2.7 Dasar Teori & Formula.....	14
BAB 3 METODOLOGI.....	18
3.1 Penjelasan Tahapan mengacu dari gambar.....	19
3.2 Langkah-Langkah Metodologi Data Kualitatif.....	20
BAB 4 HASIL.....	1
4.1 Identifikasi Risiko.....	3
4.2 Analisis Risiko.....	4
4.3 Mitigasi Risiko.....	5
4.4 Pemantauan dan Tinjauan.....	5
BAB 5 PEMBAHASAN.....	7
BAB 6 PENUTUP.....	11
DAFTAR PUSTAKA.....	12



DAFTAR GAMBAR

Gambar 1 - Lingkaran Risiko.....	16
Gambar 2 - Alur Kerangka Pemikiran	18
Gambar 3 - Flowchart	19
Gambar 4 - Kata Kunci Mengurangi Risiko	22
Gambar 5 - Hasil Desain di Android Studio	2
Gambar 6 - Hasil Kerangka di Android Studio.....	2
Gambar 7 - Alert Attack Cyber	3
Gambar 8 - Presentase Perusahaan yang sering terkena Serangan Siber.....	8



DAFTAR TABEL

Tabel 1 - Cyber Security trends 2024.....	11
Tabel 2 - Perbandingan Hasil Penelitian Dahulu	17
Tabel 3 - Perbandingan Jurnal.....	22
Tabel 4 - Struktur Inti Kerja.....	1
Tabel 5 - Evaluasi Risiko Dampak & Probabilitas	4
Tabel 6 - Jenis-jenis Serangan.....	6
Tabel 7 - Nama Perusahaan yang sering terkena Serangan Siber	10

