

**PERANCANGAN TIM SIAP TANGGAP INSIDEN SIBER-
CSIRT: STUDI KUALITATIF BERDASARKAN BUSINESS
IMPACT ANALYSIS DI BANK SUMSEL BABEL**



TESIS

**HENDRA YADA PUTRA
ENTERPRISE IT INFRASTRUCTURE
192420034**

**PROGRAM STUDI TEKNIK INFORMATIKA – S2
PROGRAM PASCA SARJANA
UNIVERSITAS BINA DARMA
PALEMBANG
2023**

**PERANCANGAN TIM SIAP TANGGAP INSIDEN SIBER-
CSIRT: STUDI KUALITATIF BERDASARKAN BUSINESS
IMPACT ANALYSIS DI BANK SUMSEL BABEL**

**Tesis ini diajukan sebagai salah satu syarat
Untuk memperoleh gelar**

MAGISTER KOMPUTER



**HENDRA YADA PUTRA
ENTERPRISE IT INFRASTRUCTURE
192420034**

**PROGRAM STUDI TEKNIK INFORMATIKA – S2
PROGRAM PASCA SARJANA
UNIVERSITAS BINA DARMA
PALEMBANG
2023**

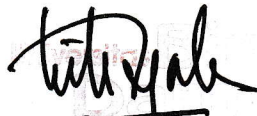
Halaman Pengesahan Pembimbing Tesis

Judul Tesis: PERANCANGAN TIM SIAP TANGGAP INSIDEN SIBER-CSIRT:
STUDI KUALITATIF BERDASARKAN BUSINESS IMPACT
ANALYSIS DI BANK SUMSEL BABEL

Oleh HENDRA YADA PUTRA NIM 192420034 Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika - S2 konsentrasi Enterprise IT Infrastructure, Program Pascasarjana Universitas Bina Darma pada 12 September 2023 dan telah dinyatakan LULUS.

Mengetahui,
Program Studi Teknik Informatika - S2
Universitas Bina Darma

Ketua,

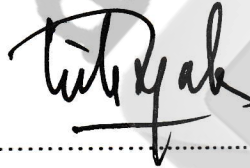


Magister Teknik Informatika

M. Izman Herdiansyah, M.M., Ph.D.



Pembimbing



M. Izman Herdiansyah, M.M., Ph.D.

Halaman Pengesahan Penguji Tesis

Judul Tesis: PERANCANGAN TIM SIAP TANGGAP INSIDEN SIBER-CSIRT:
STUDI KUALITATIF BERDASARKAN BUSINESS IMPACT
ANALYSIS DI BANK SUMSEL BABEL

Oleh HENDRA YADA PUTRA NIM 192420034 Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika - S2 konsentrasi Enterprise IT Infrastructure, Program Pascasarjana Universitas Bina Darma pada 12 September 2023 dan telah dinyatakan LULUS.

Palembang, 12 September 2023

Mengetahui,

Program Pascasarjana
Universitas Bina Darma

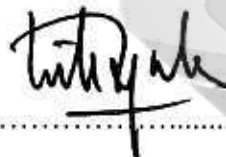
Direktur,



Prof. Hj. Isnawijayani, M.Si., Ph.D.

Tim Penguji :

Penguji I,



M. Izman Herdiansyah, M.M., Ph.D.

Penguji II,



Dr. Tata Sutabri, S.Kom., MMSI.

Penguji III,



Dr. Yesi Novaria Kunang, S.T., M.Kom.

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : HENDRA YADA PUTRA

NIM : 192420034

Dengan ini menyatakan bahwa:

1. Karya tulis Saya Tesis ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik Magister di Universitas Bina Darma;
2. Karya tulis ini murni gagasan, rumusan dan penelitian Saya sendiri dengan arahan tim pembimbing;
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar pustaka;
4. Karena yakin dengan keaslian karya tulis ini, Saya menyatakan bersedia Tesis yang Saya hasilkan di unggah ke internet;
5. Surat Pernyataan ini Saya tulis dengan sungguh-sungguh dan apabila terdapat penyimpangan atau ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima sanksi dengan aturan yang berlaku di perguruan tinggi ini.

Demikian Surat Pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 12 September 2023
Yang Membuat Pernyataan,



HENDRA YADA PUTRA
NIM : 192420034

ABSTRAK

Perancangan tim Siap Tanggap Insiden Siber-CSIRT: studi kualitatif berdasarkan Business Impact Analysis di PT. Bank Sumsel Babel adalah judul tesis yang diambil oleh peneliti, dimana judul ini diangkat karena semua insiden keamanan siber dikelola oleh Divisi Teknologi Informasi dan belum ada batasan secara spesifik menangani insiden siber khusus skala besar, dalam hal ini terkait dengan pembentukan Tim kerja dengan fungsi yang tidak hanya melakukan pemulihan insiden secara teknis saja, melainkan juga secara berkolaboratif dari sisi non teknis, mengingat reputasi bank dipertaruhkan saat pemulihan insiden keamanan berlangsung, selain itu perlu adanya pengaturan secara spesifik mengenai alur kerja, Lingkup layanan dan limit dampak yang akan menjadi trigger kapan tim ini akan mulai bekerja, sehingga peneliti merasa perlu untuk melakukan penelitian dengan tujuan untuk mengembangkan pengelolaan Insiden Keamanan Siber yang lebih efektif dan efisien dalam bentuk perencanaan Tim Siap Tanggap Insiden Siber (TTIS), atau lebih dikenal dengan Computer Security Incident response Team (CSIRT) yang mengacu pada tingkat kritikalitas pada analisis Business Impact Analysis (BIA). Dalam penelitiannya sendiri peneliti mengacu pada standard ISO/TS 22317:2021 sebagai panduan analisis BIA dan ISO/IEC 27035:2023 dalam penyusunan kerja Tim TTIS.

Kata kunci: BIA, CSIRT, Tim Tanggap Insiden Siber, Kritikalitas

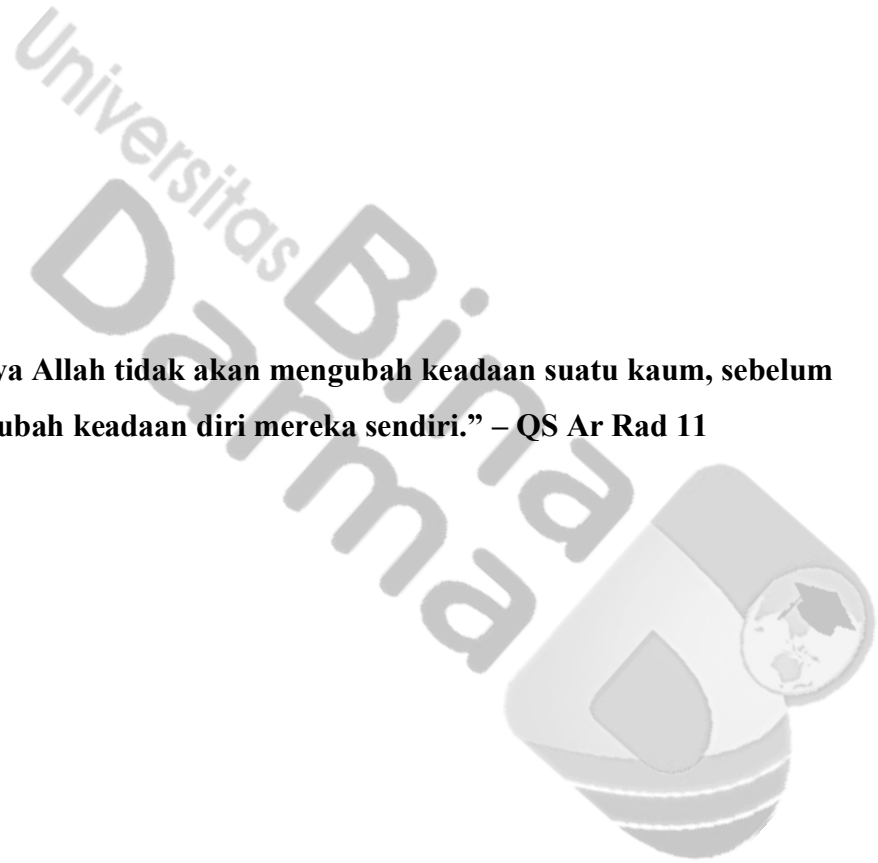
ABSTRACT

Design of Cyber Incident Response Team-CSIRT: a qualitative study based on Business Impact Analysis at Bank Sumsel Babel is the title of the thesis taken by researchers, where this title was chosen because all cyber security incidents are managed by the Information Technology Division and there are no specific restrictions on handling cyber incidents especially on a large scale, in this case related to the formation of a work team with a function that does not only carry out technical incident recovery, but also collaboratively from a non-technical perspective, bearing in mind that the bank's reputation is at stake when security incident recovery takes place, besides that it is necessary to have specific arrangements regarding workflow, scope of service and impact limits that will be the trigger when this team will start working, so researchers feel the need to conduct research with the aim of developing a more effective and efficient management of Cyber Security Incidents in the form of planning a Tim Tanggap Insiden Siber (TTIS), or known as the Computer Security Incident Response Team (CSIRT) which refers to the level of criticality in the Business Impact Analysis (BIA) analysis. In his own research, the researcher refers to the ISO/TS 22317:2021 standard as a guide for BIA analysis and ISO/IEC 27035:2023 in preparing the work of the TTIS Team.

Keywords: *BIA, CSIRT, TTIS, Criticality*

MOTTO

“Sesungguhnya Allah tidak akan mengubah keadaan suatu kaum, sebelum mereka mengubah keadaan diri mereka sendiri.” – QS Ar Rad 11



KATA PENGANTAR

Pertama-tama saya panjatkan puji dan syukur kehadirat Allah SWT yang telah memberikan keimanan, kesehatan, kekuatan dan kesabaran didalam menyelesaikan studi ini. Tidak lupa juga sholawat serta salam saya haturkan kepada nabi mulia nabi Muhammad SAW, keluarga, sahabat, hingga umatnya hingga akhir zaman. Selanjutnya, terima kasih yang tidak akan pernah lupa seumur hidup saya kepada orang tua dan mertua saya tercinta, atas motivasi, dukungan, dan doa yang selalu dipanjatkan dalam setiap sholat supaya saya selalu dimudahkan dalam setiap urusan dan menjalani kehidupan ini dengan penuh restu orang tua.

Saya ucapkan juga terima kasih kepada keluarga tercinta, istri saya Ida Anika Ariani yang selalu sabar, memberikan semangat, doa dan dorongan agar saya selalu maju dan motivasu untuk meyelesaikan studi ini, kemudian juga untuk anak saya Ghaisan Ziyad Arrafif yang sering memberikan kejutan membanggakan, Ghea Zivana Assahlah yang selalu ceria sehingga menghibur hati dan Ghataf Ziyad Arrafif yang selalu lucu dan menggemaskan, sehingga saya lupa akan aktivitas yang menghabiskan waktu saya selama bekerja dari pagi sampai pulang sore hari. Tidak lupa juga saya ucapkan terima kasih kepada sahabat saya satu angkatan Ichan yang selalu memberikan semangat dan dukungan.

Selanjutnya, saya ucapkan terima kasih kepada pembimbing saya yang juga selaku Kaprodi Magister Teknik Informatika, M. Izman Herdiansyah, M.M., Ph.D., atas motivasi, dukungan dan sharing pengalaman serta ilmu-ilmunya mengenai tesis ini, khususnya didalam menyusun setiap bab dan juga publikasi jurnal, sehingga penelitian ini dapat selesai. Saya ucapkan juga terima kasih juga kepada Ibu Rektor Universitas Bina Darma Palembang, Dr. Sunda Ariana, M.Pd., M.M. yang telah memberikan kesempatan untuk menuntut ilmu dilembaga ini. Ucapan terima kasih kepada bapak-bapak dan Ibu dosen Pasca Sarjana Teknik Informatika khususnya yang telah memberikan materi dan sharing ilmunya kepada saya. Saya juga ucapkan terima kasih kepada tim sekretariat pasca sarjana khususnya Sdr. Dendi yang telah memberikan dukungan dan pelayanan dengan sangat baik bagi saya sehingga dapat memudahkan saya menyelesaikan studi di Kampus Bina Darma.

Tidak lupa juga saya ucapkan terima kasih kepada Bapak Rofalino Kurnia selaku Pemimpin Divisi Management Risiko dan Bapak Indra Erawan selaku Pemimpin Bagian Profil Risiko Operasional dan TSI atas dukungan, nasehat, dorongan dan semangat sehingga membantu penelitian ini dengan baik. Ucapan terima terima kasih juga untuk teman-teman saya angkatan 21/B semoga semuanya menjadi pribadi yang memberikan kemanfaatan bagi orang lain.

Terima kasih untuk semuanya.



DAFTAR ISI

KATA PENGANTAR.....	1
DAFTAR ISI.....	3
DAFTAR TABEL	5
DAFTAR GAMBAR.....	6
BAB I PENDAHULUAN.....	7
1.1 Latar Belakang	7
1.2 Identifikasi Masalah	11
1.3 Batasan Masalah.....	11
1.4 Rumusan Permasalahan.....	11
1.5 Tujuan Penelitian.....	12
1.6 Manfaat Penelitian.....	12
1.7 Susunan Dan Struktur Penelitian.....	13
BAB II LANDASAN TEORI	14
2.1. Sistem Keamanan Siber	14
2.2. Serangan Siber (Cyber Attack)	14
2.3. Cyber Security Maturiy	15
2.4. Resiko dan Bisnis Impact Analysis	16
2.4.1. Identifikasi Resiko.....	16
2.4.2. Ancaman resiko	17
2.4.3. BIA	18
2.5. Standar Keamanan ISO/IEC 27001 & ISO/IEC 27035	22
2.5.1. ISO/IEC 27001	22
2.5.2. Standard ISO/IEC 27035.....	23
2.6. Penelitian Terdahulu	26
BAB III METODOLOGI PENELITIAN	28
3.1. Pendekatan Penelitian	28
3.2. Tempat dan Waktu Penelitian	29
3.3. Teknik dan Metode Pengumpulan Data	29
3.3.1. Wawancara	30
3.3.2. Studi Pustaka	30
3.4. Instrument Penelitian.....	30
3.5. Teknik Analisis Data	31
3.6. Jadwal Penelitian	32

BAB IV HASIL DAN PEMBAHASAN	33
4.1. Hasil Analisis BIA	33
4.1.1. Penentuan Tipe Area Dampak dan Tingkat Area Dampak.....	33
4.1.2. Penentuan parameter Frame waktu	35
4.1.3. Penentuan Kriteria MTD (Maximum Tolerable Downtime)	35
4.1.4. Kertas Kerja.....	35
4.1.5. Penentuan kelompok Tingkat Kritikalitas	36
4.1.6. Hasil Analisis	37
4.2. Hasil Penyusunan Tim	39
4.3. Hasil Penyusunan Alur Kerja Tim	39
4.3.1 Alur kerja eksisting	39
4.3.2 Hasil pengembangan Alur Kerja tim.....	40
4.4. Hasil Analisa untuk Lingkup kerja TTIS/CSIRT	42
4.4.1. Pengelolaan Insiden Keamanan Siber dengan dampak berskala besar	43
4.4.2. Lingkup Pengelolaan Insiden Tim TTIS/CSIRT	44
BAB V KESIMPULAN DAN SARAN	45
5.1 Kesimpulan.....	45
5.2 Saran	45
DAFTAR PUSTAKA	46

DAFTAR TABEL

Tabel 2.1. Parameter Waktu.....	20
Tabel 2.2. Parameter Dampak Berdasarkan Aspek Area.....	21
Tabel 3.1. Kertas Kerja BIA	28
Tabel 3.2. Jadwal Penelitian.....	32
Tabel 4.1. Parameter Kriteria Tingkat Dampak.....	33
Tabel 4.2. Parameter Kriteria tingkat dampak berdasarkan Area Dampak.....	34
Tabel 4.3. Parameter frame waktu	35
Tabel 4.4. Parameter MTD.....	35
Tabel 4.5. Tabel Tingkat Kritikalitas	37
Tabel 4.6. Tabel Hasil BIA	38
Tabel 4.7. Parameter Limit Dampak TTIS/CSIRT	43
Tabel 4.8. Group Proses Bisnis Kritikalitas Tinggi	44

DAFTAR GAMBAR

Gambar 1.1 Laporan Risk Global 2023	9
Gambar 2.1. Hasil Pengukuran Kematangan Keamanan Siber.....	16
Gambar 2.2. BCM berdasarkan ISO 22313	18
Gambar 4.1 Struktur Tim TTIS/CSIRT	39
Gambar 4.2. Alur Kerja Eksisting Pengelolaan Insiden	40
Gambar 4.3. Alur Kerja Pengembangan Pengelolaan Insiden	41
Gambar 4.4. Detil Alur Kerja Pengembangan Pengelolaan Insiden	42

