

**PERENCANAAN ISO 27001 DALAM MENGAMANKAN JARINGAN
PADA UNIVERSITAS BINA DARMA**

RIDWAN WAHYU M

15.142.0174

Skripsi ini diajukan sebagai syarat memperoleh gelar Sarjana Komputer



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BINA DARMA PALEMBANG**

2019



**PERENCANAAN ISO 27001 DALAM MENGAMANKAN JARINGAN
PADA UNIVERSITAS BINA DARMA**

RIDWAN WAHYU M

15.142.0174

Skripsi ini diajukan sebagai syarat memperoleh gelar Sarjana Komputer

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS BINA DARMA PALEMBANG

2019

HALAMAN PENGESAHAN

**PERENCANAAN ISO 27001 DALAM MENGAMANKAN JARINGAN
PADA UNIVERSITAS BINA DARMA**

RIDWAN WAHYU M

15.142.0174

**Telah diterima sebagai salah satu syarat untuk memperoleh gelar Sarjana
Komputer pada Program Studi Teknik Informatika**

Palembang, 9 September 2019

Fakultas Ilmu Komputer

Universitas Bina Darma

Pembimbing,



M. Izman Herdiansyah, S.T., M.M., PhD

Dekan,



Dedy Syamsuar, PhD

HALAMAN PERSETUJUAN

Skripsi Berjudul “Perencanaan ISO 27001 Dalam Mengamankan Jaringan Pada Universitas Bina Darma” Oleh “Ridwan Wahyu M”, telah dipertahankan didepan komisi penguji pada hari Selasa tanggal 27 Agustus 2019.

Komisi Penguji

- | | | |
|------------|--|---------|
| 1. Ketua | : M. Izman Herdiansyah, S.T., M.M., Ph.D | (.....) |
| 2. Anggota | : Darius Antoni, S.Kom., M.M., Ph.D | (.....) |
| 3. Anggota | : M. Akbar, S.T., M.IT. | (.....) |

Mengetahui,

Program Studi Teknik Informatika

Fakultas Ilmu Komputer

Universitas Bina Darma

Ketua,

Universitas Bina Darma
Fakultas Ilmu Komputer

A. Haidar Mirza, S.T., M.Kom

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

NAMA : Ridwan Wahyu . M

NIM : 151420174

Dengan ini menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik Sarjana di Universitas Bina Darma atau di Perguruan Tinggi lain.
2. Skripsi ini murni gagasan, rumusan dan penelitian saya sendiri dengan arahan tim pembimbing.
3. Di dalam Skripsi ini tidak terdapat karya atau pendapat yang telah di tulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukan ke dalam daftar rujukan.
4. Saya bersedia Skripsi yang saya hasilkan di cek keasliannya menggunakan *plagiarism checker* serta diunggah ke internet, sehingga dapat diakses publik secara daring.
5. Surat pernyataan ini saya tulis dengan sungguh – sungguh dan apabila terbukti melakukan penyimpangan atau ketidakbenaran dalam pernyataan ini, saya bersedia menerima sanksi sesuai dengan peraturan dan perundang – undangan yang berlaku.

Demikianlah surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 9 Agustus 2019

Yang membuat Pernyataan,



Ridwan Wahyu . M

NIM : 151420174

MOTTO

Tidak ada masalah yang tidak bisa diselesaikan selama ada komitmen untuk menyelesaikannya



Sesungguhnya bersama kesulitan ada kemudahan, maka apabila engkau telah selesai (dari sesuatu urusan), tetaplah bekerja keras (untuk urusan yang lain). Dan hanya kepada Tuhanmulah engkau berharap

HALAMAN PERSEMBAHAN

Skripsi / Tugas Akhir ini saya persembahkan kepada:

- Allah SWT atas segala kenikmatan dan ridha-Nya serta memberikan kelancaran, dipermudahkannya dalam segala hal sehingga saya dapat menyelesaikan skripsi ini dengan lancar walaupun sering dihadapkan dengan berbagai macam masalah
- Kedua Orang Tua (Bapak dan Ibu) yang telah membesarkan, mendidik, menyayangi, dan memberikan do'a yang terbaik untukku. Terimakasih untuk semua pengorbanan dan jerih payah bapak dan ibu lakukan.
- Kedua Adik ku (Ahlun Naza dan Uswatun Hasannah) yang selalu menjadi semangat untuk membuat diriku menjadi lebih baik agar bisa menjadi contoh yang baik pula untuknya.
- Keluarga Besar Ida Kemis, dan keluarga besar H. Tenggenah M yang telah memberikan motivasi dan menjadi penyemangat.
- Dosen pembimbing yang saya hormati dan banggakan Bapak M.Izman Herdiansyah, S.T., M.M., PhD yang telah memberikan bimbingan serta saran dalam penyusunan skripsi ini sampai selesai.
- Dosen bagian DSTI yang telah memberikan masukan tentang penyusunan skripsi, Bapak Suryayusra, M.Kom
- Teman – teman satu kosan dan seperjuangan Jiko Oktodi (Wong_Itam), M. Wahyudin (Wong_Layo), Fijay, Sela, Miss Nora Waroka terimakasih atas *support* yang telah kalian berikan.
- Team Kos KM5 Kak Deni Irwanda (Pak Rete), Juwanda Prasetya (Om Joe), Nasrul (Pororo / Tole), Nia, serta sahabatku sekaligus sudah seperti keluarga Ebta Sari Hidayat (Memet) yang telah memberikan motivasi sehingga bisa menyelesaikan skripsi ini.

KATA PENGANTAR

Puji syukur kehadiran Allah SWT karena berkat rahmat dan karunia-Nya jualah, skripsi ini dapat diselesaikan guna memenuhi salah satu syarat untuk diteruskan menjadi skripsi sebagai proses akhir dalam menyelesaikan pendidikan dibangku kuliah.

Dalam penulisan skripsi ini, tentunya masih jauh dari sempurna. Hal ini dikarenakan keterbatasnya pengetahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan skripsi ini diharapkan adanya saran dan kritik yang diberikan bersifat membangun.

Pada kesempatan yang baik ini, tak lupa penulis menghaturkan terima kasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasehat dan pemikiran dalam penulisan skripsi ini, terutama kepada :

1. Dr. Sunda Ariana, M.Pd., M.M. selaku Rektor Universitas Bina Darma Palembang
2. Dedy Syamsuar, PhD. selaku Dekan Fakultas Ilmu Komputer
3. A. Haidar Mirza, S.T., M.Kom., selaku Ketua Program Studi Informatika.
4. M. Izman Herdiansyah, S.T., M.M., PhD., selaku Pembimbing I yang telah memberikan bimbingan penulisan proposal ini.
5. Orang Tua, saudara-saudaraku, seluruh teman dan sahabat-sahabatku yang selalu memberikan dorongan dan masukan serta bantuan baik moril maupun material yang tak ternilai harganya

Palembang, 12 April 2019

Penulis

ABSTRAK

Semakin berkembangnya teknologi komunikasi pada saat ini maka kebutuhan akan keamanan dalam berkomunikasi jadi sangat penting. Maka penulis melakukan penelitian ini bertujuan untuk mengamankan jaringan universitas bina darma dengan menggunakan ISO 27001 untuk mengamankan jaringan tersebut. Jaringan sendiri memiliki beberapa jenis, yaitu LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), WAN (*Wide Area Network*), Internet, dan Jaringan tanpa kabel. ISO 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan serta menerapkan keamanan data atau informasi pada jaringan. Dalam mengamankan jaringan Universitas Bina Darma ISO 27001 sangat dibutuhkan agar meminimalkan kehilangan data pada saat melakukan akses pada jaringan. Keamanan jaringan adalah suatu tindakan yang dilakukan untuk mengamankan suatu jaringan dari ancaman-ancaman baik dari fisik maupun teknis. Tujuan dari penelitian ini menyusun konsep dasar dan menyusun rekomendasi tata kelola keamanan jaringan yang baik dan sesuai dengan standard ISO 27001. Metode penelitian yang digunakan yaitu penelitian deskriptif, metode pengumpulan data yang digunakan yaitu observasi, wawancara, dan kuesioner untuk mengumpulkan data-data yang dibutuhkan dalam melakukan penelitian.

Kata kunci: ISO 27001, Keamanan Jaringan, Jaringan

DAFTAR ISI

HALAMAN JUDUL	II
HALAMAN PENGESAHAN.....	III
HALAMAN PERSETUJUAN	IV
SURAT PERNYATAAN	V
MOTTO	VI
HALAMAN PERSEMBAHAN	VII
KATA PENGANTAR.....	VIII
ABSTRAK	IX
DAFTAR ISI.....	X
DAFTAR GAMBAR.....	XV
DAFTAR TABEL	XV
BAB I.....	1
PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metodologi Penelitian	3

1.7 Sistematika Penulisan.....	4
BAB II	6
TINJAUAN PUSTAKA	6
2.1 Tinjauan Umum.....	6
2.1.1 Sejarah Universitas Bina Darma	6
2.2 Landasan Teori.....	7
2.2.1 ISO 27001	7
2.2.2 Jaringan	12
2.2.3 Keamanan Jaringan	14
2.3 Penelitian Sebelumnya	15
2.4 Kerangka Berpikir	16
BAB III.....	17
METODOLOGI PENELITIAN	17
3.1 Tempat dan Waktu Penelitian	17
3.2 Alat dan Bahan	17
3.2.1 Perangkat Keras (<i>Hardware</i>)	17
3.2.2 Perangkat Lunak (<i>Software</i>).....	17
3.3 Metode Penelitian.....	18
3.4 Metode Pengumpulan Data	18
3.5 Metode Analisis Data	19
BAB IV	20
HASIL DAN PEMBAHASAN	20
4.1 Risk Management Proses	20
4.1.1 Mengidentifikasi Asset Informasi	22

4.1.1.1	Proses Informasi di Universitas Bina Darma	22
4.1.1.2	Identifikasi Informasi Kritis	25
4.1.2	Kuantifikasi dan Kualifikasi Ancaman	25
4.1.2.1	Identifikasi Ancaman Teknis dan Fisik.....	25
4.1.2.2	Identifikasi ancaman komponen proses	26
4.1.3	Nilai Kerentanan	27
4.1.3.1	Identifikasi Kontrol yang berhubungan dengan ancaman.....	27
4.1.4	Memulihkan Kesenjangan Kontrol	27
4.1.5	Mengelola Sisa Resiko	28
4.2	Klausul ISO 27001	28
4.2.1	Klausul A.5 Kebijakan Keamanan	34
4.2.1.1	Klausul A.5.1 Kebijakan Keamanan Informasi.....	34
4.2.1.1.1	Klausul A.5.1.1 Dokumen Kebijakan Keamanan Informasi.....	34
4.2.1.1.2	Klausul A.5.2 Tinjauan Kebijakan Keamanan Informasi.....	37
4.2.2	Klausul A.9 Keamanan Fisik dan Lingkungan	37
4.2.2.1	Klausul A.9.1 Keamanan Wilayah	37
4.2.2.1.1	Klausul A.9.1.1 Batas Keamanan Fisik.....	38
4.2.2.1.2	Klausul A.9.1.2 Kontrol Masuk ke Fisik.....	38
4.2.2.1.3	Klausul A.9.1.3 Keamanan Kantor, Ruangan dan Fasilitas	39

4.2.2.1.4	Klausul A.9.1.4 Perlindungan dari ancaman Pihak Luar dan Lingkungan sekitarnya.....	40
4.2.2.1.5	Klausul A.9.1.5 Bekerja di Wilayah yang aman.....	40
4.2.2.1.6	Klausul A.9.1.2 Akses Publik, Wilayah Pengiriman dan Pemuatan Barang.....	41
4.2.2.2	Klausul A.9.2 Keamanan Peralatan.....	41
4.2.2.2.1	Klausul A.9.2.1 Penempatan dan Perlindungan Peralatan	41
4.2.2.2.2	Klausul A.9.2.2 Utilitas Pendukung	42
4.2.2.2.3	Klausul A.9.2.3 Keamanan Pengkabelan	42
4.2.2.2.4	Klausul A.9.2.4 Pemeliharaan Peralatan	43
4.2.2.2.5	Klausul A.9.2.5 Keamanan Peralatan di luar lokasi Organisasi.....	43
4.2.2.2.6	Klausul A.9.2.6 Keamanan Pembuangan atau Penggunaan kembali Peralatan	44
4.2.2.2.7	Klausul A.9.2.7 Pemindahan Peralatan	45
4.2.3	Klausul A.11 Kontrol Akses	45
4.2.3.1	Klausul A.11.1 Persyaratan untuk Kontrol Akses.....	45
4.2.3.1.1	Klausul A.11.1.1 Kebijakan Kontrol Akses	45
4.2.3.2	Klausul A.11.2 Manajemen Akses Pengguna	46
4.2.3.2.1	Klausul A.11.2.1 Pendaftaran Pengguna.....	46
4.2.3.2.2	Klausul A.11.2.2 Manajemen Hak Istimewa.....	46
4.2.3.3	Klausul A.11.3 Tanggung Jawab Pengguna.....	47

4.2.3.3.1	Klausul A.11.3.1 Penggunaan kata sandi	47
4.2.3.4	Klausul A.11.4 Kontrol Akses Jaringan	47
4.2.3.4.1	Klausul A.11.4.1 Kebijakan Tentang Penggunaan Layanan Jaringan	47
4.2.3.4.2	Klausul A.11.4.2 Otentikasi Pengguna untuk koneksi Eksternal.....	48
4.2.3.4.3	Klausul A.11.4.3 Identifikasi Peralatan dalam Jaringan.....	48
4.2.3.4.4	Klausul A.11.4.4 Diagnostik jarak jauh dan Proteksi Port Konfigurasi	49
4.2.3.4.5	Klausul A.11.4.5 Pemisahan dalam Jaringan	49
4.2.3.4.6	Klausul A.11.4.6 Kontrol Koneksi Jaringan.....	49
4.2.3.4.7	Klausul A.11.4.7 Kontrol Perutean Jaringan.....	50
4.3	Hasil.....	50
BAB V	53
KESIMPULAN DAN SARAN	53
5.1	Kesimpulan.....	53
5.2	Saran.....	53

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.4 Kerangka Berfikir	16
Gambar 4.1.1 Topologi Jaringan Universitas Bina Darma	23

DAFTAR TABEL

Tabel 4.1 Tabel Risk Management.....	21
Tabel 4.2 Tabel Klausul ISO 27001	34