



**PERANCANGAN *IT RISK CONTROL* PADA LABORATORIUM
KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS
PEMBANGUNAN NASIONAL VETERAN JAKARTA
MENGUNAKAN *FRAMEWORK* ISO 27001:2022**

SKRIPSI

**MUHAMAD RONALD LULLAH
2010511002**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”
JAKARTA
2024**



**PERANCANGAN *IT RISK CONTROL* PADA LABORATORIUM
KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS
PEMBANGUNAN NASIONAL VETERAN JAKARTA
MENGUNAKAN *FRAMEWORK* ISO 27001:2022**

**SKRIPSI
DIAJUKAN SEBAGAI SALAH SATU SYARAT UNTUK
MEMPEROLEH GELAR SARJANA KOMPUTER**

**MUHAMAD RONALD LULLAH
2010511002**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”
JAKARTA
2024**

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Muhamad Ronald Lullah

NIM : 2010511002

Tanggal : 06 Juni 2024

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 06 Juni 2024

Yang Menyatakan,



(Muhamad Ronald Lullah)

**PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan dibawah ini.

Nama : Muhamad Ronald Lullah

NIM : 2010511002

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta. Hak Bebas Royalti Non Eksklusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul “PERANCANGAN IT *RISK CONTROL* PADA LABORATORIUM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA MENGGUNAKAN *FRAMEWORK* ISO 27001:2022.”

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 14 Juli 2024

Yang menyatakan,



(Muhamad Ronald Lullah)

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Skripsi ini diajukan oleh:

Nama : Muhamad Ronald Lullah
NIM : 2010511002
Program Studi : S-1 Informatika
Judul Skripsi/TA : Perancangan IT *Risk Control* Pada Laboratorium
Komputer Fakultas Ilmu Komputer Universitas
Pembangunan Nasional Veteran Jakarta Menggunakan
Framework ISO 27001:2022

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



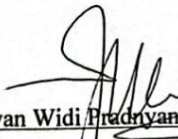
Henki Bayu Seta, S.Kom., M.TI

Penguji 1



Hamonangan Kinantan Prabu, S.T., M.T.

Penguji 2



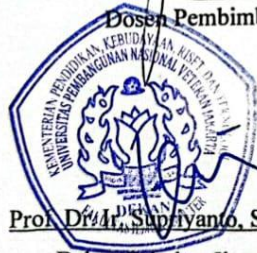
I Wayan Widi Pradnyana, S.Kom., M.TI

Dosen Pembimbing I



Novi Trisman Hadi, S.Pd., M.Kom.

Dosen Pembimbing II



Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM

Dekan Fakultas Ilmu Komputer



Dr. Widya Cholil, M.I.T

Kepala Program Studi S1 Informatika

Ditetapkan di : Jakarta

Tanggal Persetujuan : 5 Juli 2024

**PERANCANGAN *IT RISK CONTROL* PADA LABORATORIUM
KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS
PEMBANGUNAN NASIONAL VETERAN JAKARTA MENGGUNAKAN
*FRAMEWORK ISO 27001:2022***

MUHAMAD RONALD LULLAH

ABSTRAK

Perguruan tinggi merupakan tempat dimana mahasiswa dan pemangku kepentingan lain datang untuk mencari ilmu pengetahuan, oleh karena itu sudah menjadi kewajiban perguruan tinggi untuk memanfaatkan teknologi informasi dan komunikasi secara bijak dalam menunjang berbagai aktivitas. Penting untuk menerapkan kebijakan keamanan informasi untuk melindungi aset yang dimiliki universitas. Pengkajian *IT Risk Control* Laboratorium Komputer Fakultas Ilmu Komputer UPNVJ (Universitas Pembangunan Nasional Veteran Jakarta) merupakan penelitian merekomendasi kontrol semua risiko yang ada pada organisasi dan aset yang menyebabkan ancaman kerusakan, kehilangan serta memperhitungkan kemungkinan yang dapat memberikan dampak kerugian bagi keberlangsungan operasional instansi pendidikan. Penelitian ini menggunakan ketentuan ISO 27001:2022 dengan metodologi didalamnya PDCA (*Plan, Do, Check, Act*) dalam rangka mengelola keamanan teknologi informasi. Hasil dari penelitian ini menguraikan sebuah studi yang dilakukan untuk mengevaluasi dan meningkatkan kontrol risiko keamanan informasi di Laboratorium Komputer Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Kata kunci: ISO 27001:2022, PDCA, Keamanan Informasi, Kontrol Risiko Teknologi Informasi.

**DESIGN OF IT RISK CONTROL IN THE COMPUTER LABORATORY
OF THE FACULTY OF COMPUTER SCIENCE, UNIVERSITAS
PEMBANGUNAN NASIONAL VETERAN JAKARTA USING THE ISO
27001:2022 FRAMEWORK (2024)**

MUHAMAD RONALD LULLAH

ABSTRACT

Universities are places where students and other stakeholders come to seek knowledge, therefore it is the obligation of universities to utilize information and communication technology wisely in supporting various activities. It is important to implement an information security policy to protect the assets owned by the university. The IT Risk Control Assessment of the Computer Laboratory of the Faculty of Computer Science UPNVJ (Universitas Pembangunan Nasional Veteran Jakarta) is a research that recommends the control of all risks that exist in organizations and assets that cause threats of damage, loss and take into account the possibility that can have a loss impact on the operational sustainability of educational institutions. This research uses the ISO 27001: 2022 Framework with the PDCA (Plan, Do, Check, Act) methodology in order to manage information technology security. The results of this research outline a study conducted to evaluate and improve information security risk control in the Computer Laboratory of the Faculty of Computer Science, Universitas Pembangunan Nasional Veteran Jakarta.

Keywords: ISO 27001:2022, PDCA, Information Security, IT Risk Control

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa, karena hanya atas berkat dan rahmat-Nya, sehingga laporan tugas skripsi informatika yang berjudul “Perancangan *IT Risk Control* Pada Laboratorium Komputer Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta Menggunakan *Framework ISO 27001:2022*” dapat diselesaikan dengan baik dan tepat waktu. Untuk itu pada kesempatan ini penulis menyampaikan rasa terima kasih kepada yang terhormat:

1. Ayah dan Ibu yang selalu mendukung tiada henti serta mendoakan penuh untuk tercapai selesainya tugas akhir skripsi ini
2. Bapak I Wayan Widi Pradnyana, S.Kom.,MTI selaku dosen pembimbing pertama yang telah memberikan banyak masukan dan saran dalam proses pembuatan laporan tugas akhir skripsi ini.
3. Bapak Novi Trisman Hadi, S.pd., M.Kom selaku pembimbing kedua yang telah memberikan banyak masukan, saran serta membangun cara berpikir logis dan kritis, dalam proses penyusunan laporan tugas akhir skripsi ini.
4. Ibu Widya Cholil, M.I.T selaku ketua prodi informatika yang telah memberikan kemudahan dan kelancaran dalam pelaksanaan tugas akhir skripsi ini.
5. Terima kasih untuk semua sahabat saya yang selalu memberikan motivasi, dukungan serta doanya yang selalu dipanjatkan untuk kemudahan dalam mengerjakan tugas akhir skripsi ini (Yaman, Kigan, Arya,Thoriq, Piqi, Dicka, Endow, Fiqri, Ferdi, Adhi, Rangga, Wibi, Alvin, dan Fadhil).

Penulis menyadari bahwa laporan tugas akhir skripsi ini masih banyak kekurangan didalamnya, maka kritik dan saran sangat diharapkan penulis untuk perbaikan laporan tugas akhir skripsi ini. Semoga Tuhan Yang Maha Esa memberikan imbalan yang setimpal atas segala bantuan yang diberikan.

Jakarta, 25 Oktober 2023

Penulis



(Muhamad Ronald Lullah)

DAFTAR ISI

COVER	i
PERNYATAAN ORISINALITAS.....	ii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	iii
LEMBAR PENGESAHAN.....	iv
ABSTRAK.....	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN	xiv
DAFTAR RUMUS	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian	3
1.4 Manfaat Penelitian	3
1.5 Batasan Masalah	4
1.6 Luaran Yang Diharapkan.....	6
BAB II TINJAUAN PUSTAKA.....	7
2.1 Sistem Manajemen Keamanan Informasi	7
2.1.1 Definisi Keamanan Informasi	7
2.1.2 Pengertian Sistem Manajemen Keamanan Informasi.....	10
2.1.3 Manfaat SMKI.....	10
2.2 Manajemen Risiko	11
2.2.1 Mengelola Manajemen Risiko (<i>Risk Management</i>)	11
2.2.2 Penelitian Risiko (<i>Risk Assesment</i>).....	12
2.3 Mengelola Sumber Daya Manusia (SDM).....	21
2.4 Manajemen Aset	22
2.4.1 Mengidentifikasi Aset	23
2.5 Kontrol Akses	23

2.6	<i>Framework</i> Keamanan IT (<i>Information Technology</i>) <i>Risk Control</i>	23
2.6.1	Definisi ISO 27001	23
2.6.2	ISO 27001:2022.....	24
2.6.3	Pemetaan Kontrol Objektif ISO 27001:2022.....	25
2.6.4	Metode PDCA (<i>Plan-Do-Check-Act</i>)	25
2.7	Review Penelitian Relevan.....	26
BAB III METODE PENELITIAN		29
3.1	Tahapan Penelitian.....	29
3.2	Studi Literatur.....	30
3.3	Analisa Kebutuhan Masalah.....	30
3.3.1	Wawancara	31
3.3.2	Observasi.....	31
3.3.3	Kuesioner	32
3.3.4	Jenis <i>IT Risk Control</i>	32
3.4	Pembuatan Kontrol Risiko	33
3.5	Evaluasi Kontrol Risiko	35
3.6	Dokumentasi dan Rekomendasi	35
3.7	Alat Bantu Penelitian	36
3.7.1	Perangkat Keras.....	36
3.7.2	Perangkat Lunak.....	37
3.8	Jadwal Penelitian	37
BAB IV HASIL DAN PEMBAHASAN.....		38
4.1	Tahap Rencana (<i>Plan</i>).....	38
4.1.1	Menentukan Ruang Lingkup Keamanan Informasi	38
4.1.2	Menentukan Kebijakan Keamanan Informasi.....	39
4.1.3	Observasi.....	40
4.1.4	Wawancara	40
4.1.5	Kuesioner	41
4.2	Tahap Aksi (<i>Do</i>).....	42
4.2.1	Mengidentifikasi dan Menghitung Nilai Aset	42
4.2.2	Menganalisis dan Mengevaluasi Risiko.....	57
4.3	Tahap Pemantauan (<i>Check</i>).....	61
4.3.1	Pemilihan Objek Kontrol Untuk Pengelolaan Risiko.....	61
4.3.2	Pemeriksaan Aset Secara Langsung	62

4.3.3	Pemeriksaan Aset Barang Milik Negara (BMN).....	63
4.4	Tahap Evaluasi (<i>Act</i>).....	64
4.4.1	Rekomendasi Perbaikan Aset Terhadap Objektif Kontrol Risiko Keamanan Informasi Berdasarkan ISO 27001:2022.....	64
4.4.2	Hasil dan Pembahasan Metode PDCA (<i>Plan, Do, Check, Act</i>) Pada ISO 27001:2022.....	64
4.4.3	Perbedaan <i>Threat Actor</i> dan <i>Attacker</i>	65
4.4.4	<i>Procedure</i> dan <i>Policy IT Risk Control</i> Keamanan Informasi.....	66
4.4.5	Rancangan Dokumen Kebijakan Keamanan <i>IT Risk Control</i>	67
4.5	Pemetaan Matriks Kebijakan <i>IT Risk Control</i> Terhadap Norma atau <i>Annex</i> ISO 27001:2022.....	70
BAB V PENUTUP.....		74
5.1	Kesimpulan.....	74
5.2	Saran.....	75
DAFTAR PUSTAKA		76
LAMPIRAN		78

DAFTAR TABEL

Tabel 2.1 Analisa Dampak	12
Tabel 2.2 penilaian aset pada nilai kerahasiaan (<i>Confidentiality</i>).....	14
Tabel 2.3 penilaian aset pada nilai keutuhan (<i>Integrity</i>).....	14
Tabel 2.4 penilaian aset pada nilai ketersediaan (<i>Avaliability</i>).....	14
Tabel 2.5 <i>Daftar Contoh Kelemahan</i>	15
Tabel 2.6 Daftar Contoh Ancaman.....	16
Tabel 2.7 Contoh Nilai Rerata Probabilitas	18
Tabel 2.8 Nilai Skala dalam <i>Business Impact Analysis (BIA)</i>	19
Tabel 2.9 Review Penelitian Relevan.....	27
Table 3.1 Jadwal Penelitian	37
Table 3.2 Jadwal Mengerjakan Hasil dan Pembahasan.....	37
Tabel 4.1 Pelaksanaan Mencari Informasi.....	40
Tabel 4.2 Nilai Aset LAB Komputer FIK UPNVJ.....	43
Tabel 4.3 Nilai Ancaman Komputer.....	45
Tabel 4.4 Nilai Ancaman Monitor.....	45
Tabel 4.5 Nilai Ancaman Switch.....	46
Tabel 4.6 Nilai Ancaman Wifi	46
Tabel 4.7 Nilai Ancaman Air Conditioner	47
Tabel 4.8 Nilai Ancaman Server Physical	47
Tabel 4. 9 Nilai Ancaman Proyektor	48
Tabel 4. 10 Nilai Ancaman Kabel HDMI	49
Tabel 4. 11 Kabel VGA	49
Tabel 4. 12 Nilai Ancaman APAR.....	50
Tabel 4. 13 Nilai Ancaman Meja.....	50
Tabel 4. 14 Nilai Ancaman Kursi.....	50
Tabel 4. 15 Nilai Ancaman Keyboard	51
Tabel 4. 16 Nilai Ancaman Mouse	51
Tabel 4. 17 Nilai Ancaman Headphone	52
Tabel 4. 18 Nilai Ancaman Papan Tulis Kaca.....	52
Tabel 4. 19 Nilai Ancaman Stabillizer Electrical	52
Tabel 4. 20 Nilai Ancaman Windows 10	53

Tabel 4. 21 Nilai Ancaman Microsoft Office 2019	53
Tabel 4. 22 Nilai Ancaman Microsoft SQL	54
Tabel 4. 23 Nilai Ancaman Antivirus	54
Tabel 4. 24 Nilai Ancaman Oracle Database	55
Tabel 4.25 Kategori Nilai Ancaman Pada Aset.....	55
Tabel 4. 26 Tabel <i>Business Impact Analysis (BIA)</i>	57
Tabel 4. 27 Tabel <i>Nilai Level Risiko</i>	59
Tabel 4. 28 Perbedaan <i>Threat Actor dan Attack</i>	65
Tabel 4. 29 Matriks Kebijakan IT Risk Control Terhadap Annex ISO 27001:2022	71

DAFTAR GAMBAR

Gambar 2. 1 CIA Triad	7
Gambar 2. 2 <i>Hilangnya Kerahasiaan Data</i> (Rao 2014).....	8
Gambar 2. 3 Hilangnya Keutuhan Data (Rao 2014)	8
Gambar 2. 4 Hilangnya Ketersediaan Data (Rao 2014)	8
Gambar 2. 5 Lapisan Utama Keamanan Informasi	9
Gambar 2. 6 Cara mengelola risiko (Prima Gandhi SP, MSi 2019).....	11
Gambar 2.7 Analogi Tentang Aset (Ratih Kusumastuti1, I Ketut Kusuma Wijaya, Sarni Handayani Puspita Sari, Fitriani 2023)	22
Gambar 2. 8 Metode PDCA dalam Sistem Manajemen Keamanan Informasi....	26
Gambar 3.1 Kerangka Berfikir.....	29
Gambar 4.1 Struktur Pengurus Laboratorium Komputer FIK UPNVJ	39

DAFTAR LAMPIRAN

Lampiran 1. Hasil Turnitin Tugas Akhir	78
Lampiran 2. Surat Permohonan Riset Mahasiswa	81
Lampiran 3. Tabel Identifikasi Aset LAB FIK UPNVJ	84
Lampiran 4. Observasi seluruh ruangan LAB KOMPUTER FIK UPNVJ	90
Lampiran 5. Annex/Norma ISO 27001:2022	96
Lampiran 6. Dokumen Kebijakan Kontrol Risiko Teknologi Informasi Pada Organisasi.....	106
Lampiran 7. Dokumen Kebijakan Kontrol Risiko Teknologi Informasi Pada Pengendalian Individu.....	109
Lampiran 8. Dokumen Kebijakan Kontrol Risiko Teknologi Informasi Pada Fisik atau Hardware.....	112
Lampiran 9. Dokumen Kebijakan Kontrol Risiko Teknologi Informasi Pada Teknologi.....	116
Lampiran 10. Prosedur Membuat Dokumen Kebijakan Kontrol Risiko Tentang Organisasi	120
Lampiran 11. Prosedur Membuat Dokumen Kebijakan Kontrol Risiko Tentang Pengendalian Individu.....	121
Lampiran 12. Prosedur Membuat Dokumen Kebijakan Kontrol Risiko Tentang Kontrol Fisik.....	122
Lampiran 13. Prosedur Membuat Dokumen Kebijakan Kontrol Risiko Tentang Kontrol Teknologi.....	123
Lampiran 14. Surat Tata Tertib Laboratorium Komputer FIK UPNVJ	124
Lampiran 15. Tabel Ulasan Kelebihan dan Kekurangan Seluruh Ruangan LAB Komputer FIK UPNVJ.....	125
Lampiran 16. Rekomendasi Perbaikan Aset.....	127
Lampiran 17. Tampilan Dashboard Website Pencacatan BMN.....	131
Lampiran 18. Hasil Metode PDCA.....	134
Lampiran 19. Daftar Riwayat Hidup.....	137

DAFTAR RUMUS

(2.1).....	14
(2.2).....	18
(2.3).....	21