LAPORAN AKHIR PENELITIAN

UNIVERSITAS ESA UNGGUL

MANAJEMEN RISIKO PADA PENGGUNAAN APLIKASI SISTEM INFORMASI DI DINAS KOMINFO STATISTIK DAN PERSANDIAN KAB. XYZ MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDART AND TECHNOLOGY (NIST SP 800-30)

Oleh

BUDI TJAHJONO

MIRI ARDIANSYAH

GERRY FIRMANSYAH

HABIBULLAH AKBAR

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS ESA UNGGUL
TAHUN 2023

IDENTITAS DAN URAIAN UMUM PENELITIAN DOSEN

1. Judul Penelitian :
   "MANAJEMEN RISIKO PADA PENGGUNAAN APLIKASI SISTEM INFORMASI DI DINAS KOMINFO STATISTIK DAN PERSANDIAN KAB. XYZ MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDART ANDTECHNOLOGY (NIST SP 800-30)
"

2. Tim Peneliti

No.	Nama	Jabaan	Bidang	Instansi asal	Alokasi Waktu (jam/minggu)	Keahlian
1.	Budi Tjahjono	Ketua	Informatika	Prodi MKom	6	Manajemen ResikoMana
2.	Gerry Firmansyah	Anggota 1	Informatika	Prodi MKom	6	SPBE
3.	Habibullah Akbar	Anggota 2	Informatika	Prodi Mkom	5	AI

.

3. Objek Penelitian (jenis material yang akan diteliti dan segi penelitian): Manajemen Resiko diidentifikasi dari sisi manusia dan sisi listrik

4. Masa Pelaksanaan
   Mulai : bulan Februari tahun: 2023
   Berakhir : bulan: Juli tahun: 2023

5. Usulan Biaya Internal
   Tahun ke-1 : Rp 30.000.000,00
   Tahun ke-2 : Rp
   Tahun ke-3 : Rp

6. Lokasi Penelitian (lab/studio/lapangan). Diskominfo Kab. XYZ, Bengkulu

7. Instansi lain yang terlibat (jika ada, dan uraikan apa kontribusinya)

8. Temuan yang ditargetkan (penjelasan gejala atau kaidah, metode, teori, produk, atau rekayasa)
a. Mengidentifikasi ancaman resiko dari sisi manusia dan sisi listrik
b. Hasil perbandingan antara metode NIST 800-30 dan Permenpan RB no. 5 tahun 2020.

9. Kontribusi mendasar pada suatu bidang ilmu (uraikan tidak lebih dari 50 kata, tekankan pada gagasan fundamental dan orisinal yang akan mendukung pengembangan iptek)
   Penerapan E-government atau Sistem Berbasis Pemerintahan (SPBE) ada risiko yang harus diperhatikan misalnya kehilangan data, pencurian data, kerusakan hardware, peretasan, yang akan menimbulkan dampak negatif bagi organisasi pemerintahan. Perpres No.95 Tahun 2018 mengamanatkan agar SPBE dapat meminimalkan risiko untuk menjaga agar

pelayanan publik tetap maksimal. Fokus penelitian ini adalah melakukan proses manajemen risiko menggunakan framework NIST SP 800-30

10. Jurnal ilmiah yang menjadi sasaran (tuliskan nama terbitan berkala ilmiah internasional bereputasi, nasional terakreditasi, atau nasional tidak terakreditasi dan tahun rencana publikasi)
    Jurnal Ilmu Pengetahuan dan Teknologi Komputer, jurnal nasional terakreditasi Sinta 2 (Telah publikasi pada JITK Vol 9 No. 1, Agustus 2023) P-ISSN:2685-8223 E-ISSN 2527-4864 DOI: 10.33480 /jitk.v9i1.4080

11. Rencana luaran HKI, buku, purwarupa atau luaran lainnya yang ditargetkan, tahun rencana perolehan atau penyelesaiannya

Lembar Pengesahan Laporan Akhir

Program Penelitian
Universitas Esa Unggul

1. Judul Kegiatan Penelitian : MANAJEMEN RISIKO PADA PENGGUNAAN APLIKASI SISTEM INFORMASI DI DINAS KOMINFO STATISTIK DAN PERSANDIAN KAB. XYZ MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDART ANDTECHNOLOGY (NIST SP 800-30)
2. Nama Mitra Sasaran : Diskominfor Statistik dan Persandian
3. Ketua Tim
   a. Nama Lengkap : Dr. BUDI TJAHJONO, S.Kom, M.Kom
   b. NIDN 0330126703
   c. Jabatan Fungsional : Lektor Kepala (700)
   d. Fakultas/ Program Studi : Fakultas Ilmu Komputer/ Fasilkom/Program Studi Magister Ilmu Komputer
   e. Bidang Keahlian :
   f. Nomor Telepon/ HP 08983444426
   g. Email : budi.tjahjono@esaunggul.ac.id
4. Jumlah Anggota Dosen : 2 orang
5. Jumlah Anggota Mahasiswa : 1 orang
6. Lokasi Kegiatan Mitra
   Alamat Kab. XYZ, Propinsi Bengkulu
   Kabupaten/ Kota KAUR
   Provinsi BENGKULU
7. Periode/ Waktu Kegiatan : 2 Februari 2023 s/d 27 Juli 2023
8. Luaran yang Dihasilkan : Jurnal Nasional terakreditasi Sinta 2
9. Usulan/ Realisasi Anggaran
   a. Dana Mandiri : 30.000.000
   b. Sumber Dana Lain (1) : 30.000.000

Jakarta, 29 September 2024
Ketua Peneliti,

(Dr. BUDI TJAHJONO, S.Kom, M.Kom)
NIDN/K. 0330126703

Menyetujui,
Dekan Fakultas Ilmu Komputer

(Dr. VITRI TUNDJUNGSARI, ST., M.Sc., M.M)

NIP/NIK. 222010872

Mengetahui,
Ketua Lembaga Penelitian dan Pengabdian Masyarakat Universitas Esa Unggul

(LARAS SITOAYU, S.Gz, M.K.M)

NIK. 215080596

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

E-Government pada praktiknya memang membuat pelayanan pemerintah terhadap masyarakat menjadi mudah. Namun dibalik kemudahan dirasakan tentunya akan ada risiko yang muncul misalnya kehilangan data, pencurian data, salah akses, akses illegal, kerusakan hardware, peretasan, dll yang sebaliknya akan menimbulkan dampak negatif bagi suatu organisasi.

Dinas Kominfo Statistik dan Persandian Kab. XYZ adalah sebuah instansi atau organisasi pemerintahan dibidang Komunikasi dan Informatika yang ada di Kab, XYZ yang mengawasi aplikasi yang ada pada Organisasi Perangkat Daerah (OPD) Kab. XYZ dalam menjalankan dan memaksimalkan pelayanan pemerintahannya. Namun permasalahan yang muncul adalah bahwa terdapat beberapa jenis ancaman yang ada pada penerapan aplikasi di Kab. XYZ. Ancaman yang paling sering ditemukan adalah ancaman yang bersumber dari manusia dan listrik. Ancaman dari manusia dalam hal ini adalah Sumber Daya Manusia (SDM) yang kurang memadai sehingga menimbulkan beberapa risiko seperti masalah login, kesalahan akses menu, data terhapus secara tidak sengaja, ceroboh, dll.

Sementara sumber ancaman dari listrik dikarenakan tidak stabilnya infrastruktur listrik akan menimbulkan risiko kerusakan *hardware*, *hardware* terbakar, kehilangan data, data korup, sinyal internet mati sehingga hal ini jelas akan mengganggu pelayanan pemerintahan berbasis elektronik di Kab. XYZ yang tentuny jika diabaikan akan berpotensi menyebabkan dampak negatif dan dapat menurunkan reputasi hingga menimbulkan kerugian finansial.

Berdasarkan Perpres No.95 Tahun 2018 yang mengatakan semua Sistem Berbasis Pemerintahan (SPBE) diharapkan untuk meminimalkan risiko untuk menjaga agar pelayanan publik tetap maksimal. Dengan demikian jelas bahwa hendaknya setiap penyelenggara

pemerintahan dapat membuat sebuah manajemen risiko. Manajemen risiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidak pastian yang berkaitan dengan ancaman suatu rangkaian aktivitas manusia termasuk: Penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan/pengelolaan sumber daya (Saepul et al., 2017).

Ada banyak metode yang dapat digunakan untuk melakukan manajemen risiko keamanan informasi seperti Octave, NIST SP 800-30 dan ISO 27001 (Elanda & Buana, 2021). Namun pada penelitian ini metode yang akan dipakai dalam melakukan manajemen risiko adalah NIST SP 800-30 (*National Institute Of Standarts and Technology SP 800-30*). Alasan memilih NIST SP 800-30 adalah berdasarkan penelitian terdahulu yaitu penelitian yang dilakukan oleh (Syafitri, 2016) dan penelitian yang dilakukan oleh (Elanda & Buana, 2021) bahwa NIST SP 800-30 telah terbukti memberikan kontribusi yang lebih seperti: memberikan wawasan keamanan informasi yang sifatnya konsisten dan komprehensif bagi pengambil kebijakan, pemodelan sumber daya yang terstruktur, wawasan keamanan informasi dapat diterima oleh berbagai pengambil resiko, penentuan ancaman dapat diidentifikasi dengan mudah, pengambil keputusan tidak ragu-ragu untuk mengambil resiko karena setiap resiko telah diselidiki dengan baik (Ekelhart et al., 2009). NIST SP 800-30 terbaik dari 3 metode untuk analisa resiko yaitu *Mehari*, *Magerit* dan *Microsoft's Security Management Guide* terutama pada saat melakukan analisa resiko, NIST SP 800-30 memberikan rekomendasi kontrol (Syalim et al., 2010).

Atas dasar latar belakang inilah peneliti bermaksud untuk melakukan penelitian yang berjudul "Manajemen Risiko Pada Penggunaan Aplikasi Sistem Informasi Di Dinas kominfo statistik dan persandian kab. XYZ menggunakan *Framework National Institute Of Standart And Technology* (NIST SP 800-30)" sebagai tugas akhir yang dibuat untuk menyelesaikan studi S2 Ilmu Komputer di Universitas Esa Unggul.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat ditarik rumusan masalah pada penelitian ini adalah sebagai berikut :

1. Bagaimana melakukan pengukuran risiko pada penggunaan aplikasi di Dinas

Kominfo Statistik dan Persandian Kab. XYZ menggunakan *framework NIST 800-30* ?

2. Bagaimana hasil identifikasi ancaman dan kerentanan pada penggunaan aplikasi di Dinas Kominfo Statistik dan Persandian Kab. XYZ ?
3. Bagaimana mengatasi ancaman risiko dan kerentanan yang ada pada proses penggunaa aplikasi di Dinas Kominfo Statistik dan Persandian Kab. XYZ ?

1.3. Batasan Penelitian

Agar cakupan penelitian tidak terlalu luas, maka peneliti menetapkan Batasan penelitian sebagai berikut :

1. Penelitian ini terbatas pada manajemen dan pegukuran risiko terhadap kelancaran jalannya penggunaan aplikasi secara umum di Diskominfo Kab. XYZ dan tidak detail pada tiap-tiap aplikasi yang digunakan.
2. Pembuatan dan pengukuran manajemen risiko menggunakan *framework National Institute Of Standarts And Technology* (NIST SP 800-30).

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

1. Melakukan penilaian risiko serta rekomendasi pengendalian pada asset aplikasi yang digunakan sesuai dengan *framework National Institute Of Standarts And Technology* (NIST SP 800-30).
2. Membuat dokumentasi terkait dengan hasil pengukuran yang dilakukan.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dan dapat diambil dengan adanya penelitian ini adalah :

1. Dinas Kominfo Statistik dan Persandian Kab. XYZ dapat memahami dengan baik terkait dengan kondisi serta karakteristik pada asset yang berkaitan dengan aplikasi serta menyadari risiko-risiko yang ada pada setiap aplikasi.
2. Dinas Kominfo Statistik dan Persandian Kab. XYZ dapat mengambil langkah yang cepat, tepat dan terukur dalam merespon risiko-risiko yang ada berdasarkan pengukuran dan rekomendasi yang dihasilkan.

BAB II.
RENSTRA DAN PETA JALAN PENELITIAN PERGURUAN TINGGI

2.1. Latar Belakang

Pembangunan sumberdaya manusia berkualitas dan berdaya saing merupakan salah satu isu prioritas dalam Rencana Pembangunan Jangka Menengah Nasional IV 2020-2024 yang digulirkan Pemerintah. Kemenristek DIKTI telah mengeluarkan suatu Rencana Induk Riset Nasional (RIRN) 2015-2045 yang bertujuan untuk: (1) Meningkatkan kapasitas dan kompetensi riset Indonesia di ranah global; (2) Meningkatkan literasi IPTEK masyarakat; dan (3) Meningkatkan ekonomi berbasis IPTEK. Perguruan tinggi berperan penting dalam peningkatan penguasaan dan pemanfaatan ilmu pengetahuan dan teknologi (IPTEK) melalui penelitian, pengembangan, dan penerapan menuju inovasi yang berkelanjutan. Universitas Esa Unggul yang memiliki visi "Menjadi perguruan tinggi kelas dunia berbasis intelektualitas, kreatifitas dan kewirausahaan, yang unggul dalam mutu pengelolaan dan hasil pelaksanaan Tridarma Perguruan Tinggi pada Tahun 2033". Visi Esa Unggul perlu untuk mengembangkan Rencana Induk Penelitian (RIP) yang sejalan dengan RIRN dan Renstra Universitas dalam jangka waktu lima tahun ke depan (2024-2028), sebagai kelanjutan dari RIP terdahulu (2019-2023). RIP ini menjadi pedoman dan kebijakan UEU dalam mengarahkan penelitian dan inovasi dosen agar efisiensi dan efektivitas riset dapat terwujud dan menghasilkan luaran sesuai kebutuhan masyarakat dan negara.

2.**2 Tujuan Penyusunan Rencana Induk Penelitian**

Sebagai acuan penelitian dalam rangka meningkatkan sistem penjaminan mutu penelitian.
1. Mengembangkan payung penelitian unggulan di Universitas Esa Unggul baik nasional maupun internasional. 2. 3.Meningkatkan jumlah dan kualitas publikasi dosen baik nasional maupun internasional. 4.Menciptakan kolaborasi riset dengan mitra kerjasama berdaya saing global. 5.Membangun budaya kolaborasi penelitian antara dosen dan mahasiswa.

2.3. RENCANA INDUK PENELITIAN

Peta jalan penelitian UEU telah ditetapkan dengan mengacu pada tahapan dalam Renstra

Universitas 2012-2037. Berdasarkan tahapan dalam Kebijakan UEU maka peta jalan penelitian dibagi menjadi lima tahapan yaitu Tahap Peningkatan (2014-2018), Tahap Pemantapan (2019-2023), Tahap Pendalaman (2024-2028), Tahap Pematangan (2029-2033), sebagaimana tertera pada Gambar 1. 9 BAB III RENCANA INDUK PENELITIAN 3.1 Peta Jalan Penelitian

Gambar 2. Peta Jalan Penelitian

Arah pengembangan UEU tertuang secara rinci dalam Rencana Strategis 2024-2028 dan secara dinamis selalu disinkronkan dengan Renstra Universitas Esa Unggul 2005-2025. Visi UEU adalah “Menjadi perguruan tinggi kelas dunia berbasis intelektualitas, kreatifitas dan kewirausahaan, yang unggul dalam mutu pengelolaan dan hasil pelaksanaan Tridarma Perguruan Tinggi pada tahun 2033”, dan dalam tahapan milestone UEU, periode 2019-2023 telah memasuki Fase V yaitu pencapaian world class university, sebelum memasuki tahapan menjadi world class university di tahun 2030. Sebagai universitas yang akan menjadi world class university, UEU harus memberikan prioritas tinggi untuk pengembangan programprogram penelitian.

Berikut penjelasan masing-masing tahap:

Tema Unggulan Penelitian

Tema Unggulan Penelitian

Tahap	Periode	Penjelasan
Peningkatan	2014-2018	Universitas mempersiapkan sumberdaya riset, sistem manajemen penelitian, penguasaan budaya riset, dan jumlah penelitian.
Pemantapan	2019-2023	Universitas memperkuat sistem manajemen penelitian, mendorong luaran penelitian, dan penguatan budaya riset dosen.
Pendalaman	2024-2028	Pengembangan penelitian terapan, peningkatan kualitas publikasi internasional, peningkatan joint research internasional, dan peningkatan kolaborasi penelitian kerjasama.
Pematangan	2029-2033	Pemantapan dan penguatan joint research internasional, menuju penelitian excellent yang berdaya saing global.

2.4 Tema Unggulan

Kesehatan dan

Kesehatan dan Kesejahteraan

Kesejahteraan psikologi, kesehatan mental, dan kualitashidup.

1. *Complementary therapy Nursing home care* danpenerapan telemedicine
2. Analisis pengembangan obat, kosmetik, fitofarmaka, dan nutraseutikal dari bahan alam..
3. Penggunaan sel induk untuk pengobatan regeneratif, serta terapi gen untuk mengobati penyakit genetic
4. Pemanfaatan organisme untuk menghasilkanobat/antibiotik dan vaksin
5. Pemanfaatan *antibody monoclonal* untuk mengobati penyakit
6. Keberlanjutusiaan, kesehatan ibu, anak, dan remaja
7. Promotif, preventif, kuratif, serta rehabilitatif penyakit menular dan tidak

menular

8. Aplikasi big data, bioinformatika dan kecerdasanbuatan.
9. Manajemen Sumber Daya Manusia, Kesejahteraan Karyawan, dan perilaku konsumen
10. Pengembangan model pembiayaan jaminan kesehatannasional
11. Analisis kelayakan, pengungkapan dan pelaporankeberlanjutan pada industri

Teknologi Energi Baru

Energi Teknologi Baru danTerbarukan

enologi Energi Baru

Teknologi Energi Baru

1. Teknologi Informasi dan Komunikasi untuk mendukung Industri 4.0
2. Pemanfaatan sumberdaya alam dan pengelolaan limbah
3. Kebijakan penggunaan Teknologi baterai
4. *Sustainable Cities & Smart City*
5. Pengelolaan, pemetaan wilayah, dan manajemen proyek
6. Rantai pasokan dan logistik
7. Pengelolaan dan pengembangan keterampilan SDM dalam industri energi terbarukan
8. Pengembangan model bisnis dan penerapan akuntansikarbon
9. Perpajakan dan analisis kelayakan yang mendukungpengembangan energi terbarukan
10. Dampak energi terbarukan terhadap ketahanan dan kedaulatan energi nasional
11. *Software Science, Infromation Science, Programming,* IT, *Infrastructure and Platform,* dan *Enterprise System*
12. Sosial Humaniora dan

Sosial Humaniora dan Industri Kreatif

1. Hukum ketenagakerjaan, Kebijakan dan perundang- undangan.
2. Artificial inteligient dari sisi regulasi
3. Perlindungan data privacy pribadi di era digital.
4. Tata negara dan sistem demokrasi
5. Pertanahan dan reforma agrarian
6. Produk furniture desain, desain Interior, fotografi produk, media promosi produk, dan animasi
7. Sustainable design, material daur ulang, desain environmental, dan transportasi publik yang berbasiskearifan lokal.
8. Technical Vocational Education, multimodality andLanguage Learning
9. Kompetensi Cyber Pedagogy dalam menghadapipembelajaran 4.0
10. Seni dan sastra sebagai komunikasi non verbal sertapenerapkan kearifan lokal.
11. Teacher Professional Development and tranformasi kurikulum dalam pendidikan
12. STEM and Integration of Technology in education
13. Strategi pemasaran yang efektif untuk produk atau layanan di sektor industri kreatif
14. Kreativitas dan inovasi dalam tim industri kreatif.
15. Creative work behavior, design thinking, and learningorganization
16. Penerapan akuntansi, pengembangan model bisnis, dan self leadership pada usaha kecil dan menengah (UMKM)
17. Akuntansi hijau, sektor publik, kinerja keuangan bisnis, audit sektor bisnis,dan akuntabilitas publik
18. Digitalisasi akuntansi keuangan dan pelayanan publik
19. Analisis kinerja keuangan bisnis, kebijakan pengendalian I flasi, dan perilaku pasar modal.
20. Ketimpangan Gender dan Kerentanan Pekerja Perempuan dalam Perspektif Psikologi Sosial

21. Penggunaan media dalam pembentukan brand image
22. Komunikasi dan Media Baru, Budaya Digital, Komunikasi Antarbudaya, dan komunikasi organisasi
23. Semiotika Komunikasi, manejemen penyiaran, dan Digital Marketing Communication

Kebijakan dan
Kebijakan dan Pengembangan Ppendidikan

1. Penerapan kebijakan Kesehatan
2. Layout Ruang Pengembangan Pendidikan
3. Sustainable improvement on the pre service teachercompetecy
4. Implementasi International Financial Reporting Standards (IFRS)

2.5 Strategi Penelitian

Strategi Penelitian

Untuk mencapai tujuan dan sasaran penelitian yang telah dirumuskan, perlu dirancang langkah- langkah strategi penelitian dengan filosofi memaksimalkan kekuatan dan memanfaatkan peluang yang ada serta perbaikan kelemahan dan meminimalkan pengaruh ancaman.

Strategi yang perlu dikembangkan untuk mencapai arah kebijakan pengembangan bidang penelitian adalah sebagai berikut.

Strategi Penelitian

Standar	Indikator	Strategi
Standar isi penelitian	1. Tersedianya Rencana Induk Penelitian (RIP). 2. Relevansi penelitian dosen dengan tema – tema unggulan yang tertuang pada RIP.	1. Melakukan penyusunan, pengembangan, dan pemutakhiran Rencana Induk Penelitian secara berkala 2. Melakukan sosialisasi rencana induk penelitian dan standar isi penelitian ke seluruh dosen berkoordinasi dengan fakultasdan prodi. 3. Melakukan sosialisasi dokumen Pedoman Penelitian sebagai acuan seluruh dosen dalam melaksanakan kegiatan penelitian. 4. Memfasilitasi proses review dan seleksi proposal penelitian setiap tahun melalui tenaga reviewer internal yang telah ditetapkan. 5. Mengarahkan luaran kegiatan penelitian dalam bentuk publikasi, buku, prosiding, HAKI/Paten.
Standar proses penelitian	1. Tersedianya panduan penelitian. 2. Adanya perencanaan kegiatan penelitian dosen. 3. Adanya proses penjaminan mutu penelitian dosen mencakup: pengajuan, diseminasi dan monev dan laporan.	1. Menetapkan kebijakan proses pengelolaan penelitian mulai dari proses pengumpulan proposal, laporan Akhir dan laporan akhir. 2. Berkoordinasi dengan fakultas dan prodi melakukan sosialisasasi standar proses penelitian ke seluruh dosen dan mahasiswa. 3. Melakukan pendampingan dalam meningkatkan kompetensi dosen terkait metodologi penelitian melalui kegiatan workshop/pelatihan/diseminasi 4. Melaksanakan kegiatan penelitian berpedoman pada prosedur proses penelitian. 5. Berkoordinasi dengan Kapusdi dalam melakukan monitoring dan evaluasi terhadap proses penelitian yang dilakukan oleh seluruh dosen
Standar penilaian penelitian	1. Tersedianya kebijakan, pedoman dan prosedur tentang penilaian penelitian dosen. 2. Tersedianya instrumen penilaian peneliltian dosen. 3. Adanya tim reviewer internal.	1. Melakukan koordinasi dengan Fakultas, Prodi, Kapusdi dalam melakukan sosialisasi ke seluruh dosen dan mahasiswa terkait dengan standar penilaian penelitian. 2. Memfasilitasi reviewer internal dalam melakukan review dan penilaian penelitian yang mengacu pada pedoman yang telah ditetapkan. 3. Memfasilitasi reviewer dalam melakukan penilaian menggunakan instrumen yang telah ditetapkan berdasarkan prinsip edukatif, obyektif, akuntabel, dan transparan dalam melakukan proses penilaian. 4. Menetapkan mekanisme review proposal penelitian, mekanisme monitoring dan evaluasi pelaksanaan penelitian, serta mekanisme pengumpulan laporan hasil penelitian.

Standar	Indikator	Strategi
Standar peneliti	1. Adanya persyaratan minimum sebagai peneliti. 2. Tersedianya kelompok penelitian/kluster penelitian bidang ilmu.	1. Melakukan sosialisasi standar peneliti ke seluruh dosen 2. Melakukan pembentukan kelompok peneliti/kluster penelitian bidang ilmu sesuai dengan Tema Unggulan Universitas 3. Mengadakan kegiatan pelatihan dalam bentuk workshop maupun Bimtek dalam meningkatkan kompetensi dosen terkait dengan metodologi penelitian, luaran kegiatan penelitian, maupun peningkatan proposal hibah. 4. Menyelenggarakan kegiatan pelatihan bagi dosen dalam penulisan dan publikasi karya ilmiah dalam jurnal internasional bereputasi.
Standar pengelolaan penelitian	1. Adanya Lembaga Pusat Penelitian dan PkM yang terpusat di tingkat universitas. 2. Tersedianya RIP. 3. Monitoring dan evaluasi kegiatan penelitian secara berkala. 4. Tersedianya sistem informasi penunjang kegiatan penelitian.	1. KPM dan LPPM mengadakan sosialisasi terhadap standar, peraturan, panduan, program, dan sistem penjaminan mutu internal dalam kegiatan penelitian. 2. Mewajibkan Dosen melaksanakan kegiatan penelitian yang mengacu pada roadmap penelitian yang telah ditetapkan. 3. Melakukan kerjasama dengan mitra dalam rangka meningkatkan pelaksanaan kegiatan penelitian. 4. Memfasilitasi Dosen dalam melakukan diseminasi kegiatan penelitian melalui seminar/conference 5. Menetapkan sistem penghargaan bagi dosen yang menghasilkan luaran penelitian 6. Memberikan penghargaan berupa insentif kepada semua dosen yang menghasilkan luaran penelitian sesuai dengan aturan yang berlaku
Standar Reviewer Internal Penelitian	1. Tersedianya kebijakan tentang syarat minimum reviewer internal. 2. Pelatihan dan sertifikasi reviewer internal. 3. Laporan hasil moniitoring dan evaluasi.	1. Rektor mengesahkan dan menetapkan standar reviewer internal penelitian yang telah disetujui oleh Senat Universitas. 2. Wakil Rektor Bidang Riset, Pengembangan dan Inovasi, menginstruksikan Biro LPPM, untuk mensosialisasikan standar reviewer internal penelitian. 3. Biro LPPM membentuk tim reviewer internal penelitian sesuai dengan kriteria yang ditetapkan. 4. Biro LPPM menugaskan Tim reviewer internal untuk memonitoring serta mengevaluasi seluruh pelaksanaan kegiatan penelitian yang dilakukan para dosen.

Standar Kolaborasi Penelitian Dosen dan Mahasiswa	1. Tersedianya kebijakan dan pedoman kolaborasi penelitian dosen dan mahasiswa. 2. Penelitian payung dosen dan mahasiswa. 3. Keikutsertaan mahasiswa dalam conference.	1. Mensosialisasikan kebijakan dan panduan kolaborasi penelitian dosen dan mahasiswa secara berkala. 2. Wakil Rektor Bidang Riset, Pengembangan dan Inovasi menetapkan target jumlah minimal luaran penelitian yang dilakukan dosen bersama dengan mahasiswa yaitu satu kegiatan dalam satu tahun. 3. Fakultas dan prodi menetapkan kebijakan kegiatan penelitian payung dosen dan mahasiswa untuk kriteria tugas akhir.
Standar	Indikator	Strategi
Standar peneliti	3. Adanya persyaratan minimum sebagai peneliti. 4. Tersedianya kelompok penelitian/kluster penelitian bidang ilmu.	5. Melakukan sosialisasi standar peneliti ke seluruh dosen 6. Melakukan pembentukan kelompok peneliti/kluster penelitian bidang ilmu sesuai dengan Tema Unggulan Universitas 7. Mengadakan kegiatan pelatihan dalam bentuk workshop maupun Bimtek dalam meningkatkan kompetensi dosen terkait dengan metodologi penelitian, luaran kegiatan penelitian, maupun peningkatan proposal hibah. 8. Menyelenggarakan kegiatan pelatihan bagi dosen dalam penulisan dan publikasi karya ilmiah dalam jurnal internasional bereputasi.
Standar pengelolaan penelitian	5. Adanya Lembaga Pusat Penelitian dan PkM yang terpusat di tingkat universitas. 6. Tersedianya RIP. 7. Monitoring dan evaluasi kegiatan penelitian secara berkala. 8. Tersedianya sistem informasi penunjang kegiatan penelitian.	7. KPM dan LPPM mengadakan sosialisasi terhadap standar, peraturan, panduan, program, dan sistem penjaminan mutu internal dalam kegiatan penelitian. 8. Mewajibkan Dosen melaksanakan kegiatan penelitian yang mengacu pada roadmap penelitian yang telah ditetapkan. 9. Melakukan kerjasama dengan mitra dalam rangka meningkatkan pelaksanaan kegiatan penelitian. 10. Memfasilitasi Dosen dalam melakukan diseminasi kegiatan penelitian melalui seminar/conference 11. Menetapkan sistem penghargaan bagi dosen yang menghasilkan luaran penelitian 12. Memberikan penghargaan berupa insentif kepada semua dosen yang menghasilkan luaran penelitian sesuai dengan aturan yang berlaku

Standar Reviewer Internal Penelitian	4. Tersedianya kebijakan tentang syarat minimum reviewer internal. 5. Pelatihan dan sertifikasi reviewer internal. 6. Laporan hasil moniitoring dan evaluasi.	5. Rektor mengesahkan dan menetapkan standar reviewer internal penelitian yang telah disetujui oleh Senat Universitas. 6. Wakil Rektor Bidang Riset, Pengembangan dan Inovasi, menginstruksikan Biro LPPM, untuk mensosialisasikan standar reviewer internal penelitian. 7. Biro LPPM membentuk tim reviewer internal penelitian sesuai dengan kriteria yang ditetapkan. 8. Biro LPPM menugaskan Tim reviewer internal untuk memonitoring serta mengevaluasi seluruh pelaksanaan kegiatan penelitian yang dilakukan para dosen.
Standar Kolaborasi Penelitian Dosen dan Mahasiswa	4. Tersedianya kebijakan dan pedoman kolaborasi penelitian dosen dan mahasiswa. 5. Penelitian payung dosen dan mahasiswa. 6. Keikutsertaan mahasiswa dalam conference.	4. Mensosialisasikan kebijakan dan panduan kolaborasi penelitian dosen dan mahasiswa secara berkala. 5. Wakil Rektor Bidang Riset, Pengembangan dan Inovasi menetapkan target jumlah minimal luaran penelitian yang dilakukan dosen bersama dengan mahasiswa yaitu satu kegiatan dalam satu tahun. 6. Fakultas dan prodi menetapkan kebijakan kegiatan penelitian payung dosen dan mahasiswa untuk kriteria tugas akhir.

BAB III

TINJAUAN PUSTAKA DAN LANDASAN TEORI

3.1. Manajemen Risiko

3.1.1. Pengertian Manajemen Risiko

Risiko adalah variasi dalam hal-hal yang mungkin terjadi secara alami atau kemungkinan terjadinya peristiwa diluar yang diharapkan yang merupakan ancaman terhadap properti dan keuntungan finansial akibat bahaya yang terjadi. Menurut Besis, risiko ada hanya ketika ketidakpastian dapat memiliki efek samping potensial, yang merupakan kemungkinan kerugian. Risiko dapat ditafsirkan sebagai bentuk keadaan ketidakpastian tentang suatu keadaan yang akan terjadi nantinya dengan keputusan yang diambil berdasarkan berbagai pertimbangan pada saat ini (Ramadhani & Baharudin, 2019).

3.1.2. Tujuan Manajemen Risiko

Manajemen risiko merupakan kegiatan manajemen yang dilakukan pada tingkat pimpinan pelaksana. Yaitu kegiatan penemuan dan analisis sistematis atas kerugian yang mungkin dihadapi oleh badan usaha, akibat suatu risiko serta metode yang paling tepat untuk menangani kerugian tersebut yang dihubungkan dengan tingkat profitabilitas badan usaha. Dengan demikian manajemen risiko mempunyai beberapa tujuan, yaitu (Harimurti, 2006) :

3.1.2.1. Tujuan sebelum terjadinya kerugian meliputi : efisiensi, meningkatkan kepercayaan, menanggulangi tanggung jawab pihak luar.

3.1.2.2. Tujuan setelah terjadinya kerugian, meliputi : kontinuitas operasi, tetap survive, stabilitas pendapatan dan pertumbuhan.

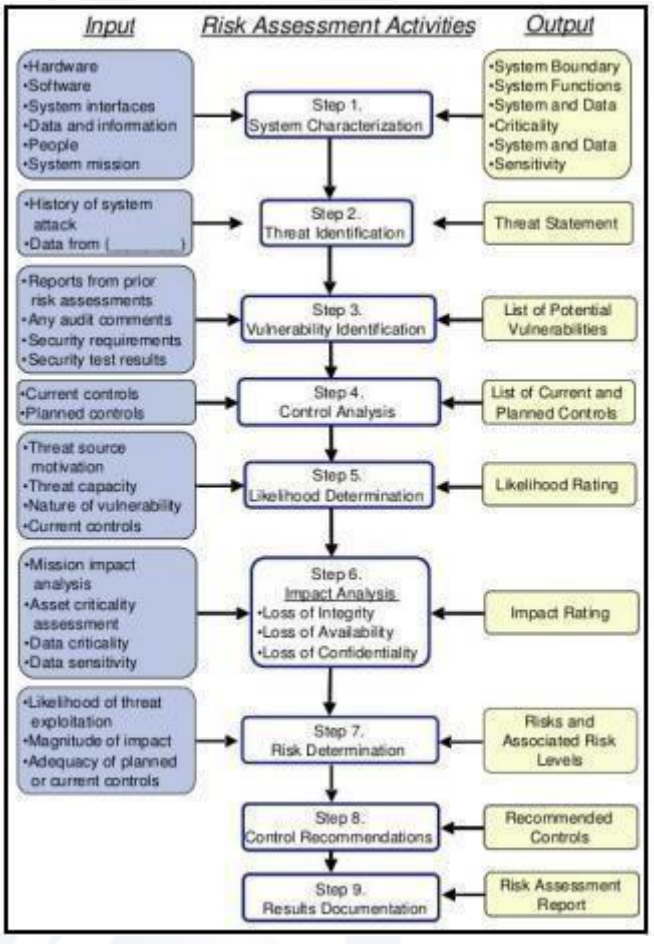
Jadi secara umum tujuan dari manajemen risiko adalah untuk menciptakan tingkat perlindungan yang meringankan kerentanan terhadap ancaman dan potensi

konsekuensi, sehingga mengurangi risiko ke tingkat yang dapat diterima (Muka & Wibowo, 2021).

3.1.3. *Framework* NIST SP 800-30

Framework National Institute of Standards and Technology (NIST) merupakan pengukuran risiko standar Internasional kumpulan standar atau langkah-langkah dan dapat memberikan pemahaman dalam proses manajemen risko, NIST mengeluarkan rekomendasi melalui publikasi khusus framework NIST SP 800-30 tentang *Risk Management Guide For Information Technology System*. NIST lebih menyajikan langkah- langkah untuk mengukur tingkat risiko yang ada (Harsanto & Hidayat, 2018).

Sedangkan tahapan proses penilaian risiko dalam *framework* NIST SP 800-30 adalah sebagai berikut (Saepul et al., 2017) :



Gambar 2. 1 Proses Manajemen Risiko NIST SP 800-30

Berikut penjelasannya :

A. *System Characterization*

Langkah pertama dalam menilai risiko adalah untuk menentukan ruang lingkup usaha. Untuk melakukan hal ini, mengidentifikasi di mana dibuat, diterima, dipelihara, diproses, atau ditransmisikan.

B. *Threat Identification*

Untuk langkah ini, potensi ancaman (potensi sumber ancaman untuk berhasil melaksanakan kerentanan tertentu) diidentifikasi dan didokumentasikan. Sumber ancaman adalah setiap keadaan atau peristiwa dengan potensi untuk menyebabkan kerusakan pada sistem IT (disengaja atau tidak disengaja).

C. *Vulnerability Identification*

Tujuan dari langkah ini adalah untuk mengembangkan daftar kerentanan sistem teknis dan non-teknis (kekurangan atau kelemahan) yang dapat dimanfaatkan atau dipicu oleh sumber-sumber ancaman - potensial.

D. *Control Analysis*

Tujuan dari langkah ini adalah untuk mendokumentasikan dan menilai efektivitas pengendalian teknis dan non-teknis yang telah atau akan dilaksanakan oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan (probabilitas) dari sumber ancaman–mengeksploitasi kerentanan sistem.

E. *Likelihood Determination*

Tujuan dari langkah ini adalah untuk menentukan nilai keseluruhan kemungkinan yang menunjukkan kemungkinan bahwa kerentanan dapat dimanfaatkan oleh sumber ancaman yang diberikan kontrol keamanan yang ada atau yang direncanakan

F. *Impact Analysis*

Tujuan dari langkah ini adalah untuk menentukan tingkat dampak negatif yang akan dihasilkan dari ancaman yang berhasil mengeksploitasi kerentanan.

G. *Risk Determination*

Menghitung level risiko dengan mengalikan peringkat dari penentuan

kemungkinan dan analisis dampak.

H. Control Recommendations

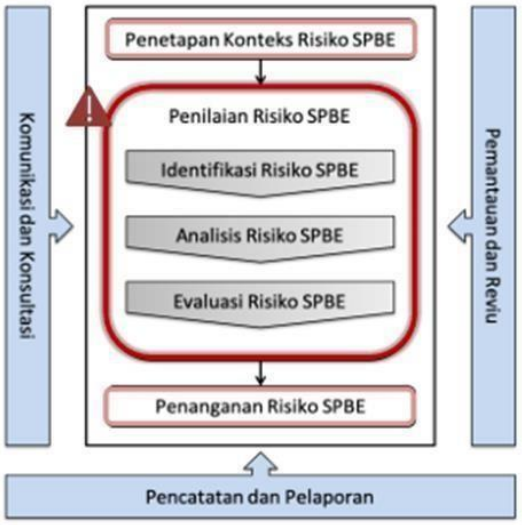
Tujuan dari langkah ini adalah untuk mengidentifikasi kontrol yang dapat mengurangi atau menghilangkan risiko yang teridentifikasi, sesuai dengan operasi organisasi.

I. Result Documentation

Penyusunan laporan keseluruhan proses penilaian risiko.

3.1.4. SPBE Permenpan RB No.5 Tahun 2020 (Standar Nasional)

Pengamatan dilakukan langsung pada bagian tahapan pengukuran risiko yang terdapat pada Permenpan RB No.5 Tahun 2020 dan membandingkannya dengan panduan pengukuran risiko pada NIST SP 800-30.



Gambar 2. 2 SPBE Permen PAN RB No.5 Tahun 2020 (Standar Nasional)

Pengukuran / penilaian risiko Permenpan RB No.5 Tahun 2020 memiliki 3 langkah sebagai berikut :

1. Identifikasi Risiko

   Pada tahapan ini terdapat informasi yang perlu dicantumkan seperti berikut ini :

   a. Jenis Risiko (Negatif dan Positif)

b. Kejadian
c. Penyebab
d. Kategori
e. Dampak
f. Area dampak.

Pada NIST SP 800-30 ini terdapat pada Step 2 (*Threat Identification*), Step 3 (*Vulnerability Identification*), Step 6 (*Impact Analysis*). Yang berbeda disini adalah NIST SP 800-30 tidak ada identifikasi terhadap jenis risiko Negatif, kategori risiko, dan area dampak risiko.

2. Analisis Risiko

Pada tahap analisis risiko informasi yang perlu dicantumkan adalah sebagai berikut :

a. Sistem pengendalian
b. Level kemungkinan
c. Level dampak
d. Besaran risiko SPBE dan level risiko SPBE.

Pada NIST SP 800-30 dimuat pada step 4 (*Control Analysis*), step 5 (*Likelihood Determination*), Step 6 (*Impact Analysis*) dan Step 7 (*Risk Determination*). Perbedaannya adalah pada sistem pengendalian sebagaimana disebutkan pada poin a, belum ada penekanan pada Analisa pengendalian sebagaimana yang pada NIST step 4 dimana input pada tahapan ini adalah *current control* dan *planned control* yang

menekankan bahwa control yang sudah dilakukan atau control yang akan dilakukan tidak menutup kemungkinan akan membuka celah yang baru.

3. Evaluasi Risiko

Pada tahap evaluasi risiko dilakukan pengambilan keputusan apakah perlu atau tidaknya dilakukan upaya penanganan dari risiko yang ada. Adanya tahapan ini disebabkan oleh beberapa hal seperti :

a. Menuntut penerapan skala prioritas terhadap penanganan risiko agar dapat memilih mana yang harus ditangani secara cepat dan mana yang tidak. Tentunya ini ditentukan oleh level risiko yang dihasilkan pengukuran risiko pada tahap sebelumnya.
b. Terdapat risiko positif dari setiap kejadian atau kerentanan sehingga harus melakukan jenis risiko manakah yang dominan serta memperhatikan keuntungan dan kerugiannya.

Perbedaan dengan NIST SP 800-30 adalah bahwa pada NIST SP 800-30 tidak ada istilah risiko positif, melainkan semua dianggap negatif sehingga harus dilakukan penanganan untuk menghilangkan atau meminimalkan risiko. Maka dari itu setelah melakukan pengukuran risiko, maka NIST SP 800-30 memberikan tahapan Rekomendasi Kontrol untuk menghilangkan atau meminimalkan risiko.

Tabel 2. 1 Perbedaan NIST SP 800-30 dengan PERMENPANRB No.5 Tahun 2020

SPBE PERMENPAN RB NO.5 TAHUN 2020	**NIST SP 800-30**
Adanya Risiko Positif dan Negatif	Hany Risiko Negatif

Risiko bisa ditangani, dibiarkan atau bahkan di tingkatkan untuk mengejar peluang	Setiap risiko harus ditangani untuk menghilangkan atau meminimalkan risiko.
Terdapat 5 level Kemungkinan dan dampak	Hanya 3 Level Kemungkinan dan Dampak
Setelah pengukuran risiko, masih ada tahap Evaluasi risiko yang menentukan risiko tersebut ditanggapi atau tidak	Setelah pengukuran risiko, maka semua risiko yang terdeteksi merupakan risiko negative yang harus ditanggapi untuk menghilangkan atau meminimalkan risiko.

Secara umum pengukuran Risiko berdasarkan PERMENPAN RB No. 5 Tahun 2020 (Standar Nasional) dengan NIST SP 800-30 (Standar International) memiliki beberapa perbedaan sebagai berikut : Dari beberapa perbedaan diatas yang paling utama adalah cara keduanya dalam memandang risiko. SPBE pada PERMENPAN RB No. 5 Tahun 2020 berusaha melihat dan menemukan potensi keuntungan yang dapat diambil atau dimanfaatkan pada setiap kejadian atau risiko. Ini menjadi salah satu alasan adanya pertimbangan untuk memutuskan apakah risiko tersebut perlu ditangani atau tidak yaitu pada tahapan evaluasi risiko. Akan tetapi terlalu fokus memperhatikan sisi positif juga berpotensi abai terhadap risiko negatif yang tentunya pada sudut perlindungan keamanan informasi pada skala pemerintahan tidak boleh abai pada risiko sekecil apapun itu karena akan berpotensi merugikan. Sementara NIST SP 800-30 tidak mengenal risiko positif dan menilai setiap risiko harus ditangani. Hal tersebut dapat dilihat pada *Risk Assesment Activities* yang langsung menunjukkan langkah *control recommendation* setelah pengukuran risiko.

Maka dari itu kembali ke sasaran yang ingin dicapai, jika sasaran yang ingin dicapai adalah fokus mengendalikan semua

risiko yang ada, maka peneliti beranggapan NIST SP 800-30 lebih baik diterapkan. Namun jika sasaran tetap ingin memperhatikan potensi / hal positif yang bisa dikembangkan untuk mendukung kemajuan dan perkembangan kedepannya yang ada pada setiap risiko, maka Pengukuran Risiko berdasarkan PERMENPAN RB No. 5 Tahun 2020 lebih baik.

Akan tetapi jika dikaitkan dengan asumsi publik bahwa kata "risiko" sudah terlanjur dimaknai sebagai potensi kejadian yang akan berdampak negatif, maka ini sejalan dengan NIST SP 800-30 yang mengenal bahwa risiko adalah hal negatif yang harus diperhatikan dan ditangani. Terlebih lagi penerapan secara nasional berarti menyentuh ke setiap pelosok daerah dan melibatkan Sumber Daya Manusia didaerah yang juga masih terbatas. Maka peneliti tetap beranggapan bahwa NIST SP 800-30 lebih baik diterapkan karna hanya mengenal risiko negatif, kemudian panduan pengukuran detail langkah demi langkah bahkan sampai ke *input* dan *output* pada setiap tahapannya yang terdapat pada *Risk Assesment Acitivities*. Sehingga peneliti beranggapan dengan memakai NIST SP 800-30 pengukuran risiko lebih mudah dipahami dan diterapkan pada skala nasional. Alasan lain peneliti memilih NIST SP 800-30 adalah karena adanya tahapan *control recomendation* yang memungkinkan peneliti sebagai orang yang berada diluar organisasi dapat memberikan rekomendasi kontrol yang dapat dijadikan pertimbangan oleh tim terkait didalam organisasi untuk menghilangkan atau meminimalkan risiko.

3.1.4.1.Dinas Kominfo Statistik dan Persandian Kab. XYZ

Sebelum tahun 2016, Dinas Kominfo Statistik dan Persandian Kab. XYZ pada saat itu bernama DISHUB KOMINFO diisi oleh pegawai

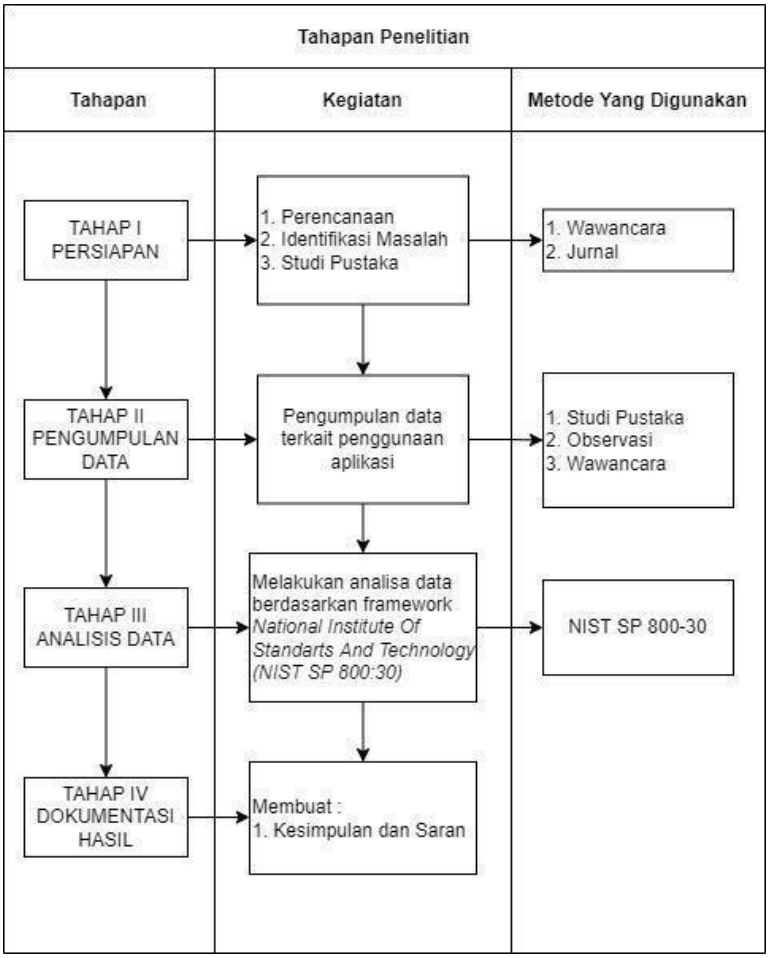
berjumlah sekitar 30 pegawai terdiri dari Bagian Sekretariat (Urusan Umum dan Keuangan) Bidang Perhubungan Darat Bidang Komunikasi dan Bidang Informatika. Kemudian pada Tahun 2016 DISHUB KOMINFO terbagi menjadi dua dinas yaitu Dinas Perhubungan dan Dinas Komunikasi Informasi Statistik dan Persandian Kabupaten XYZ. Sebagai bagian yang paling bertanggung jawab terhadap

teknologi informasi di Kab. XYZ, Dinas Kominfo Statistik dan Persandian Kab. XYZ mengawasi beberapa aplikasi yang diterapkan di Kab. XYZ.

BAB IV
METODE PENELITIAN

4.1. Metode Penelitian

Pendekatan yang akan dipakai pada penelitian ini adalah pendekatan Kualitatif. Adapun tahapan-tahapan penelitian yang akan dilakukan terdiri dari 4 (empat) tahapan sistematis dapat dilihat pada gambar 3.1 dibawah ini.



Gambar 3. 1 Tahapan Penelitian

4.2. Tahapan Penelitian

Adapun tahapan-tahapan dari awal sampai akhir yang akan dilakukan pada penelitian ini adalah sebagai berikut :

1. Persiapan

Pada tahapan persiapan meliputi Melakukan Perancangan, Identifikasi Masalah, dan Studi Pustaka. Sedangkan metode yang digunakan adalah wawancara.

2. Pengumpulan Data

   Pengumpulan data dilakukan untuk mendapatkan data terkait dengan penelitian yang dilakukan. Metode yang digunakan pada pengumpulan data ini adalah studi pustaka, observasi dan wawancara.

3. Tahap Analisis

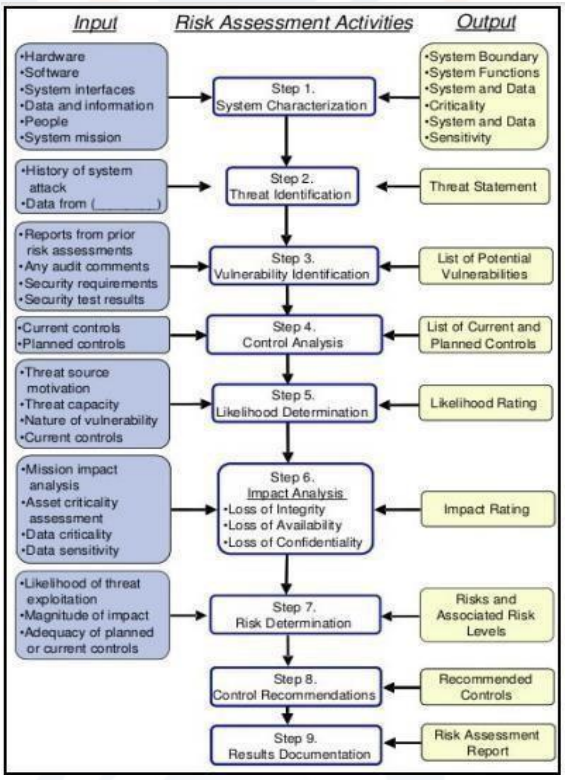
   Langkah ketiga adalah melakukan analisis data yang sudah didapat pada proses sebelumnya dengan menggunakan *framework* NIST SP 800-30.

4. Dokumentasi / Kesimpulan dan Saran

   Langkah terakhir dilakukan dokumentasi laporan kesimpulan dan saran dalam bentuk tugas akhir sesuai dengan format yang berlaku.

4.2.1. Tahapan Analisis Data dan Hasil

Pada tahap Analisa digunakan kerangka kerja *National Institute Of Standarts and Technology* (NIST SP 800-30).



Gambar 3. 2 Langkah-langkah NIST 800-30

Berikut penjelasan terhadap tahap-tahapan / *risk assessment activities* serta *input* dan *output* dari setiap tahapan yang ada pada NIST SP 800-30 (Harsanto & Hidayat, 2018) :

4.2.1.1. System Characterization

Menilai karakteristik dari sistem, melihat sudut pandang *hardware, software infterface*, data dan informasi, hingga tujuan sistem..

4.2.1.2. Threat Identification

Mengenali berbagai ancaman dan sumber yang akan menjadi gangguan pada sistem / mengenali sumber-sumber ancaman pada sistem.

4.2.1.3. Vulnerability Assesment

Pada tahapan ini diidentifikasi berbagai kerentanan yang memungkinkan terjadi ancaman terhadap sistem. *Input* yang ada pada tahapan ini adalah laporan atau *output* dari penilaian risiko sebelumnya. Sementara *output* yang dihasilkan adalah list kerentanan yang ada pada sistem.

4.2.1.4. Control Analysis

Tujuan utama dari tahap ini untuk menganalisis kontrol yang telah diterapkan atau yang akan diterapkan, untuk meminimalisasi kemungkinan terjadinya ancaman.

4.2.1.5. Likelihood Determination

Tahapan ini digunakan untuk memperoleh nilai kecenderungan yang mungkin terjadi atas kelemahan dari sistem.

4.2.1.6. Impact Analysis

Menilai dampak yang terjadi terhadap serangan atas bagian lemah dari sebuah sistem.

4.2.1.7. Risk Determination

Risk determination ini bertujuan untuk menilai tingkat risiko terhadap sistem, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan.

4.2.1.8. Control Recommendation

Tujuannya dari tahapan ini adalah untuk mengurangi level risiko pada sistem TI sehingga mencapai level yang bisa diterima.

4.2.1.9. Result Document

Merupakan laporan dokumentasi dari kegiatan yang ada, dimulai tahap karakteristik hingga rekomendasi kontrol.

BAB V.
BIAYA DAN JADWAL PENELITIAN

1.1.Anggaran Biaya

Justifikasi anggaran biaya ditulis dengan terperinci dan jelas dengan format sebagaimana pada Lampiran B. Sedangkan ringkasan anggaran biaya disusun sesuai dengan format Tabel 5.1 dengan komponen sebagai berikut.

Tabel 5.1 Anggaran Biaya

No	**Jenis Pengeluaran**	**Biaya Yang Diusulkan (Rp.)**
1	Honorarium untuk pelaksana, petugas laboratorium, pengumpul data, pengolahdata, penganalisis data	Rp. 2.500.000,-
2	Pembelian bahan habis pakai untuk ATK, fotocopy, surat menyurat,penyusunan laporan, cetak, penjilidan laporan, publikasi, pulsa, internet,bahan laboratorium, langganan jurnal	Rp. 1.500.000,-
3	Perjalanan untuk biaya survei/sampling data seminar/workshop DN-LN, biaya akomodasi-konsumsi, perdiem/lumpsum, transport, penerbitan luaran penelitian	Rp. 8.100.000,-
4	Sewa untuk peralatan/mesin/ruang laboratorium, kendaraan, peralatan penunjang penelitian lainnya	Rp. 3.400.000,-
	Jumlah	Rp. 14.500.000,-

1.1.**Jadwal Penelitian**

Jadwal pelaksanaan penelitian dibuat dengan tahapan yang jelas untuk 1 tahun dalam bentuk tabel berikut ini

Tabel 5.2. Jadwal Penelitian

No.	Jenis Kegiatan	Tahun 2023											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Persiapan Proposal												
2	Pengumpulan Data												
3	Penelitian Lapangan 1 (Analisa Sistem)												
4	Penelitian Lapangan 2 (Perancangan Sistem)												
5	Penulisan Laporan awal												
6	Penelitian Lapangan 3 (Implementasi Aplikasi)												
7	Penelitian Lapangan 4 (Uji Coba Aplikasi)												
8	Penulisan Laporan Akhir												

BAB VI

HASIL DAN PEMBAHASAN

6.1. Hasil

Hasil dari penelitian ini berupa rekomendasi dari analisis masalah dan pemecahannya. Hasil rekomendasi berupa *Control Recommendation* merupakan tahapan pemberian rekomendasi control untuk menghilangkan atau meminimalkan risiko. Untuk rekomendasi yang diberikan pada tiap jenis risiko dapat dilihat pada table berikut ini.

Tabel 6.1 *Control Recomendation*

Kode	**Sumber**	**Ancaman**	**Celah / Kerawanan**	**Tingkat Risk**	**Rekomendasi Control**
A001	**Manusia**	Lupa Sandi / Username	Turn Over sehingga menyebabkan sering terjadinya pergantian operator / Operator kurang terlatih	*Low*	1. Memberi Username dan sandi yang mudah diingat oleh operator. 2. Memberikan catatan khusus terkait akun kepada operator dan mewajibkan operator terkait untuk menyimpan dan menjaga catatan tersebut agar ketika lupa dapat membuka kembali catatan.

					3. Tim teknis membuat dan menyimpan dokumen yang berisi list akun yang digunakan oleh operator tiap-tiap OPD sebagai backup agar cepat tanggap menanggulangi risiko.
A002		Kebocoran Data Oleh Internal	Tidak Tersedianya Perjanjian Kerja sama yang berisi tanggung jawab kepada operator aplikasi OPD	*High*	1. Membuat perjanjian kerja terkait dengan kewajiban bertanggung jawab atas keamanan dan integritas data yang dikelola oleh operator. 2. Melakukan sosialisasi terkait dengan tingkat sensitifitas data serta pentingnya keamanan data ataupun dokumen.
A003		Aplikasi Error	Pemberian Hak Akses Penuh Pada SDM yang belum memahami sepenuhnya tentang aplikasi yang digunakan.	*Low*	Membuat SOP terkait dengan pemberian jenis Hak Akses operator oleh tim teknis.

A004		Kesalahan Akses	Kurang Terlatihnya SDM	*Low*	Melakukan sosialisasi / pelatihan dan membuatkan dokumen yang berisi penjelasan tentang karakter tiap-tiap aplikasi, sensitifitas data yang dikelola, serta petunjuk lengkap tentang penggunaan aplikasi.
A005		Penyalah Gunaan Hak Akses	Operator Tidak Logout / Exit setelah penggunaan aplikasi.	*Low*	Membuat dan SOP menempelkan terkait penggunaan aplikasi ditempat kerja operator
A006		Data Terhapus	Kurang Terlatihnya SDM,	*Medium*	Melakukan sosialisasi / pelatihan dan membuatkan dokumen yang berisi penjelasan tentang karakter tiap-tiap aplikasi, sensitifitas data yang dikelola, serta Petunjuk lengkap tentang penggunaan aplikasi.
A007		Lupa Cara / alur penggunaan aplikasi	Turn Over Tinggi sehingga menyebabkan sering terjadinya pergantian operator	*Medium*	Melakukan sosialisasi / pelatihan dan membuatkan dokumen yang berisi penjelasan tentang karakter tiap-tiap aplikasi, sensitifitas data yang dikelola, serta petunjuk lengkap tentang

					penggunaan aplikasi.
A008		Mantan Karyawan Nakal	OPD tidak konfirmasi terkait dengan keluarnya operator aplikasi Sehingga tim teknis tidak membekukan hak akses operato tsb / masih punya akses.	*Medium*	1. Membuat perjanjian kerja terkait dengan kewajiban bertanggung jawab atas keamanan dan integritas data yang dikelola oleh operator. 2. Berkoordinasi dan mewajibkan tiap-tiap OPD agar selalu melakukan konfirmasi terkait masuk keluarnya operator kepada tim teknis agar tim teknis dapat mengambil tindakan pembekuan akun yang dimiliki atau diketahui oleh mantan karyawan yang dimaksud.

A009		Hacker / Cracker	Tidak adanya tim khusus yang bertanggung jawab terhadap keamanan sistem.	*Low*	Membentuk tim khusus yang bertanggung jawab terhadap keamanan sistem informasi agar dapat fokus terhadap pencegahan serangan dari luar
A010		Internal Nakal	Tidak Tersedianya Perjanjian Kerja sama yang beris tanggung jawab kepada operator aplikasi OPD	*Low*	Membuat perjanjian kerja terkait dengan kewajiban bertanggung jawab atas keamanan dan integritas data yang dikelola oleh operator.
A011	Listrik	Kerusakan Hardware / PC Rusak	Listrik Sering Padam Tidak tersedianya UPS	*High*	1. Menyediakan *Uninteruptible Power Supply* (UPS) agar PC tidak
A012		Hardware Terbakar	Listrik Sering Padam Tidak tersedianya UPS	*High*	mati secara mendadak ketika listrik padam agar dapat melakukan penyimpanan terhadap dokumen yang dikerjakan sehingga file tidak hilang / korup. Kemudian agar dapat mematikan PC secara Normal. 2. Menyediakan
A013		Kehilangan Data / Data Korup	Listrik Sering Padam Tidak tersedianya UPS	*High*	
A014		Sinyal Internet Mati	Listrik Sering Padam, Tidak tersedianya UPS dan Genset Generator sebagai listrik cadangan.	*Medium*	

A015		Aplikasi Tidak Dapat Digunakan	Listrik Sering Padam, Tidak tersedianya UPS dan Genset sebagai listrik cadangan.	*Low*	Genset Generator sebaga sumber listrik cadangan.
A016	Teknis (Virus)	Hilangnya data /asset penting. Software tidak dapat diakses. Hilang atau rusaknya data – data penting.	Tidak Tertib penggunaan Flasdisk	*High*	1. Selalu memasang dan merawat anti virus. 2. Mengunduh aplikasi dari sumber terpercaya. 3. Menggunakan aplikasi yang berlisensi resmi. 4. Selalu melakukan *backup* terhadap data-data yang penting.
A017			Tidak tertibnya penggunaan anti virus	*Low*	
A018			Mengunduh dan menginstal aplikasi secara sembarangan	*Medium*	

Dokumen hasil rekomendasi merupakan thapan dokumentasi rangkuman hasil proses pengukuran manajemen resiko berdasarkan *risk assessment activities* pada *framework National Institute of Standard and Technology* (NISP) SP 800-3-. Rekomendasi tersebut dapat dilihat pada pembahasan dibawah ini.

6.2. Pembahasan

6.2.1. Pengumpulan Data

1. Studi Pustaka

   Studi pustaka dilakukan untuk 7 mendukung dalam pengerjaan tugas akhir, mulai dari tahap pengembangan hingga tahap akhir.

2. Wawancara

   Wawancara dilakukan dengan dua orang yaitu Bapak Ayubi Khaafidh selaku kepala tim teknis / *local it support* karena kepala tim teknis yang diwawancara saat proses identifikasi masalah yang dilakukan sebelumnya yaitu Bapak Gusta, S.Kom sudah tidak di Diskominfo melainkan sudah pindah ke BKD-PSDM. Dan Bapak Indra Asura selaku tim yang mengelola dan melakukan control terhadap penggunaan SPBE / *E-Government* sekaligus operator umum SPBE Diskominfo Kab. XYZ. Wawancara dilakukan untuk memenuhi kebutuhan data pada proses Analisa manajemen / pengukuran risiko pada penelitian ini sesuai dengan konsep dari *framework NIST 800-30*.

3. Observasi

   Observasi dilakukan bertujuan untuk melakukan pengamatan langsung dilokasi atau tempat objek penelitian.:

   a. Diskominfo Kab. XYZ

      Dinas Komunikasi, Informasi, Statistik dan Persandian Kabupaten XYZ adalah sebuah instansi pemerintah yang bertanggung jawab dalam pelaksanaan urusan pemerintaha dibidang komunikasi, informatika, statistic dan persandian di Kabupaten XYZ. Dinas Komunikasi Informasi Statistik dan Persandian Kabupaten XYZ beralamatkan di Jl. Lintas Barat Desa Sinar Pagi Kec. XYZ Selatan, Kab. XYZ.

Gambar 6.1. Diskominfo Kab. XYZ

6.2.2. Daftar Aplikasi

Adapun daftar aplikasi yang aktif digunakan di Kabupaten XYZ berdasarkan hasil interview yang sudah dilakukan :

Tabel 6.2. Daftar Aplikasi

No	Jenis	Fungsi	OPD Yang Menggunakan
1	SP4N LAPOR	Pengaduan / Pelaporan	Semua OPD
2	SANAKKITE	Pelayanan Dukcapil	DUKCAPIL
3	WEBSITE INDUK	Website Kabupaten yang berisi semua sistem informasi pemkab XYZ (OPD, Kecamatan, dll).	Semua OPD sampai Kecamatan.
4	FILE BERKALA	Pengajuan Kenaikan Gaji Secara Berkala	Semua OPD
5	PPID	Pengelola Informasi dan Dokumentasi	Diskominfo
6	SAKIP	Akuntabilitas Kinerja Instansi Pemerintah	Semua OPD
7	IPKD	Pengelolaan Keuangan Daerah	Keuangan

6.2.3. Analisis Data Dengan NIST SP 800-30

Pada tahap ini dilakukan analisis / pengukuran risiko pada Dinas Komunikasi Informasi Statistik dan Persandian Kabupaten XYZ dengan menggunakan *framework National Institute Of Standarts And Technology*.

Adapun proses-prosesnya adalah sebagai berikut :

6.2.3.1. *System. Characterization*

Aplikasi sistem informasi yang ada di Kabupaten dan dibawah naungan Diskominfo Kabupaten XYZ merupakan aplikasi berbasis website dan berbasis online. Sumber daya perangkat keras yakni *Personal Computer* (PC) yang digunakan untuk mengoperasikan aplikasi sistem informasi dengan sistem operasi windows 10. Sedangkan data dan informasi yang yang dikelola oleh aplikasi-aplikasi yang ada pada kabupaten adalah Dokumen Kabupaten, Data Statistik, Data masyarakat, dan data penting lainnya sementara Sumber daya manusia adalah operator dari aplikasi sistem informasi. Aplikasi – aplikasi ini berbasis online dan dioperasikan melalui PC. Oleh karena itu maka penggunaan aplikasi sangat bergantung dengan sumber daya listrik dan internet karena aplikasi tidak dapat dijalankan jika tidak ada sumber daya listrik dan sumber daya internet. Aplikasi – aplikasi yang dipakai pada pemerintahan dioperasikan oleh OPD terkait dan diawasi oleh pihak Diskominfo Kabupaten dalam penggunaannya.

6.2.3.2. Threat Identification

Berdasarkan hasil wawancara yang sudah dilakukan kepada dua narasumber di Diskominfo Kabupaten XYZ, maka diperolah ancaman sebagai berikut :

Tabel 6.3. Threat Identification / Identifikasi Ancaman

Sumber	Motivasi / Penyebab	Ancaman	Kode

Manusia	Human Error	1. Lupa Sandi / Username 2. Kebocoran Data Oleh Internal 3. Aplikasi Error 4. Kesalahan Akses 5. Penyalah Gunaan Hak Akses 6. Data Terhapus 7. Lupa Cara / alur penggunaan aplikasi	A001 A002 A003 A004 A005 A006 A007
	Ego	1. Mantan Karyawan Nakal 2. Hacker / Cracker 3. Internal Nakal	A008 A009 A010
Listrik	Kerusakan Jaringan Listrik	1. Kerusakan Hardware / PC Rusak 2. Hardware Terbakar 3. Kehilangan Data / Data Korup 4. Sinyal Internet Mati 5. Aplikasi Tidak Dapat Digunakan	A011 A012 A013 A014 A015
Teknis	Virus	1. Hilangnya data /asset penting 2. Software tidak dapat diakses 3. Hilang atau rusaknya data – data penting	A016 A017 A018

6.2.3.3. Vulnerability Identification

Berdasarkan wawancara yang dilakukan didapatkan bahwa kerentanan sistem pada Diskominfo Kab. XYZ adalah sebagai berikut :

Tabel 6.4. *Vulnerability Identification*

Sumber	Ancaman	Celah / Kerawanan	Kode
	Lupa Sandi / Username	Turn Over Tinggi sehingga menyebabkan sering terjadinya pergantian operator / Operator kurang terlatih	A001
	Kebocoran Data	Tidak Tersedianya Perjanjian Kerja sama yang berisi tanggung jawab kepada operator aplikasi OPD	A002
	Aplikasi Error	Pemberian Hak Akses Penuh	

Manusia		Pada SDM yang belum memahami sepenuhnya tentang aplikasi yang digunakan.	A003
	Kesalahan Akses	Kurang Terlatihnya SDM,	A004
	Penyalah Gunaan Hak Akses	Operator Tidak Logout / Exit setelah penggunaan aplikasi.	A005
	Data Terhapus	Kurang Terlatihnya SDM,	A006
	Lupa Cara / alur penggunaan aplikasi	Turn Over Tinggi sehingga menyebabkan sering terjadinya pergantian operator	A007
	Mantan Karyawan Nakal	OPD tidak konfirmasi terkait dengan keluarnya operator aplikasi. Sehingga tim teknis tidak membekukan hak akses operator tsb / masih punya akses.	A008
	Hacker / Cracker	Tidak adanya tim khusus yang bertanggung jawab terhadap keamanan sistem.	A009
	Internal Nakal	Tidak Tersedianya Perjanjian Kerja sama yang berisi tanggung jawab kepada operator aplikasi OPD	A010
Listrik	Kerusakan Hardware / PC Rusak	Listrik Sering Padam Tidak tersedianya UPS	A011
	Hardware Terbakar	Listrik Sering Padam Tidak tersedianya UPS	A012
	Kehilangan Data / Data Korup	Listrik Sering Padam Tidak tersedianya UPS	A013
	Sinyal Internet Mati	Listrik Sering Padm Tidak tersedianya UPS dan Genset / Generator sebagai listrik cadangan.	A014

	Aplikasi Tidak Dapat Digunakan	Listrik Sering Padam Tidak tersedianya UPS dan Genset sebagai listrik cadangan.	A015
Teknis (Virus)	1. Hilangnya data /asset penting. 2. Software tidak dapat diakses 3. Hilang atau rusaknya data – data penting	Tidak Tertib penggunaan Flasdisk	A016
		Tidak tertibnya penggunaan anti virus	A017
		Mengunduh dan menginstal aplikasi secara sembarangan	A018

6.2.3.4. *Control Analysis*

Berdasarkan hasil wawancara yang sudah dilakukan maka didapatkan hasil berupa control sebagai berikut :

Tabel 6.5. *Control Analysis*

Kode	Ancaman	Control
A001	Lupa Sandi / Username	Melakukan Koordinasi dan penjelasan ulang terhadap hal yang belum diketahui atau lupa kepada operator terkait.
A004	Kesalahan Akses	
A007	Lupa Cara / alur penggunaan aplikasi	
A002	Kebocoran Data	Melakukan Koordinasi terkait dengan sensitifitas data serta pentingnya keamanan data dan tanggung jawab terhadap keamanan data oleh operator.
A003	Aplikasi Error	
A005	Penyalah Gunaan Hak Akses	
A006	Data Terhapus	
A008	Mantan Karyawan Nakal	Melakukan koordinasi terkait sensitifitas data, pentingnya keamanan data, tanggung jawab yang diemban terkait keamanan
A010	Internal Nakal	
		data, dan pentingnya bersikap jujur dan professional kepada operator.

A009	Hacker / Cracker	Sosialisasi / koordinasi dengan karyawan dan pimpinan terkait penguatan keamanan sistem.
A011	Kerusakan Hardware / PC Rusak	Sosialisasi / koordinasi dengan karyawan / pimpinan OPD terkait terkait pencegahan. misalnya menggunakan UPS.
A012	Hardware Terbakar	
A014	Sinyal Internet Mati	
A015	Aplikasi Tidak Dapat Digunakan	
A013	Kehilangan Data / Data Korup	Sosialisasi kepada operator agar dapat sering menyimpan file yang sudah di buat/edit agar tidak hilang atau korup. Serta melakukan backup terhadap file-file yang penting.
A016	Hilangnya data /asset penting	Melakukan koordinasi dan sosialisai dengan operator terkait dengan sensitifitas data, agar memasang anti virus, tertib dalam penggunaan flasdisk, dan bahaya virus terhadap data dan sumber-sumber dari virus.
A017	Software tidak dapat diakses	
A018	Hilang atau rusaknya data – data penting	

6.2.3.5. .*Likelihood Determination*

Pada tahapan ini dicari kemungkinan terjadinya sebuah risiko dari ancaman yang ada. Penentuan kemungkinan dibagi menjadi tiga jenis yaitu *High*, *Medium*, dan Level kemungkinan terjadinya risiko dari tiap ancaman adalah sebagai berikut :

Tabel 6.6. Likelihood Determination

Kode	**Sumber**	**Ancaman**	**Celah / Kerawanan**	**Tingkat Kemungkinan**

A001	**Manusia**	Lupa Sandi / Username	Turn Over sehingga menyebabkan sering terjadinya pergantian operator / Operator kurang terlatih	*Medium*
A002		Kebocoran Data	Tidak Tersedianya Perjanjian Kerja sama yang berisi tanggung jawab kepada operator aplikasi OPD	*High*
A003		Aplikasi Error	Pemberian Hak Akses Penuh Pada SDM yang belum	*Low*
			memahami sepenuhnya tentang aplikasi yang digunakan.	
A004		Kesalahan Akses	Kurang Terlatihnya SDM	*Low*
A005		Penyalah Gunaan Hak Akses	Operator Tidak Logout / Exit setelah penggunaan aplikasi.	*Low*
A006		Data Terhapus	Kurang Terlatihnya SDM,	*Medium*
A007		Lupa Cara / alur penggunaan aplikasi	Turn Over Tinggi sehingga menyebabkan sering terjadinya pergantian operator	*Medium*
A008		Mantan Karyawan Nakal	OPD tidak konfirmasi terkait dengan keluarnya operator aplikasi. Sehingga tim teknis tidak membekukan hak akses operator tsb / masih punya akses.	*Medium*
A009		Hacker / Cracker	Tidak adanya tim khusus yang bertanggung jawab terhadap keamanan sistem.	*Low*
A010		Internal Nakal	Tidak Tersedianya Perjanjian Kerja sama yang berisi tanggung jawab kepada operator aplikasi OPD	*Low*
A011		Kerusakan Hardware / PC Rusak	Listrik Sering Padam Tidak tersedianya UPS	*High*

A012	Listrik	Hardware Terbakar	Listrik Sering Padam Tidak tersedianya UPS	*High*
A013		Kehilangan Data / Data Korup	Listrik Sering Padam Tidak tersedianya UPS	*High*
A014		Sinyal Internet Mati	Listrik Sering Padam, Tidak tersedianya UPS dan Genset / Generator sebagai listrik cadangan.	*High*
A015		Aplikasi Tidak Dapat Digunakan	Listrik Sering Padam, Tidak tersedianya UPS dan Genset sebagai listrik cadangan.	*Medium*
A016	Teknis (Virus)	1. Hilangnya data/asset penting	Tidak Tertib penggunaan Flasdisk	*High*
A017			Tidak tertibnya penggunaan anti virus	*Low*
A018		2. Software tidak dapat diakses 3. Hilang atau rusaknya data –data penting	Mengunduh dan menginstal aplikasi secara sembarangan	*Medium*

6.2.3.6. *Impact Analysis*

Berikut adalah level dampak yang dihasilkan oleh ancaman risiko :

Tabel 6.7. Impact Analysis

Kode	Sumber	Ancaman	Tingkat Dampak
A001	Manusia	Lupa Sandi / Username	*Low*
A002		Kebocoran Data	*High*
A003		Aplikasi Error	*Low*
A004		Kesalahan Akses	*Low*
A005		Penyalah Gunaan Hak Akses	*Medium*
A006		Data Terhapus	*High*
A007		Lupa Cara / alur penggunaan aplikasi	*Medium*
A008		Mantan Karyawan Nakal	*High*
A009		Hacker / Cracker	*High*

A010		Internal Nakal	*Medium*
A011	Listrik	Kerusakan Hardware / PC Rusak	*High*
A012		Hardware Terbakar	*High*
A013		Kehilangan Data / Data Korup	*High*
A014		Sinyal Internet Mati	*Medium*
A015		Aplikasi Tidak Dapat Digunakan	*Low*
A016	Teknis *(Virus)*	1. Hilangnya data /asset penting 2. Software tidak dapat diakses 3. Hilang atau rusaknya data – data penting	*High*
A017			*Medium*
A018			*High*

6.2.3.7. *Risk Determination*

Tahapan ini bertujuan untuk melakukan penilaian terhadap tingkat risiko yang dihadapi pada penggunaan aplikasi sistem informasi di Diskominfo Kabupaten XYZ. Penilaian risiko ini diperoleh dengan melakukan perkalian antara level – level yang ditetapkan pada proses

Likelihood Identification (Identifikasi kemungkinan) dengan *impact analysis* (Analisa Dampak) seperti ditunjukkan pada rumus berikut ini :

Penilaian Risiko = Dampak (*impact*) x Peluang (*Likelihood*)

Untuk menentukan atau penilaian risiko digunakan matriks seperti pada table dibawah ini sebagai acuan perhitungan. Matriks ini menunjukkan bagaimana tingkat risiko secara keseluruhan. Adapun range angka dalam penentuan penilaian risiko ini adalah 1 sampai 10 tingkat risiko *Low*, lebih dari 10 sampai 50 tingkat risiko *Medium*, sedangkan lebih dari 50 sampai 100 tingkat risiko *High.*

Threat Likelihood	Impact		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Gambar 6.2. Matriks Level Risiko (Sumber : Nugraha et al., 2020)

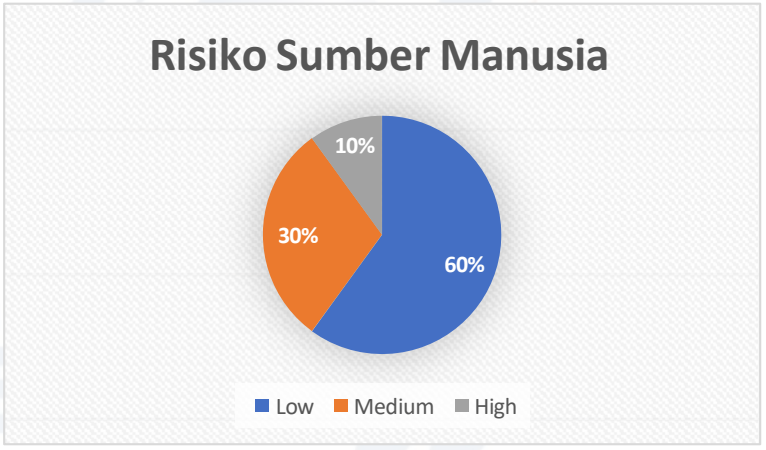
Selanjutnya, dari matriks diatas, proses perhitungan dan penilaian risiko dapat dilihat pada table dibawah ini :

Tabel 6.8. Risk Determination

Kode	Sumber	Ancaman	Tingkat Kemungkinan	Tingkat Dampak	Kemungkinan x Dampak
A001	Manusia	Lupa Sandi / Username	*Medium (0.5)*	*Low (10)*	0.5 x 10 = 5 (*Low*)
A002		Kebocoran Data Oleh Internal	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A003		Aplikasi Error	*Low (0.1)*	*Low (10)*	0.1 x 10 = 1 (*Low*)
A004		Kesalahan Akses	*Low (0.1)*	*Low (10)*	0.1 x 10 = 1 (*Low*)
A005		Penyalah Gunaan Hak Akses	*Low (0.1)*	*Medium (50)*	0.1 x 50 = 5 (*Low*)
A006		Data Terhapus	*Medium (0.5)*	*High (100)*	0.5 x 100 = 50 (*Medium*)
A007		Lupa Cara / alur penggunaan aplikasi	*Medium (0.5)*	*Medium (50)*	0.5 x 50 = 25 (*Medium*)
A008		Mantan Karyawan Nakal	*Medium (0.5)*	*High (100)*	0.5 x 100 = 50 (*Medium*)
A009		Hacker / Cracker	*Low (0.1)*	*High (100)*	0.1 x 100 = 10 (*Low*)
A010		Internal Nakal	*Low (0.1)*	*Medium (50)*	0.1 x 50 = 5 (*Low*)
A011	Listrik	Kerusakan Hardware / PC Rusak	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A012		Hardware Terbakar	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A013		Kehilangan Data / Data Korup	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A014		Sinyal Internet Mati	*High (1.0)*	*Medium (50)*	1.0 x 50 = 50 (*Medium*)
A015		Aplikasi Tidak Dapat Digunakan	*Medium (0.5)*	*Low (10)*	0.5 x 10 = 5 (*Low*)

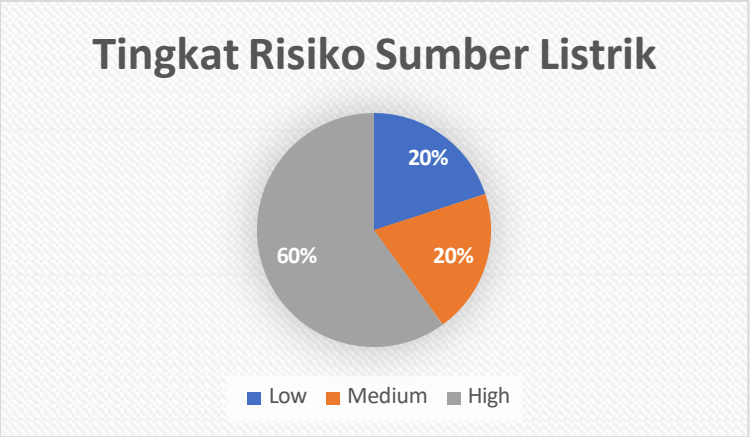
A016	Teknis (Virus)	1. Hilangnya data /asset penting 2. Software tidak dapat diakses 3. Rusaknya data – data penting	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A017			*Low (0.1)*	*Medium (50)*	0.1 x 50 = 5 (*Low*)
A018			*Medium (0.5)*	*High (100)*	0.5 x 100 = 50 (*Medium*)

Adapun berdasarkan hasil dari perhitungan diatas risiko yang bersumber dari manusia telah ditemukan risiko dengan tingkat *medium* hingga *high*. Berdasarkan perhitungan diatas, tingkat risiko yang bersumber dari manusia adalah 6 risiko dengan tingkat risiko *Low*, 3 risiko dengan tingkat risiko *Medium*, dan 1 risiko dengan tingkat risiko *High*. Berikut adalah grafik tingkat risiko yang bersumber dari manusia.



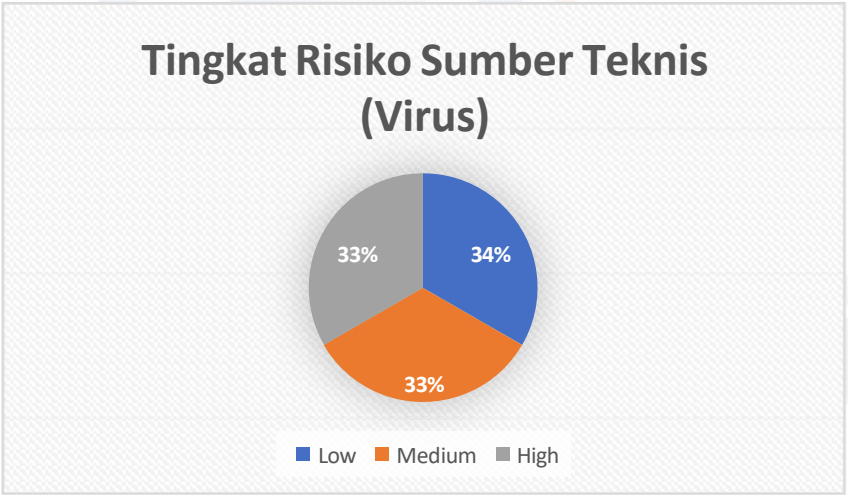
Gambar 6. 2 Grafik Risiko Bersumber dari Manusia

Sedangkan risiko yang berasal dari Listrik berdasarkan perhitungan yang dilakukan diatas adalah 1 risiko dengan tingkat *Low*, 1 risiko dengan tingkat risiko *Medium*, dan 3 risiko dengan tingkat *High*. Berikut tampilan grafik tingkat risiko yang bersumber dari Listrik.



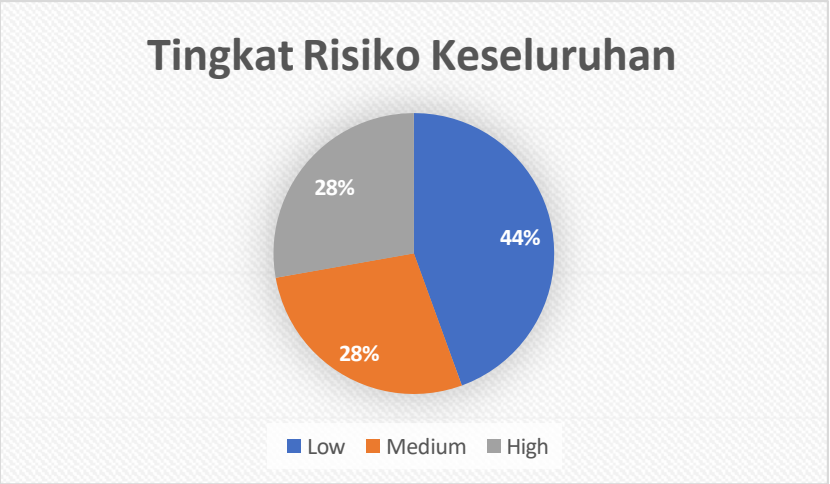
Gam ɔar 6. 4 Grafik Tingkat Risiko Bersumber Dari Listrik

Sedan gkan Risiko yang berasal dari sumber Teknis (Virus) berdasa rkan perhitungan pada table diatas didapatkan hasil 1 risiko dengan tingkat risiko*Low*, 1 risiko tingkat *Medium,* dan 1 risiko tingkat *High.* Berikut grafik risikoyang bersumber dari Virus.



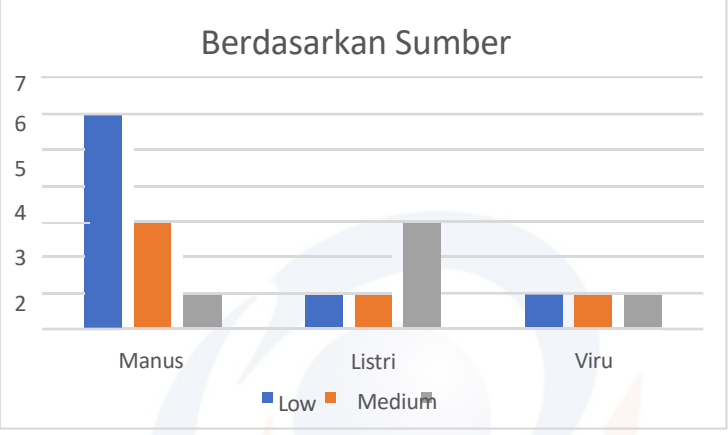
Gambar 6. 5 Grafik Tingkat Risiko Bersumber dari Virus

Secara keseluruhan grafik penilaian risiko berdasarkan perhitungan pada table diatas adalah didapatkan 8 risiko dengan tingkat risiko *Low*, 5 risiko dengan tingkat risiko *Medium*, dan 5 risiko dengan tingkat *High.* Berikut grafik yang secara keseluruhan hasil perhitungan atau pengukuran risiko yang ada di Dikominfo Kab. XYZ.



Gambar 6. 6 Grafik Tingkat Risiko Keseluruhan

Dan berdasarkan sumber risiko, ancaman risiko dengan tingkatan *low* terbanyak dari sumber Manusia dengan 6 ancaman risiko, sedangkan untuk ancaman bsersumber dari listrik dan virus masing – masing memiliki 1 ancaman risiko. Untuk tingkatan risiko *medium* terbanyak adalah ancaman risiko yang juga bersumber dari Manusia dengan 3 ancaman risiko, kemudian yang bersumber dari listrik dan virus juga masing-masing memiliki 1 ancaman risiko. Dan terakhir untuk risiko *high* paling banyak ditimbulkan dari ancaman risiko yang bersumber dari Listrik dengan 3 ancaman risiko, kemudian untuk yang bersumber dari manusia dan virus masing-masing memiliki 1 ancaman risiko. Untuk selengkapnya ditunjukkan pada grafik dibawah ini :



Gambar 6. 7 Grafik Berdasarkan Sumber Risiko

BAB VII

KESIMPULAN DAN SARAN

7.1. Kesimpulan

Berdasarkan pembahasan yang sudah dibahas pada bab sebelumnya, maka kesimpulan yang dapat ditarik dari hasil penelitian ini adalah sebagai berikut :

1. Ancaman risiko yang ada pada penggunaan aplikasi sistem informasi Kabupaten XYZ yang dikelola atau dinaungi oleh Dinas Komunikasi Informatika Statistik dan Persandian Kabupaten XYZ yang terdeteksi berasal dari tiga sumber yaitu 10 ancaman risiko bersumber dari Manusia, 5 ancaman risiko bersumber dari Listrik, dan 3 ancamn risiko yang bersumber dari Teknis, dengan total 18 ancaman risiko.
2. Dari hasil pengukuran risiko yang sudah dilakukan berdasarkan NIST 800-30 didapatkan hasil bahwa ancaman risiko yang bersumber dari manusia adalah 60% risiko dengan tingkat *Low,* 30% risiko dengan tingkat *Medium*, dan 10% risiko dengan tingkat *High*. Sedangkan risiko yang bersumber dari listrik adalah 20% risiko dengan tingkat *Low,* 20% risiko dengan tingkat *Medium,* dan 60% risiko dengan tingkat *High*. Dan terakhir yang bersumber dari Teknis adalah 34% risiko dengan tingkat *Low,* 33% risiko tingkat *Medium,* dan 33% risiko tingkat *High*. Secara keseluruhan hasil penilaian risiko adalah 39% ancaman risiko dengan tingkat *Low,* 33% ancaman risiko dengan tingkat *Medium,* dan 28% ancaman risiko dengan tingkat *High*.
3. Dari hasil pengukuran yang dilakukan untuk tingkatan risiko *high* paling banyak berasal dari sumber Listrik, tingkatan *medium* paling banyak berasal dari Manusia, sedangkan untuk tingkatan ancaman isiko *low* paling banyak juga bersumber dari manusia *low* paling banyak juga bersumber dari manusia.
4. Berdasarkan Analisa yang sudah dilakukan, disimpulkan bahwa ancaman risiko yang muncul sesuai dengan hasil wawancara yang dilakukan secara umum disebabkan oleh masih belum matangnya sistem yang dijalankan terkait dengan penggunaan aplikasi pada pemerintahan.

7.2. Saran

Adapun saran yang dapat diberikan oleh peneliti adalah sebagai berikut :

1. Melakukan pengamatan secara terus menerus dan intensif dalam rangka memperbaharui informasi terkait dengan penggunaan aplikasi sistem informasi untuk mendapatkan ancaman-ancaman risiko yang belum terdeteksi agar dapat melakukan tindakan untuk mencegah ataupun meminimalkan risiko.
2. Perlu adanya kesadaran dan kerja sama antar seluruh komponen yang terlibat dan bertanggung jawab dalam penggunaan aplikasi sistem informasi untuk mengikuti prosedur dan melakukan control agar tidak terjadinya ancaman risiko serta manajemen risiko dapat berjalan dengan sebagimana mestinya

DAFTAR PUSTAKA

Ekelhart, A. S. Fenz och T. Neubauer. (2009). AURUM: A Framework for Information Security Risk Management. *Hawaii International Conference on System Sciences*.

Elanda, A., & Buana, R. L. (2021). Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus: STMIK Rosma). *Elkom: Jurnal Elektronika Dan Komputer*. https://journal.stekom.ac.id/index.php/elkom/article/view/387

Fahrudin, N. fitrianti, Nugraha S, A., & Ramadhan Putra, K. (2022). Penilaian Risiko Keamanan Data Karyawan Pada Sistem Informasi Dengan Menggunakan Framework Nist Sp 800-30 pada PT. ABC. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *8*(3). https://doi.org/10.33197/jitter.vol8.iss3.2022.900

Harimurti, F. (2006). Manajemen Risiko, Fungsi dan Mekanismenya. *Fakultas Ekonomi Universitas Slamet Riyadi*, 105–112.

Harsanto, K., & Hidayat, D. (2018). Sistem Informasi Manajemen Risiko dengan Menggunakan Framework National Institute of Standards and Technology pada Lembaga Pendidikan. *Jurnal Ipsikom*, *6*(1).

Mahardika, F. (2017). *Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)*. *02*(02), 1–8.

Martin Halomoan Lumbangaol, M. R. R. (2020). Rancang Bangun Sistem Informasi Penjualan dan Penyewaan Properti Berbasis WEB Di Kota Batam. *Jurnal Comasie*, *01*(03), 83–92.

Muka, W., & Wibowo, M. A. (2021). Penerapan Manajemen Risiko pada ProsespengembanganProperti. *Jurnal Permukiman*, *16*(1) 31. https://doi.org/10.31815/jp.2021.16.31-40

Nugraha, B. A., Perdanakusuma, A. R., & (2020). Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika …. *... Teknologi Informasi Dan …*. http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6884

Putro, A. A., Ambarwati, A., & Setiawan, E. (2021). Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1. *... Teknologi Dan Informasi*. https://ojs.unikom.ac.id/index.php/jati/article/view/5314

Ramadhani, S. N., & Baharudin, M. (2019). Efektivitas Manajemen Risiko Dan Hasil Suswati Risnaeni. *Jurnal Akuntansi Dan Keuangan Islam*, *1*(2), 6.

Saepul, A., C, Y. H., & Hadiana, A. I. (2017). Manajemen Risiko Teknologi Informasi Berbasis National Institute of Standards and Technology SP800-30 di Universitas Jenderal Achmad Yani. *Seminar Nasional Informatika Dan Aplikasinya (SNIA) 2017, September*, 44–48.

Somantri, G. R. (2005). Gumilar Rusliwa Somantri. *Makara, Sosial Humaniora*,

9(2), 57–65. https://media.neliti.com/media/publications/4388-ID-memahami-metode-kualitatif.pdf

Sompie, M. D. J. S. B. F. (2014). MANAJEMEN RISIKO PADA PERUSAHAAN JASA
PELAKSANA KONSTRUKSI DI PROPINSI PAPUA (Study Kasus di Kabupaten Sarmi). *Jurnal Ilmiah Media Engineering*, *4*(2), 109–118.

Sulthoni, A. (2014). SISTEM INFORMASI E-COMMERCE PEMASARAN HASIL PERTANIAN DESA KLUWAN BERBASIS WEB. *Jurnal Sistem Informasi*, *58*(12), 7250–7257. https://doi.org/10.1128/AAC.03728-14

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30. *Jurnal CoreIT*, *2*(2), 6.

Tri, M. B. (2020). Perancangan Sistem Informasi Management Siswa Berprestasi Berbasis Android Pada Smk Pgri Rawalumbu. *Jurnal Sains & Teknologi Fakultas Teknik*, *X*(2), 30–39.

Tukino. (2020). Computer Based Information System Journal Rancang Bangun Sistem Informasi E-Marketing Pada PT Pulau Cahaya Terang. *Cbis Journal*, *08*(01), 25.

Widarma, A., & Kumala, H. (2018). Perancangan Gaji Karyawan Pada PT. PP London Sumatra.Tbk. *Jurnal Teknologi Informasi*, *1*(2), 166.

Tempat : **Diskominfo Kab. XYZ**

Hari : **Selasa 31 Januari 2023**

Waktu : **09.20 – 10.12**

Surat Pernyataan Ketua Pelaksana Penelitian

Yang bertadatangan di bawah ini:

Nama	: Budi Tjahjono
NIDN/NIK	: 0330126703/205040315
Fakultas/ Prodi	: Ilmu Komputer/Magister Komputer
Jabatan fungsional	: Lektor Kepala

Dengan ini saya menyatakan bahwa proposal program penelitian yang diajukan dengan judul:

"MANAJEMEN RISIKO PADA PENGGUNAAN APLIKASI SISTEM INFORMASI DI DINAS KOMINFO STATISTIK DAN PERSANDIAN KAB. XYZ MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDART AND TECHNOLOGY (NIST SP 800-30)

"

Yang saya usulkan dalam skema penelitian dasar internal Universitas Esa Unggul tahun 2024 bersifat original dan belum pernah dibiayai oleh lembaga/ sumber dana lain.

Bilamana diketahui dikemudian hari adanya indikasi ketidakjujuran/ itikad kurang baik sebagaimana dimaksud di atas, maka kegiatan ini dibatalkan dan saya bersedia mengembalikan dana yang telah diterima kepada pihak Universitas Esa Unggul melalui LPPM.

Demikian pernyataan ini dibuat dengan sesumgguhnya dan dengan sebenar-benarnya.

Jakarta, 22 September 2024

Yang menyatakan,

Nama Ketua: Budi Tjahjono
NIDN: 0330126703

SURAT TUGAS
No. 010/ST-PEN/LPPM/UEU/IX/2024

Yang bertandatangan di bawah ini:

Nama : LARAS SITOAYU, S.Gz, M.K.M
Jabatan : Kepala LPPM

Menugaskan nama-nama dibawah ini:

No.	Nama	Jabatan	NIDN/NIDK/NUP	Fakultas
1	Dr. BUDI TJAHJONO, S.Kom, M.Kom	Ketua	0330126703	Fakultas Ilmu Komputer
2	20200804012 - Miri Ardiansyah	Anggota 1		
3	Dr. GERRY FIRMANSYAH, S.T.M.Kom	Anggota 2	0305116804	Fakultas Ilmu Komputer
4	HABIBULLAH AKBAR, S.Si, M.Sc, Ph.D	Anggota 3	0315108201	Fakultas Ilmu Komputer

Untuk melakukan kegiatan penelitian dengan judul:
"MANAJEMEN RISIKO PADA PENGGUNAAN APLIKASI SISTEM INFORMASI DI DINAS KOMINFO STATISTIK DAN PERSANDIAN KAB. XYZ MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDART ANDTECHNOLOGY (NIST SP 800-30)"

Demikian surat tugas ini dibuat untuk dipergunakan sebagaimana mestinya.

Jakarta, 27 September 2024
Kepala LPPM

LARAS SITOAYU, S.Gz, M.K.M
NIK. 215080596

Lampiran 3. Biodata Ketua Pengusul

KETUA PENELITI

A. Identitas Diri

1	Nama Lengkap (dengan gelar)	: Dr. Budi Tjahjono, S.Kom, M.Kom
2	Jenis Kelamin	: Laki-laki
3	Alamat	: Kampung Parung Serab RT. 05/04 Depok
4	Jabatan Fungsional	: Lektor Kepala
5	NIP/NIK/Identitas Lainnya	: 205040315/3276063012670002
6	NIDN	: 0330126703
7	Tempat dan Tanggal Lahir	: Surabaya, 30-12-1967
8	Agama	: Islama
7	E-mail	: budi.tjahjono@esaunggul.ac.id
8	Nomor Telepon/HP	: 08983444426
9	Alamat Kantor	: Jl. Arjuna Utara no. 9, Kebon Jeruk, Jakbar
10	Nomor Telepon/Faks	: 021 5674223
11	Mata Kuliah yang Diampu	1. Matematika Diskrit
		2. Topik dalam Pemrograman
		3. Jaringan Komputer

B. Riwayat Pendidikan

	S-1	**S-2**	S-3
Nama Perguruan Tinggi	Sekolah Tinggi Teknik Surabaya	Universitas Indonesia	Universitas Negeri Jakarta
Bidang Ilmu	Ilmu Komputer	Ilmu Komputer	Manajemen Pendidikan
Tahun Masuk-Lulus	1994	1999	2020
Judul Skripsi/Tesis/Disertasi	Jaringan Komputer Mainframe	Information Economics	Kinerja Dosen
Nama Pembimbing/Promotor	Khinardi Gunawan	Benny Ranti	Muchner Muchtar

A. Riwayat Pendidikan

	S-1	**S-2**	S-3
Nama Perguruan Tinggi	Sekolah Tinggi Teknik Surabaya	Universitas Indonesia	Universitas Negeri Jakarta
Bidang Ilmu	Ilmu Komputer	Ilmu Komputer	Manajemen Pendidikan
Tahun Masuk-Lulus	1994	1999	2020
Judul Skripsi/Tesis/Disertasi	Jaringan Komputer Mainframe	Information Economics	Kinerja Dosen
Nama Pembimbing/Promotor	Khinardi Gunawan	Benny Ranti	Thamrin Abdullah

C. Pengalaman Penelitian dalam 5 Tahun Terakhir

(Bukan Skripsi, Tesis, dan Disertasi)

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber*	Jml (Juta Rp)

D. Pengalaman Pengabdian kepada Masarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber*	Jml (Juta Rp)
1	2024	Tim Penilaian Angka Kredit Jabatan Akademik Asisten Ahli dan Lektor sebagai bagian dari Pengabdian Masyarakat		
2	2023	Tim Penilai LLDikti 3 dalam penilaian angka kredit jabatan fungsional New Formasi 1		
3	2022	PENGENALANTEKNOLOGI BLOCKCHAIN DAN PERKEMBANGANNYA BAGI MASA DEPAN		
4	2021	PELATIHAN HIDROPONIK RAKIT APUNG DI ERA PANDEMI COVID-19 SEBAGAI KETAHANAN PANGAN MASYARAKAT		
5	2021	Sosialisasi Paten Aplikasi Online Bagi Inventor Dalam Pengusulan Patent Sederhana dengan Menggunakan Laman 4 Portal Global Sebagai Perlindungan Hak Kekayaan Intelektual di Universitas Esa Unggul Jakarta		

E. Publikasi Artikel Ilmiah dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor/Tahun

1	Utilization of LSTM (Long Short Term Memory) Based Sentiment Analysis for Stock Price Prediction	IJSTM	4(4)/2023
2	Performance Evaluation of Business Continuity Plan in Dealing with Threats and Risks in Cilegon Companies Use ISO 22301: 2019 & NIST Sp 800-30 R1 Frameworks Case Study: PT. X	IJOSH	1(12)/2023
3	Preventing Child Kidnaping at Home Using CCTV that Utilizes Face Recognition with You Only Look Once (YOLO) Algorithm	IJSR	2(9)/2023
4	Prototyping Of Precission Farming Hydroponic Garden Using Arduino Using Design Thinking Method At Puriponic Greenhouse Depok	IJSTM	4(2)/2023
5	Analisis Quality of Service Jaringan Internet pada Bts Perangkat Ericsson Provider Indosat (Studi Kasus: Bts Indosat)	Journal Locus Penelitian dan Pengabdian Proceeding MIMSE 2022	3(6)/2024
6	Mobile Application Based Parking System Control and Monitoring Model with Motor Vehicle Parking		Proceeding MIMSE 2022

F. Pelatihan/ Seminar dalam 5 Tahun Terakhir

No	Nama Pelatihan/Seminar/Sertifikasi	Waktu dan Tempat

G. Karya Buku Dalam 5 Tahun Terakhir

No	Judul Buku	Tahun	Jumlah Halaman	Penerbit

H. Perolehan HaKI dalam 5-10 Tahun Terakhir

No	Judul HaKI	Tahun	Jenis	No. P/ID

I. Pengalaman Merumuskan Kebijakan Publik/Rekayasa Sosial Lainnya dalam 5 Tahun Terakhir

No	Judul	Tahun	Tempat Penerapan	Respon Masyarakat

J. Penghargaan dalam 10 tahun Terakhir (dari pemerintah, asosiasi atau institusi lainnya)

No.	Jenis Penghargaan	Instansi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan penelitian skema dasar hibah internal.

Jakarta, 23-09-2024

Dr. Budi Tjahjono, S.Kom, M.Kom

Biodata Anggota Pengusul

Anggota 1

A. Identitas Diri

1	Nama Lengkap (dengan gelar)	: Dr. Gerry Firmansyah S.T, M.Kom
2	Jenis Kelamin	: Laki-laki
3	Alamat	
4	Jabatan Fungsional	: Lektor
5	NIP/NIK/Identitas Lainnya	: 216040631
6	NIDN	: 0305116804
7	Tempat dan Tanggal Lahir	: Bandung, 5 November 1968
8	Agama	: Islam
7	E-mail	: gerry@esaunggul.ac.id
8	Nomor Telepon/HP	: +62 811 8111 610
9	Alamat Kantor	: Jl. Arjuna Utara no. 9, Kebon Jeruk, Jakbar
10	Nomor Telepon/Faks	: 021 5674223
11	Mata Kuliah yang Diampu	1. IT Infrastruktur Service Manajement
		2. Disaster Recovery Plan
		3. Perancangan Strategis Sistem Informasi

B. Riwayat Pendidikan

	S-1	**S-2**	S-3
Nama Perguruan Tinggi	Institut Teknologi Bandung	Universitas Indonesia	Universitas Indonesia
Bidang Ilmu	Teknik Informatika	Ilmu Komputer	Ilmu Komputer
Tahun Masuk-Lulus	1993-2000	2004-2006	2004-2006
Judul Skripsi/Tesis/Disertasi	Jaringan Komputer Mainframe	Information Economics	Kinerja Dosen
Nama Pembimbing/Promotor	Dr. dr. Oerip	Prof. Aniaty	Prof. Zainal Hasibu

C. Pengalaman Penelitian dalam 5 Tahun Terakhir

(Bukan Skripsi, Tesis, dan Disertasi)

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber*	Jml (Juta Rp)
	2020	E-Learning Issues and Challenges: an Exploratory Study		

D. Pengalaman Pengabdian kepada Masarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber*	Jml (Juta Rp)
1	2019	IMPLEMENTASI TEKNOLOGI SMARTCITY INTERNET OF THINGS (IoT) DALAM MEWUJUDKAN POTENSI MASYARAKAT DI WILAYAH KABUPATEN SUMEDANG JAWA BARAT		
	2019	Pemanfaatan IoT Untuk Menentukan Pemilihan Komunitas Tanaman		

E. Publikasi Artikel Ilmiah dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor/Tahun
1	Sentiment Analysis of 5G Implementation and Its Impact on Technological Developments in Jakarta using the Latent Dirichlet Allocation Mode	Proceeding KNSi	2021
2	Optimization of Delay Using Killer Whale Algorithm (KWA) on NB-IoT	Proceeding MIMSE	2023
3	Risk Management Domain Application Plan Electronic Based Governance System (SPBE) Case Study: Tangerang Government Communications and Informatics Service	Jurnal Minfo Polgan	2023
4	Analysis of Drowsiness Detection based on Images Using Convolutional Neural Network	Jurnal Aston Jadro	2024

F. Pelatihan/ Seminar dalam 5 Tahun Terakhir

No	Nama Pelatihan/Seminar/Sertifikasi	Waktu dan Tempat

G. Karya Buku Dalam 5 Tahun Terakhir

No	Judul Buku	Tahun	Jumlah Halaman	Penerbit

H. Perolehan HaKI dalam 5-10 Tahun Terakhir

No	Judul HaKI	Tahun	Jenis	No. P/ID
1	Sentiment Analysis of 5G Implementation and Its Impact on Technological Developments in Jakarta using the Latent Dirichlet Allocation Mode	2021	Penemuan teknologi	
2	Implementasi Performance Reference Model Dalam Enterprise Architecture Di Sistem Pemerintahan Berbasis Elektronik	2019	Hak Cipta	

I. Pengalaman Merumuskan Kebijakan Publik/Rekayasa Sosial Lainnya dalam 5 Tahun Terakhir

No	Judul	Tahun	Tempat Penerapan	Respon Masyarakat
1	RPerpres e-Government	2015	Kemenpan	

J. Penghargaan dalam 10 tahun Terakhir (dari pemerintah, asosiasi atau institusi lainnya)

No.	Jenis Penghargaan	Instansi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan penelitian skema dasar hibah internal.

Jakarta, 23-09-2024

Dr. Gerry Firmansyah.Kom, M.Kom

Biodata Anggota 2

A. Identitas Diri

1	Nama Lengkap (dengan gelar)	: Habibullah Akbar, S.Si, M.Sc, Ph.D
2	Jenis Kelamin	: Laki-laki
3	Alamat	:
4	Jabatan Fungsional	: Lektor
5	NIP/NIK/Identitas Lainnya	: 218030726
6	NIDN	: 0315108201
7	Tempat dan Tanggal Lahir	: Jakarta 15 Oktober 1982
8	Agama	: Islam
7	E-mail	: habibullah.akbar@esaunggul.ac.id
8	Nomor Telepon/HP	: 081319110259
9	Alamat Kantor	: Jl. Arjuna Utara no. 9, Kebon Jeruk, Jakbar
10	Nomor Telepon/Faks	: 021 5674223
11	Mata Kuliah yang Diampu	1. Topik dalam *Artificial Intelligence*
		2. Topik dalam *Image Processing*
		3. Topik dalam *Data Mining*
		4. Pemrograman Mobile

B. Riwayat Pendidikan

	S-1	**S-2**	S-3
Nama Perguruan Tinggi	ITB	UTeM	UTeM
Bidang Ilmu	Fisika	Teknologi Informasi dan Komunikasi	Teknologi Informasi dan Komunikasi
Tahun Masuk-Lulus	2002-2006	2008-2010	2010-2016
Judul Skripsi/Tesis/Disertasi	Study dari Pengaruh Medan Magnet Ring terhadap Film Tipis CoFe pada Reaktor Opposed Target Magnetron Sputtering	Defect Inspection Algorithm in Intelligent Real-Time Vision System for Small and Medium Industries	3D Intrinsic Scene Characteristic Extraction Framework for a Single Image
Nama Pembimbing/Promotor	Prof. Dr Mitra Djamal	Prof. Dr Nanna Suryana Herman	Prof. Dr Nanna Suryana Herman Prof. Dr Shahrin Sahib

C. Pengalaman Penelitian dalam 5 Tahun Terakhir

(Bukan Skripsi, Tesis, dan Disertasi)

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber*	Jml (Juta Rp)
1	2022	SISTEM DETEKSI BANJIR DI AREA PERKOTAAN		

		MENGGUNAKAN JARINGAN KONVOLUSI U-NETS		
2	2021	Implementasi Service Oriented Architecture (SOA) Sistem Monitoring Seleksi Penerimaan Beasiswa		
3	2020	Pengembangan e-Mental Health Berbasis Knowledge Management dalam Mendukung Sistem Informasi Kesehatan Nasional (SIKNAS)		

D. Pengalaman Pengabdian kepada Masarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber*	Jml (Juta Rp)
1	2022	Pelatihan Pembuatan Video Pembelajaran Berbasis Multimedia dengan Metode Community Based Participatory Action Research (CBPAR)		

E. Publikasi Artikel Ilmiah dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor/Tahun
1	KLASIFIKASI KANKER SERVIKS MENGGUNAKAN MODEL CONVOLUTIONAL NEURAL NETWORK ALEXNET	JIKO (Jurnal Informatika dan Komputer)	4(1)/April 2021
2	An Application design thinking in the internal quality audit system	JISAMAR Komputasi	6(1)/Pebruari 2022
3	Aplikasi DonasiKu Berbasis Android	Jurnal Dan Penelitian Teknik Informatika	10(1)/2022
4	Optimization of Delay Using Killer Whale Algorithm (KWA) on NB-IoT		7(4)2023
5	PENGEMBANGAN APLIKASI MENTALFIRST BERBASIS ANDROID SEBAGAI MEDIA DETEKSI AWAL PTSD DAN MEDIA INFORMASI SEPUTAR PTSD	SIMETRIS	14(1)/Mei 2023
6		Aston Jadro	13(2) Mei 2024

	Analysis of Drowsiness Detection based on Images Using Convolutional Neural Network		

F. Pelatihan/ Seminar dalam 5 Tahun Terakhir

No	Nama Pelatihan/Seminar/Sertifikasi	Waktu dan Tempat

G. Karya Buku Dalam 5 Tahun Terakhir

No	Judul Buku	Tahun	Jumlah Halaman	Penerbit

H. Perolehan HaKI dalam 5-10 Tahun Terakhir

No	Judul HaKI	Tahun	Jenis	No. P/ID

I. Pengalaman Merumuskan Kebijakan Publik/Rekayasa Sosial Lainnya dalam 5 Tahun Terakhir

No	Judul	Tahun	Tempat Penerapan	Respon Masyarakat

J. Penghargaan dalam 10 tahun Terakhir (dari pemerintah, asosiasi atau institusi lainnya)

No.	Jenis Penghargaan	Instansi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan penelitian skema dasar hibah internal.

Jakarta, 23-09-2024

Habibullah Akbar, S.Si, M.Sc, Ph. D

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v9i1.4080

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

RISK MANAGEMENT OF INFORMATION SYSTEM IN DISKOMINFO STATISTIC AND ENCODING USING NIST SP 800-30

Budi Tjahjono[1*]; Miri Ardiansyah[2]; Gerry Firmansyah[3]; Habibullah Akbar[4]

Master of Computer Science[1,2,3,4]
Universitas Esa Unggul
www.esaunggul.ac.id
budi.tjahjono@esaunggul.ac.id[1], miriardiansyah805@student.esaunggul.ac.id[2], gerry@esaunggul.ac.id[3], habibullah.akbar@esaunggul.ac.id[4]

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract— E-Government is a form of government service in digital form that utilizes the internet network which makes government services to the community easy. However, behind the perceived convenience, of course, there will be risks that arise, for example data loss, data theft, mis-access, illegal access, hardware damage, hacking, etc. which will have a negative impact on an organization, including in the Statistics and Encryption Communication and Information Service, XYZ Regency. The most commonly found threats are those that come from humans and electricity. In addition, there are still many sources of threats that have the potential to pose risks that will interfere with the implementation of electronic-based government. From the results of risk measurements that have been carried out based on NIST SP 800-30 By multiplying between the levels determined in the likelihood and impact processes to produce a number to be used as a guide in determining the level of risk, it was found that the risk threats originating from humans are 60% risk with Low level, 30% risk with Medium level, and 10% risk with High level. While the risk derived from electricity was 20% risk with Low level, 20% risk with Medium level, and 60% risk with High level. Lastly sourced from Technical is 34% risk with Low level, 33% Medium level risk, and 33% High level risk. Overall the risk assessment results were 39% risk threats with Low level, 33% risk threat with Medium level, and 28% risk threat with High level.

Keywords*: E-Government, Diskominfo of XYZ District, Risk Management, NIST SP 800-30.*

Abstract— *E-Government* merupakan bentuk pelayanan pemerintah dalam bentuk digital yang memanfaatkan jaringan *internet* yang membuat pelayanan pemerintah kepada masayrakat menjadi mudah. Namun dibalik kemudahan yang dirasakan tentunya akan ada risiko yang muncul misalnya kehilangan data, pencurian data, salah akses, akses illegal, kerusakan *hardware*, peretasan, dll yang akan menimbulkan dampak negatif bagi suatu organisasi tidak terkecuali di Dinas Kominfo Statistik dan Persandian Kab. XYZ. Ancaman yang paling sering ditemukan adalah ancaman yang bersumber dari manusia dan listrik. Selain itu juga masih banyak sumber-sumber ancaman yang berpotensi menimbulkan risiko yang akan mengganggu penyelenggaraan pemerintahan berbasis elektronik. Dari hasil pengukuran risiko yang sudah dilakukan berdasarkan NIST SP 800-30 dengan melakukan perkalian antara level-level yang ditetapkan pada proses *likelihood* dan *impact* sehingga menghasilkan angka untuk dijadikan pedoman dalam menetapkan level risiko, didapatkan hasil bahwa ancaman risiko yang bersumber dari manusia adalah 60% risiko dengan tingkat *Low*, 30% risiko dengan tingkat *Medium*, dan 10% risiko dengan tingkat *High*. Sedangkan risiko yang bersumber dari listrik adalah 20% risiko dengan tingkat *Low*, 20% risiko dengan tingkat *Medium*, dan 60% risiko dengan tingkat *High*. Dan terakhir yang bersumber dari Teknis adalah 34% risiko dengan tingkat *Low*, 33% risiko tingkat *Medium*, dan 33% risiko tingkat *High*. Secara keseluruhan hasil penilaian risiko adalah 39% ancaman risiko dengan tingkat *Low*, 33% ancaman risiko dengan tingkat *Medium*, dan 28% ancaman risiko dengan tingkat *High*.

Keywords*: E-Government, Diskominfo Kab. XYZ, Manajemen Risiko, NIST SP 800-30*

INTRODUCTION

E-Government is a form of government service in digital form that utilizes the internet network which aims to make government services to the community easy. However, behind the ease of being felt, of course, there will be risks that arise, for example data loss, data theft, mis-access, illegal

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

access, hardware damage, hacking, etc. which will otherwise have a negative impact on an organization, including the Department of Communication and Information Statistics and Encoding of XYZ Regency which supervises applications in the Regional Device Organization (OPD) of XYZ Regency in running and maximizing its government services. However, the problem that arises is that there are several types of threats that exist in the application implementation in XYZ Regency. The most commonly found threats are those that come from humans and electricity. Apart from the two sources of threats described above, of course, there will be many other sources of threats that can occur and can pose risks that will interfere with the running of government services.

Risk is a state of uncertainty over the level of probability. Risk is closely related to unpleasant things, so it is very important to continue to be careful in all aspects with the right calculations [1]. Risk can be considered as a possible obstacle that has the potential to have a negative impact on the goals to be achieved [2]. Risks cannot be allowed to appear so casually that they have a negative impact. Risk can be controlled by doing risk management [3].

Risk management is defined as the implementation of internal management functions dealing with various kinds of uncertain situations that will be faced company, which includes the function of planning, organizing, implementing, supervising, and evaluating risk management programs [4]. Risk is an integral part of business and inherent in company activities [5]. The aim of risk management is to create level protection Which mitigate vulnerability to threats and potential consequences, thus reducing the risk to acceptable level [6].

There are many methods that can be used to perform information security risk management such as Octave, NIST SP 800-30 and ISO 27001 [7]. However, in this study, the method that will be used in carrying out risk management is NIST SP 800-30 (National Institute Of Standarts and Technology SP 800-30). NIST (National Institute of Standard Technology) is a non-regulatory federal agency in the United States that has a mission to develop and promote measurements, standards and technology to increase productivity and improve the quality of human life[8].

The reason for choosing NIST SP 800-30 is based on previous research, namely research conducted by [7] that NIST SP 800-30 has been shown to make more contributions such as: providing consistent and comprehensive information security insights for policymakers, structured resource modeling, information security insights acceptable to various risk takers, threat determination can be identified easily, decision makers do not hesitate to take risks because each risk has been properly investigated. NIST SP 800-30 is the best of 3 methods for risk analysis, namely Mehari, Magerit and Microsoft's Security Management Guide, especially when conducting risk analysis, NIST SP 800-30 provides control recommendations.

The stages of risk management using NIST are divided into three stages, namely :

1. Risk Assesment
   Organizations use risk assessment to define potential threats and risks related to the use of information technology. The output of this process is expected help identify how controls to perform reductions and omissions risks during the mitigation process. This process consists of 9 (nine) steps in the risk assessment activities [9].
2. Risk Mitigation
   Risk mitigation Is the second stage of the risk management process issued by NIST, mitigation or reduction risk is a systemic methodology used by management to reduce the impact of risk [10].
3. Risk Evaluation
   The evaluation stage is the stage where an assessment of the implementation is carried out risk control. For example every year this is done to reassess whether the tool or method of risk reduction still relevant [11].

in this study will focus more on the risk assessment stage.

MATERIALS AND METHODS

A. Research Methodology

The stages of research that will be carried out consist of 4 (four) systematic stages can be seen in figure 1 below.

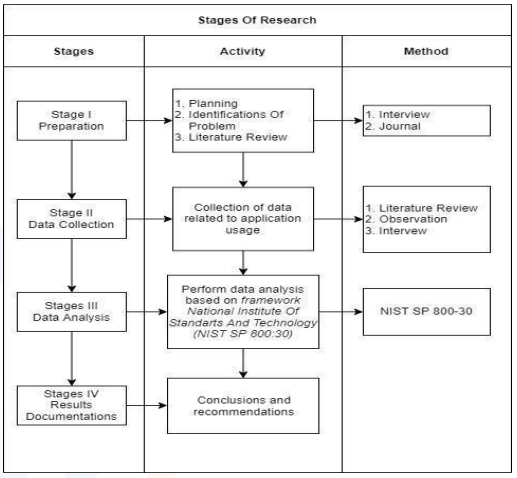


Figure 1. Stages of Research

The stages from beginning to end that will be carried out in this study are as follows :

1. Preparation

The preparation stage includes Designing, Problem Identification, and Literature Study. While the method used is an interview to find out if there has ever been a problem in the use of the application in the Regency, then what problems occur most often, the source of the problem that occurs, what control is carried out on the problem that occurs.

2. Data Collection

Data collection is carried out to obtain data related to the research carried out. The methods used in this data collection are literature studies, observations and interviews. Observation is a form of observation or direct sensing of something object, condition, situation, process or behavior [12]. Interviews is a technique data collection is done through face-to-face and direct Q&A between collectors sources/data sources [13]. Interviews at the data collection stage were conducted to obtain data that will be used for the analysis process in accordance with the NIST SP 800-30 method.

3. Analysis Stage

The third stage is to analyze the data that has been obtained in the previous process using the NIST SP 800-30 framework. Analysis is a way of finding and processing data properly (systematically) good record of the results of interviews, observations, and others in order to increase knowledge researcher of the research problem under study and its presentation as subsequent findings [14].

4. Documentation / Conclusions and Suggestions

The last stage is carried out documentation of the report of conclusions and suggestions in the form of a final project in accordance with the applicable format.

B. Data Analysis with NIST SP 800-30

At the Analysis stage, the framework NIST SP 800-30 is used.

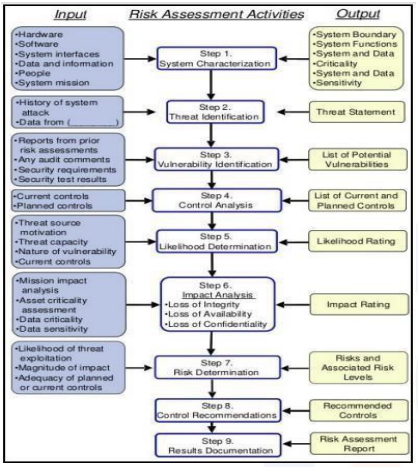


Figure 2. NIST SP 800-30 Risk Assessment Activities [15]

The following is an explanation of the stages / risk assessment activities as well as the inputs and outputs of each stage in NIST SP 800-30 [15] :

1. System Characterization

Assessing the characteristics of the system, see the point of view of hardware, software interface, data and information, to the purpose of the system. This point of view will be the input of the process, so that it will produce outputs, namely system limitations, system functionality, data and sensitivity levels, users and others.

2. Threat Identification

Recognizing various threats and sources that will be a disruption to the system / recognize the sources of threats on the system. The input of this process is a report of a problem or attack that has occurred. While the output of this process is a threat statement, which is a set of risks that may occur as well as a source of risk that can cause vulnerabilities in the system.

3. Vulnerability Assessment

At this stage, various vulnerabilities are identified that allow threats to occur to the system. The inputs at this stage are reports or outputs from previous risk assessments. While the output produced is a list of vulnerabilities that exist in the system.

4. Control Analysis

The main objective of this stage is to analyze the controls that have been implemented or that will be applied, in order to minimize the possibility of a threat. The inputs from this stage are the controls that have been implemented in each risk/vulnerability, while the output is a list of controls on the risks that are being implemented and the control plan that will be applied to possible risks.

5. Likelihood Determination

This stage is used to obtain a value of the possible tendency to weakness of the system. The inputs of this stage are the source of risk and the motivation of the cause of the source of risk, and vulnerability. While the output of this stage is the level / level of the possibility of risk threat occurrence.

6. Impact Analysis

Assessing the impact that occurs on attacks on weak parts of a system. The input of this system is the mission of the system and the level of data sensitivity or in other words how the risk will affect the system and the data being processed. Possible considerations are issues of data integrity,

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

availability of services and loss of trust. The output of this system is the magnitude of impact definition.

7. Risk Determination

Risk determination aims to assess the level of risk to the system, to assess the level of risk this refers to the possible risks and impacts of risks that have been determined. Inputs from this stage are the possibility of a threat, the magnitude of the impact of the threat, the effectiveness of controls that have already been implemented or newly planned. While the output is the risk and the level of associated risk.

8. Control Recommendation

The goal of this stage is to reduce the level of risk in the IT system so that it reaches an acceptable level. The input is the output of the previous stage i.e. risk and risk level, from here a list of control recommendations will be generated.

9. Result Document

It is a result of the activities carried out.

RESULTS AND DISCUSSION

At this stage, risk analysis / measurement is carried out at the Statistical and Encryption Information Communication Service of XYZ Regency based on data obtained using the National Institute Of Standards And Technology framework. The processes are as follows :

A. System Characterization

The information system application in XYZ Regency under the auspices of the Statistical and Encryption Information Communication Service of XYZ Regency is a website-based and online-based application. The hardware resource is a Personal Computer (PC) which is used to operate information system applications with the windows 10 operating system. Meanwhile, the data and information managed by the applications in the district are District Documents, Statistical Data, Community data, and other important data. Human resources are operators of information system applications. These applications are based online and operated via PC. Therefore, the use of the application is very dependent on electricity and internet resources patent in its use.

B. Threat Identification

Based on the results of interviews that have been conducted with two speakers at Statistical and Encryption Information Communication Service of XYZ Regency The interview was conducted with two people, namely Mr. Ayubi Khaafidh as the head of the technical team / local it supports and Mr. Indra Asura as the team that manages and controls the use of SPBE / E-Government as well as the general operator of SPBE Statistical and Encryption Information Communication Service, the threat data can be seen in table 1 below :

Table 1. Threat Identification

Source	Motivation	Threat	Code
Human	Human Error	Forgot Password / Username	A001
		Data Leakage by Internal	A002
		Application Crash	A003
		Access Errors	A004
		Misuse of Access Rights	A005
		Data Deleted	A006
		Forgot the way /flow of using the app	A007
	Ego	Former Employee Rogue	A008
		Hacker / Cracker	A009
		Internal Rogue	A010
		Hardware Damage / PC Damage	A011
Elctricity	Electrical	Burnt Hardware	A012
	Network Damage	Lost Data/Corrupt Data	A013
		Lost Internet Signal	A014
Technical	Virus	Unusable Application	A015
		Loss of important data/assets	A016
		Software cannot be accessed	A017
		Lost or damaged data - important	A018

data

C. Vulnerability Identification

Based on the interviews conducted, it was found that the system vulnerabilities in Statistical and Encryption Information Communication Service of XYZ Regency are shown in table 2 below :

Table 2. Vulnerability Identification

Code	Gaps / Insecurity
A001	High Turn Over so as to cause frequent changes of operators / Poorly trained operators
A002	Unavailability of Cooperation Agreement containing responsibility to OPD application operators
A003	Granting Full Access Rights To HR who do not fully understand the application being used.
A004	Lack of HR Training,
A005	Operator Does Not Logout / Exit after using the application.
A006	Lack of trained human resources,
A007	High Turn Over causing frequent operator changes
A008	OPD did not confirm the release of the application operator. So that the technical team does not freeze the operator's access rights / still have access.
A009	There is no special team responsible for system security.
A010	Unavailability of a Cooperation Agreement containing responsibility for OPD application operators
A011	Hardware Damage / PC Damage

Code	Gaps / Insecurity
A012	Burnt Hardware
A013	Lost Data/Corrupt Data
A014	Lost Internet Signal
A015	Unusable Application
A016	Irregular use of Flashdisk
A017	Improper use of anti-virus
A018	Downloading and installing apps carelessly

D. Control Analysis

Based on the results of the interview that has been conducted, the results are obtained in the form of control are shown in table 3 below :

Table 3. Control Analysis

Code	Control
A001, A004, A007	Coordinating and re-explaining things that are not yet known or forgotten to the relevant operator.
A002, A003, A005, A006,	Coordinating related to data sensitivity and the importance of data security and responsibility for data security by operators.
A008, A010, A009	Socialization / coordination with employees and leaders related to strengthening system security.
A011, A012, A014, A015	Socialization / coordination with employees / leaders of related OPDs related to prevention. e.g. using a UPS.
A013	Socialization to operators so that they can often save files that have been created / edited so that they are not lost or corrupted. As well as backing up important files.
A016, A017, A018	Coordinating and socializing with operators related to data sensitivity, in order to install anti-virus, orderly use of flasdisks, and virus danger to data and sources of viruses.

E. Likelihood Determination

At this stage, the possibility of a risk from the existing threat is sought. The determination of possibilities is divided into three types, namely High, which includes threat sources that have high motivation, with open loopholes and controls to prevent ineffective loopholes, medium, namely threat sources have sufficient motivation and there are gaps that can be passed but there are controls that are carried out that are likely to minimize loopholes and threats, while Low is a source of threat that lacks motivation and there are controls that are useful for preventing or blocking gaps for threats can occur. The level of possible risk of each threat is are shown in table 4:

Table 4. Likelihood Determination

Code	Threat
A001	*Medium*
A002	*High*
A003	*Low*
A004	*Low*
A005	*Low*
A006	*Medium*
A007	*Medium*
A008	*Medium*
A009	*Low*
A010	*Low*
A011	*High*
A012	*High*
A013	*High*
A014	*High*
A015	*Medium*
A016	*High*
A017	*Low*
A018	*Medium*

F. Impact Analysis

Impact Analysis is a stage of measuring or analyzing the influence of existing risk threats. In determining the impact, it also consists of three parts, namely Low, Medium, High. Low is the effect that occurs caused by the risk of lowering the reputation of the organization. Medium is the effect that is felt not only can damage the reputation but also damage to some equipment / hardware and can cause financial losses. While high, the effect felt or produced can damage the reputation of the organization at a high level because it can eliminate public trust in the organization, can damage some parts of the hardware so that it can cause high financial losses, even to the point of being life-threatening or causing death. the levels of impact generated by the risk threat can be seen in table 5 below :

Table 5. Impact Analysis

Code	Impact Analysis
A001	*Low*
A002	*High*
A003	*Low*
A004	*Low*
A005	*Medium*
A006	*High*
A007	*Medium*
A008	*High*
A009	*High*
A010	*Medium*
A011	*High*
A012	*High*
A013	*High*
A014	*Medium*
A015	*Low*
A016	*High*
A017	*Medium*
A018	*High*

G. Risk Determination

This stage aims to assess the level of risk faced in the use of information system applications in Statistical and Encryption Information Communication Service of XYZ Regency. This risk assessment is obtained by multiplying between the levels set in the Likelihood Identification process with impact analysis as shown in the following formula :

Risk Assessment = Impact x Likelihood

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)
VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

To determine or assess risk, a matrix is used as in the Table 6 as a reference for calculations. This matrix shows what the overall level of risk is. The range of numbers in determining this risk assessment is 1 to 10 Low risk levels, more than 10 to 50 Medium risk levels, while more than 50 to 100 High risk levels.

Table 6. Risk Level Matrix [16]

Thread Likelihood	Impact		
	Low (10)	Medium (50)	High (1oo)
High (1.0)	Low 10x1.0=10	Medium 50x1.0=50	High 100x1.0 = 100
Medium(0.5)	Low 10x0.5=5	Medium 50x0.5=25	Medium 100x0.5 = 50
Low (0.1)	Low 10x0.1=1	Low 50x0.1=5	Low 100x0.1 = 10

Furthermore, Based on the table 6, the process of calculating and assessing risks can be seen in the table 7 below :

Table 7. Risk Determination

Code	Likelihood Determination	Impact Analysis	Likeli x Impact
A001	*Medium (0.5)*	*Low (10)*	0.5 x 50 = 5 (*Low*)
A002	*High (1.0)*	*High (100)*	1.0 x 100 =100 (*High*)
A003	*Low (0.1)*	*Low (10)*	0.1 x 10 = 1 (*Low*)
A004	*Low (0.1)*	*Low (10)*	0.1 x 10 = 1 (*Low*)
A005	*Low (0.1)*	*Medium (50)*	0.1 x 50 = 5 (*Low*)
A006	*Medium (0.5)*	*High (100)*	0.5 x 100 =50 (*Medium*)
A007	*Medium (0.5)*	*Medium (50)*	0.5 x 50 = 25 (*Medium*)
A008	*Medium (0.5)*	*High (100)*	0.5 x 100 =50 (*Medium*)
A009	*Low (0.1)*	*High (100)*	0.1 x 100 =10 (*Low*)
A010	*Low (0.1)*	*Medium (50)*	0.1 x 50 = 5 (*Low*)
A011	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A012	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A013	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A014	*High (1.0)*	*Medium (50)*	1.0 x 50 = 50 (*Medium*)
A015	*Medium (0.5)*	*Low (10)*	0.5 x 10 = 5 (*Low*)
A016	*High (1.0)*	*High (100)*	1.0 x 100 = 100 (*High*)
A017	*Low (0.1)*	*Medium (50)*	0.1 x 50 = 5 (*Low*)
A018	*Medium (0.5)*	*High (100)*	0.5 x 100 = 50 (*Medium*)

(Calculation based on table 5 and 6)

based on the results of the calculation in table 7 above, risks sourced from humans have not been found risks with High, or Medium levels. Based on the calculations in table 7, the level of risk originating from humans is 6 risks with Low risk levels, 3 risks with Medium risk levels, and 1 risk with High risk levels. The graph can be seen in figure 3 below.

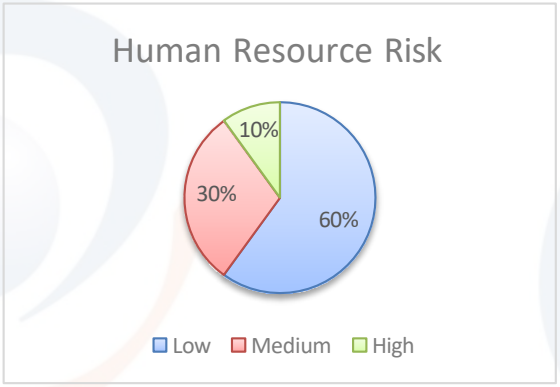


Figure 3. Human Resource Risk

Meanwhile, the risks derived from electricity based on the calculations made table 7 are 1 risk with a Low level, 1 risk with a Medium risk level, and 3 risks with a High level. In figure 4 below a look at the graph of the level of risk sourced from Electricity.

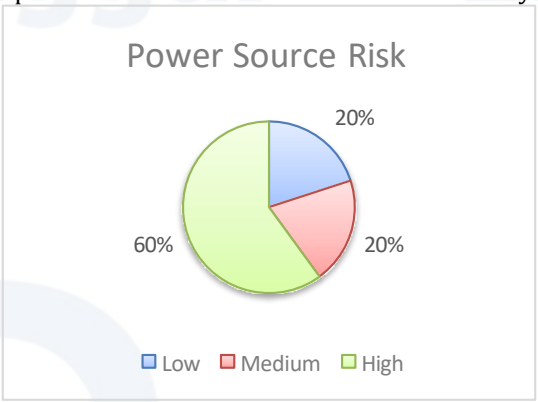


Figure 4. Power Source Risk

Meanwhile, risks derived from Technical sources (Viruses) based on calculations in the table 7 obtained results of 1 risk with a Low risk level, 1 Medium level risk, and 1 High level risk. The graph can be seen in figure 5 below.

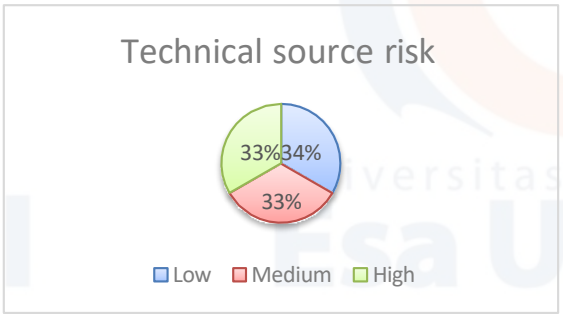


Figure 5. Technical source risks

Overall, the risk assessment chart based on the calculations in the table 7 is obtained 8 risks with Low risk levels, 5 risks with Medium risk levels, and 5 risks with High levels. In the figure 6 below is a graph that is the overall result of calculating or measuring risks in the Statistical and Encryption Information Communication Service of XYZ Regency.

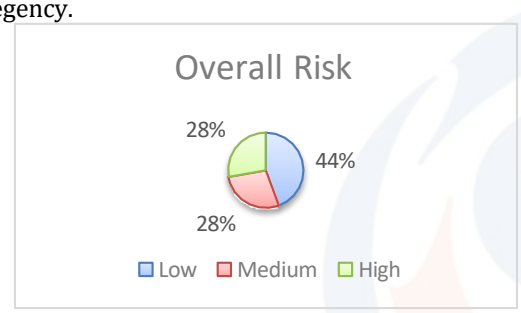


Figure 6. Overall Risk

Based on the source of risk can be seen in figure 7 below.

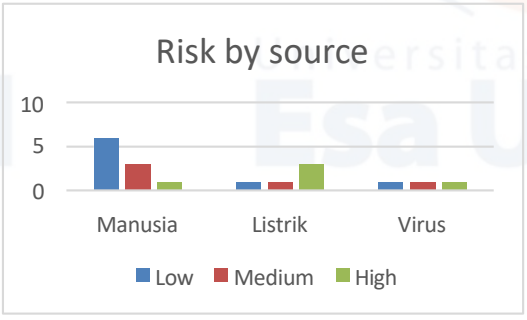


Figure 7. Risk by Source

H. Control Recommendation

Control Recommendation is the stage of providing control recommendations from researcher to eliminate or minimize risk. For recommendations given on each type of risk can be seen in table 8 below.

Table 8. Control Recommendation

Code	Risk Level	Control Recommendation
A001	*Low*	1. Giving operators a username and password that is easy to remember. 2. Providing the operator with a specific account note and require the relevant operator to keep and maintain the record so that when forgotten they can reopen the record. 3. The technical team creates and stores a document containing a list of accounts used by the operator of each OPD as a backup to quickly respond to risk mitigation.
A002	*High*	1. Creating an employment agreement related to the obligation to be responsible for the security and integrity of data managed by the operator. 2. Conducting socialization related to the level of data sensitivity and the importance of data or document security.
A003	*Low*	Creating SOPs related to the granting of operator Access Rights types by the technical team.
A004	*Low*	Conducting socialization / training and creating documents containing explanations of the character of each application, the sensitivity of the data being managed, as well as complete instructions on using the application.
A005	*Low*	Creating and pasting SOPs related to the use of applications at the operator's workplace
A006	*Medium*	Conducting socialization / training and creating documents containing explanations of the character of each application, the sensitivity of the data being managed, as well as complete instructions on using the application.
A007	*Medium*	Conducting socialization / training and creating documents containing explanations of the character of each application, the sensitivity of the data being managed, as well as complete instructions on using the application.
A008	*Medium*	1. Creating an employment agreement related to the obligation to be responsible for the security and integrity of data managed by the operator. 2. Coordinating and requiring each OPD to always confirm the entry and exit of the operator to the technical team so that the technical team can act to freeze accounts owned or known by the former employee in question.
A009	*Low*	Establishing a special team responsible for information system security in order to focus on preventing outside attacks
A010	*Low*	Creating an employment agreement related to the obligation to be responsible for the security and integrity of data managed by the operator.

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 9. NO. 1 AUGUST 2023
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i1.4080

Code	Risk Level	Control Recommendation
A011	*High*	1. Providing an Uninteruptible Power Supply (UPS) so that the PC does not turn off suddenly when the power goes out in order to save the documents that are done so that files are not lost / corrupted. Then in order to be able to turn off the PC normally. 2. Providing a generator / generator as a backup power source.
A012	*High*	
A013	*High*	
A014	*Medium*	
A015	*Low*	
A016	*High*	1. Always install and maintain anti-virus. 2. Downloading apps from trusted sources. 3. Using an officially licensed application. 4. Always back up important data.
A017	*Low*	
A018	*Medium*	

CONCLUSION

Based on the discussion that has been discussed in the previous chapter, the conclusions that can be drawn from the results of this study are as follows : The risk threats that exist in the use of the XYZ Regency information system application managed or shaded by the XYZ Regency Statistical and Encryption Informatics Communication Service that are detected come from three sources, namely 10 risk threats sourced from humans, 5 risk threats sourced from electricity, and 3 risk threats sourced from technical, with a total of 18 risk threats. From the results of risk measurements that have been carried out based on NIST 800-30, it is found that the risk threats originating from humans are 60% risk with Low level, 30% risk with Medium level, and 10% risk with High level. While the risk derived from electricity is 20% risk with Low level, 20% risk with Medium level, and 60% risk with High level. And lastly sourced from Technical is 34% risk with Low level, 33% Medium level risk, and 33% High level risk. Overall risk assessment results are 39% risk threats with Low level, 33% risk threat with Medium level, and 28% risk threat with High level. From the results of measurements made for the high-risk level, the most comes from electricity sources, the medium level comes the most from humans, while for the low risk threat level, the most also comes from humans. Based on the analysis that has been carried out, it is concluded that the risk threats that arise in accordance with the results of interviews conducted in general are caused by the immature system that is run related to the use of applications in government.

REFERENCE

[1] O. Arifudin, U. Wahrudin, and F. D. Rusmana, *Manajemen Risiko*. 2020.

[2] I. B. Indonesia, *Manajemen Risiko 1*. 2015.

[3] P. Y.A.P, *Manajemen Risiko Perusahaan*. 2017.

[4] F. H. Hotdiana, A. Ahmad Yani, M. Putri, P. Syari, and F. Ekonomi Dan Bisnis Islam, "Analisis Risiko Bisnis," *J. Visions Ideas*, vol. 2, no. 2, pp. 119–125, 2022.

[5] Muhammad Asir, R. A. Yuniawati, K. Mere, K. Sukardi, and M. A. Anwar, "Peran manajemen risiko dalam meningkatkan kinerja perusahaan: studi manajemen sumber daya manusia," *Entrep. Bisnis Manaj. Akunt.*, vol. 4, no. 1, pp. 32–42, 2023, doi: 10.37631/ebisma.v4i1.844.

[6] W. Muka and M. A. Wibowo, "Penerapan Manajemen Risiko pada Proses Pengembangan Properti," *J. Permukim.*, vol. 16, no. 1, p. 31, 2021, doi: 10.31815/jp.2021.16.31-40.

[7] A. Elanda and R. L. Buana, "Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus: STMIK Rosma)," *Elkom J. Elektron. dan Komput.*, 2021, [Online]. Available: https://journal.stekom.ac.id/index.php/elkom/article/view/387

[8] N. fitrianti Fahrudin, A. Nugraha S, and K. Ramadhan Putra, "Penilaian Risiko Keamanan Data Karyawan Pada Sistem Informasi Dengan Menggunakan Framework Nist Sp 800-30 pada PT. ABC," *J. Ilm. Teknol. Infomasi Terap.*, vol. 8, no. 3, 2022, doi: 10.33197/jitter.vol8.iss3.2022.900.

[9] D. S. Valena, rizky prabowo, anie rose irawati, and aristoteles aristoteles, "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode Nist Sp 800-30," *J. Komputasi*, vol. 7, no. 1, 2019, doi: 10.23960/komputasi.v7i1.2053.

[10] D. I. Izatri, N. I. Rohmah, and R. S. Dewi, "Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 50, 2020, doi: 10.30865/jurikom.v7i1.1756.

[11] A. N. SUSANTO and N. F. FAHRUDIN, "Penilaian Risiko Sistem Informasi Keamanan Data Karyawan Dengan Menggunakan Framework Nist Sp 800-30 pada Perusahaan XYZ Institut Teknologi Nasional Bandung," *Pros. Disem. FTI Ganjil 2021/2022*, 2022.

[12] Z. Yusra, R. Zulkarnain, and S. Sofino, "Pengelolaan Lkp Pada Masa Pendmik

Covid-19," *J. Lifelong Learn.*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.33369/joll.4.1.15-22.

[13] E. Trivaika and M. A. Senubekti, "Perancangan Aplikasi Pengelola Keuangan Pribadi Berbasis Android," *Nuansa Inform.*, vol. 16, no. 1, pp. 33–40, 2022, doi: 10.25134/nuansa.v16i1.4670.

[14] Ahmad and Muslimah, "Memahami Teknik Pengolahan dan Analisis Data Kualitatif," *Proceedings*, vol. 1, no. 1, pp. 173–186, 2021.

[15] K. Harsanto and D. Hidayat, "Sistem Informasi Manajemen Risiko dengan Menggunakan Framework National Institute of Standards and Technology pada Lembaga Pendidikan," *J. Ipsikom*, vol. 6, no. 1, 2018.

[16] B. A. Nugraha, A. R. Perdanakusuma, and ..., "Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika ...," *... Teknol. Inf. dan ...*, 2020, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6884

Accredited Rank 2 (Sinta 2) based on the Decree of the Directorate General of Higher Education, Research and Technology. Ministry of Education, Culture, Research and Technology of the Republic of Indonesia No.225/E/KPT/2022, 07 December 2022. Published by LPPM Universitas Nusa Mandiri

PERNYATAAN ORISINALITAS

Penelitian ini adalah hasil karya kami, dan semua sumber baik dikutip maupun dirujuk telah saya nyatakan dengan benar

Nama Ketua Peneliti : Budi Tjahjono

NIDN/NIK : 0330126703/205040315

Tanda tangan

30 Oktober 2024

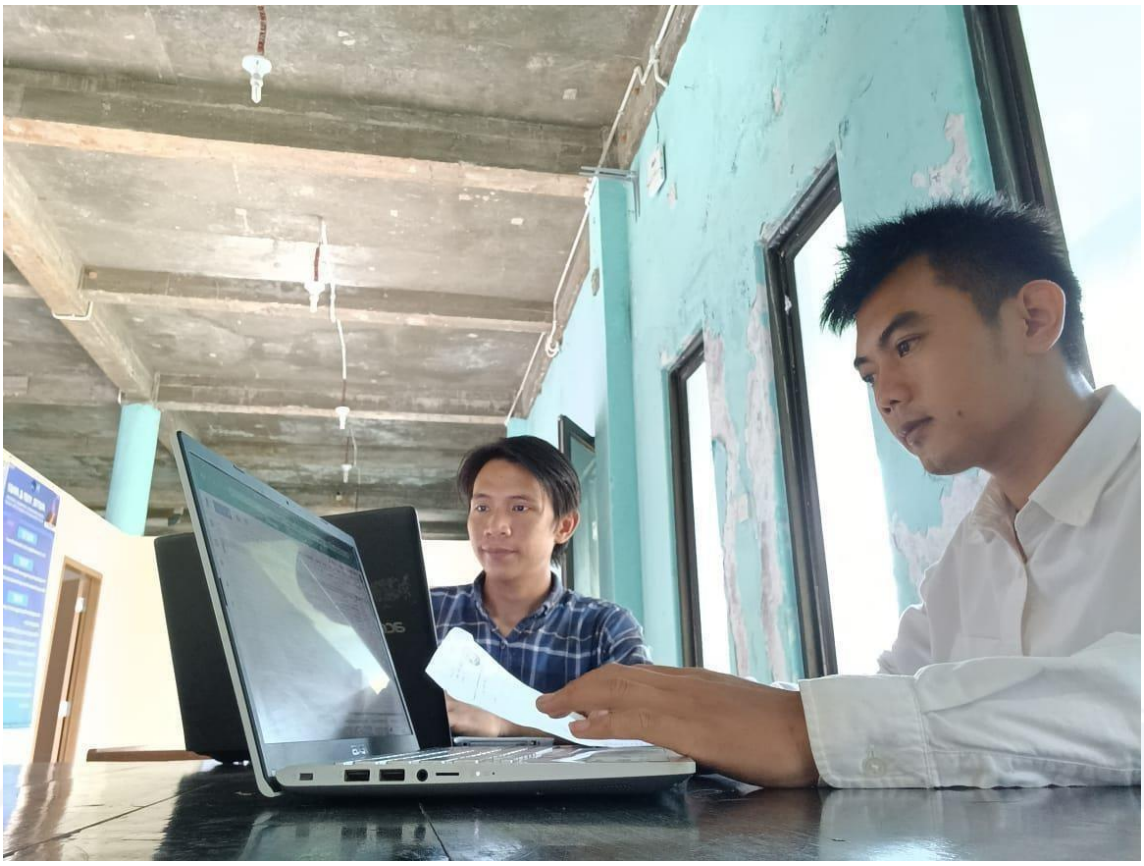
INTERVIEW DENGAN PAK AYUBI KAAFIDH

Tempat : Diskominfo

Kab. XYZ Hari : Selasa 31

Januari 2023

Waktu : 09.20 – 10.12



INTERVIEW DENGAN PAK AYUBI KAAFIDH

Tempat : Badan Pusat Statistik Kab. XYZ Hari : Rabu 02 Februari 2023

Waktu : 21.07 – 21.53