Terbit *online* pada laman : https://teknosi.fti.unand.ac.id/

Jurnal Nasional Teknologi dan Sistem Informasi

| ISSN (Print) 2460-3465 | ISSN (Online) 2476-8812 |

Studi Kasus

Manajemen Risiko Sistem Informasi Pengarsipan menggunakan NIST SP 800-30 pada Kopertis Wilayah IV Bandung

Adi Arga Arifnur [a,*], *Hery Heryanto* [b], *Yoga Megasyah* [c]

[a*] *Departemen Sistem Informasi, Universitas Andalas, Kampus Limau Manis, Padang 25163, Indonesia*
[b] *Jurusan Sistem Informasi, Institut Teknologi Harapan Bangsa, Coblong, Bandung 40132, Indonesia*
[c] *Jurusan Teknik Informatika, Universitas Nasional Pasim, Cicendo, Bandung 40175, Indonesia*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 23 Juni 2023
Revisi Akhir: 06 September 2023
Diterbitkan *Online*: 16 September 2023

KATA KUNCI

Sistem Informasi Pengarsipan,

Penilaian Risiko Network Mapper,

Mitigasi Risiko

KORESPONDENSI

E-mail: adiargaarifnur@gmail.com*

A B S T R A C T

Seiring perkembangan Teknologi informasi, kebutuhan keamanan sistem untuk layanan koordinator pendidikan di Perguruan Tinggi Swasta semakin tinggi. Hal ini dikarenakan banyaknya kasus penyerangan yang terjadi belakangan ini terutama terhadap sistem berbasis Web. *surat.kopertis4.or.id* adalah salah satu sistem informasi (SI) berbasis web yang digunakan oleh beberapa pegawai Kopertis IV Bandung untuk mengarsipkan surat berhubungan dengan kegiatan pengaduan, permohonan, dan konsultasi. Permasalahan yang terjadi pada Kopertis IV Bandung adalah belum ada standar manajemen risiko untuk menemukan risiko potensial dan menentukan cara penanggulangan risiko yang terjadi pada SI Pengarsipannya. Dengan demikian perlu adanya kegiatan penilaian dan rekomendasi kontrol risiko pada sistem tersebut. Tujuannya agar para pemangku kepentingan mendapatkan pengetahuan penanganan risiko berdasarkan standarisasi. Proses manajemen risiko menggunakan *framework* NIST SP800-30 yang telah terstandarisasi oleh Pemerintah Pusat Amerika Serikat serta sesuai dengan panduan penerapan tata kelola keamanan informasi bagi penyelenggara pelayanan publik yang dikeluarkan oleh Kementerian Komunikasi dan Informatika RI. Ada 2 proses yang dikerjakan berdasarkan *framework* NIST yaitu *Risk Assessment* dan *Risk Mitigation*. Metodologi *Risk Assessment* dikerjakan terlebih dahulu dengan menganalisis data-data yang telah didapatkan dari proses wawancara, kuisioner, dan observasi. Aplikasi *Network Mapper* digunakan sebagai teknik tambahan untuk mencari kerentanan sistem. Setelah itu, metodologi *Risk Mitigation* dilakukan untuk menyusun strategi mitigasi risiko berdasarkan hasil *Risk Assessment*. Hasilnya terdapat 20 isu risiko dalam penggunaan SI Pengarsipan. 10 diantaranya berlevel medium dan selebihnya berlevel low. Terdapat 5 terbesar dari 20 isu risiko tersebut diantaranya Mati Listrik (Medium(50)), Stabilitas Daya Listrik (Medium(50)), Penurunan Kinerja AC (Medium(50)), Renovasi Ruangan (Medium(50)), *Insiders* (Medium(50)), dan *Cracker* (Medium(50)).

1. PENDAHULUAN

Sistem informasi (SI) adalah sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, membantu dan mendukung kegiatan operasi. SI bersifat manajerial dari suatu organisasi dan membantu mempermudah penyediaan laporan yang diperlukan[1]. Seiring perkembangan Teknologi informasi (TI), kebutuhan keamanan sistem untuk layanan koordinator pendidikan di Perguruan Tinggi Swasta (PTS) semakin tinggi[[2]. Hal ini dikarenakan banyaknya kasus penyerangan yang terjadi belakangan ini terutama terhadap sistem berbasis Web. Sistem berbasis web yang diakses dengan internet memiliki potensi lebih tinggi untuk diserang karena sifatnya aksesnya yang terbuka daripada sistem yang hanya bisa diakses melalui *intranet/extranet*/non-jaringan[3]]. Serangan merupakan risiko yang terjadi pada suatu sistem informasi. Risiko ini dapat membawa kerugian pada organisasi yang terkena dampaknya. Risiko perlu diidentifikasi dan dikelola agar keamanan sistem lebih terjamin dan dampak yang akan timbul relatif lebih kecil[4].

Koordinator Perguruan Tinggi Swasta (Kopertis) wilayah IV Bandung merupakan salah satu organisasi yang sudah

https://doi.org/10.25077/TEKNOSI.v9i2.2023.208-217

memanfaatkan SI/TI berbasis web dalam pelayanannya. Infrastruktur dan aplikasi sistem informasi Kopertis wilayah IV Bandung dikembangkan secara mandiri oleh seksi sistem informasi. Penggunaan SI/TI di Kospertis meliputi kegiatan kepegawaian, kegiatan keuangan, kegiatan verifikasi dan sertifikasi serta kegiatan pengarsipan.

Situs surat.kopertis4.or.id adalah salah satu sistem informasi berbasis web yang digunakan oleh beberapa pegawai Kopertis IV Bandung untuk mengarsipkan surat berhubungan dengan kegiatan pengaduan, permohonan, dan konsultasi. Dalam menjamin pembaharuan informasi dan keefektifan sosialisasi, kegiatan penyaluran informasi bisa dilakukan oleh semua pegawai Kopertis dari berbagai bagian/sub bagian. Beberapa pegawai diantaranya bisa mengarsipkan surat menggunakan *website surat.kopertis4.or.id* dengan login sebagai operator melalui akun yang telah dibagikan berdasarkan tipe otoritasnya. SI pengarsipan ini sangat membantu dalam proses mengarsipkan data berdasarkan kategori dan waktu *posting*-nya sehingga ketika sistem informasi ini bermasalah maka proses pengumpulan, pengelolaan, penghapusan, pencetakan dan pencarian dokumen pasti terganggu.

Sistem ini dapat dikunjungi oleh siapapun, kapanpun dan dimanapun menggunakan internet. Selain itu, sistem ini juga paling banyak menyimpan data rahasia maupun data publik sehingga apabila terjadi ancaman serangan maka itu akan mempengaruhi proses bisnis dan menimbulkan kerugian paling tinggi daripada sistem lainnya yang ada di Kopertis. Rentan terhadap ancaman adalah efek yang muncul karena tidak adanya manajemen risiko[5].

"*Risk Management is implementation of measures aimed at reducing the likelihood of those threats occurring and minimising any damage if they do; Risk analysis and risk control form the basis of risk management where risk control is the application of suitable controls to gain a balance between security, usability and cost"*[6].

Manajemen risiko adalah implementasi dari pengukuran yang ditujukan pada mengurangi kejadian ancaman dan menimalisir setiap kerusakan. Analisis risiko dan pengontrolan risiko membentuk dasar manajemen risiko. Pengontrolan risiko adalah aplikasi dari pengelolaan yang cocok untuk memperoleh keseimbangan antara keamanan, penggunaan dan biaya.

Strategi yang diambil diantaranya memindahkan risiko kepada pihak lain, menghindari risiko, mengurangi efek negatif risiko, dan menampung sebagian atau semua konsekuensi risiko tertentu. Proses manajemen risiko yaitu identifikasi risiko, penilaian risiko,dan pengambilan langkah-langkah untuk mengurangi risiko sampai tingkat yang dapat diterima. Manajemen risiko mendukung manajer IT dalam menyeimbangkan operasional dan biaya ekonomi dari tindakan pengamanan serta mencapai keuntungan dalam misi dengan melindungi SI dan data yang mendukung misi organisasi.

Permasalahan yang terjadi pada Kopertis IV Bandung adalah belum adanya standar kegiatan manajemen risiko untuk menemukan risiko potensial dan menentukan cara penanggulangan risiko yang terjadi pada SI Pengarsipan Kopertis.

NIST (National Institute of Standard and Technology) Special Publication (SP) 800-30 adalah panduan manajemen risiko untuk sistem teknologi informasi yang terstandarisasi oleh Pemerintah Pusat Amerika Serikat[7]. Metodologi ini dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisis keamanan yang cukup sesuai dengan keinginan pemilik sistem dan ahli teknis untuk benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem SI/TI. Proses ini sangat komprehensif, meliputi segala sesuatu dari ancaman sampai dengan identifikasi sumber untuk evaluasi berkelanjutan dan penilaian[8]. Kerangka kerja NIST SP800-30 dijadikan sebagai rujukan dalam penyusunan dokumen manajemen risiko karena sesuai dengan panduan penerapan tata kelola keamanan informasi bagi penyelenggara pelayanan publik yang dikeluarkan oleh Kementerian Komunikasi dan Informatika RI[9].

Sumber ancaman dapat berasal dari beberapa disaster diantaranya *natural disaster, environment/technology disaster, dan human disaster*[[10]. Disaster yang sering terjadi pada sistem berbasis web adalah *human disaster*. *Human disaster* dapat berupa kesalahan input data dan peretasan. Kesalahan input data biasanya dilakukan oleh pegawai baru yang belum menguasai operasional sistem. Sedangkan peretasan biasanya dilakukan oleh *hacker/cracker* dengan memanfaatkan celah – celah keamanan website yang masih terbuka[11]. Masalah yang timbul pada sistem dapat dikategorikan sebagai risiko. Risiko yang terjadi pada sistem akan menghambat proses bisnis. Dengan demikian, manajemen risiko dibutuhkan agar risiko-risiko yang mungkin timbul bisa tertata dan terkelola dengan baik.

Beberapa penelitian terkait dengan manajemen risiko sistem informasi telah dilakukan oleh beberapa peneliti sebelumnya diantaranya penelitian yang berjudul Analisis Manajemen Risiko pada Penggunaan Sistem Informasi *Smart* PMB di STMIK AMIKOM Yogyakarta yang dilakukan oleh Asro Nasiri, dkk. Dalam penelitian tersebut, NIST SP800-30 digunakan untuk mengindentifikasi, menilai dan membuat mitigasi atas risiko-risiko dalam penggunaan sistem informasi *smart* PMB. Analisis manajemen risiko dilakukan karena di STMIK AMIKOM Yogyakarta selalu ada pergantian Petugas / masuknya petugas baru yang mengoperasikan *smart* PMB tiap tahunnya sehingga ini berpotensi tinggi menyebabkan *human error* seperti kesalahan input data. Penelitian menghasilkan strategi untuk memanajemen risiko pada sistem *smart* PMB dengan hasil penilaian risiko terdiri dari risiko human error tingkat rendah, menengah dan, tingkat tinggi. Strategi mitigasinya difokuskan pada perbaikan *software* [12].Namun penelitian tersebut belum ada penerapan *tool* untuk *system security test* pada tahap identifikasi kerentanan pada proses penilaian risiko serta tidak menyertakan analisis kontrol dan rekomendasi Control pada proses mitigasi.

Penelitian lain dengan judul Manajemen Risiko pada Sistem Penerimaan Peserta Didik Baru (PPDP *online*) Kemdikbud yang dilakukan oleh Masyhuri, dkk dimana penelitian ini bertujuan mengidentifikasi risiko pada PPDB *Online* sepanjang tahun 2012 dari 9 Kabupaten dan Kota yaitu: Kabupaten Bangli, Kota Banda Aceh, Kota Pekanbaru, Kota Tebing Tinggi, Kota Tangerang Selatan, Kota Batam, Kota Pontianak, Kota Pekalongan dan Kota

Semarang[13]. Penelitian menghasilkan skor dan level risiko dari ke-sembilan kabupaten dan kota tersebut serta mensortirnya dari level rendah ke tinggi untuk menemukan kota/kabupaten yang memiliki risiko tertinggi. Namun kekurangan penelitian ini, identifikasi kerentanan hanya dilakukan pada *port* jaringan, belum adanya pengujian keamanan sistem khususnya pada potensi kegiatan *cybercrime (human disaster)* serta penyesuaian *scoring* pada level *risk determination* dengan standar NIST SP800-30.

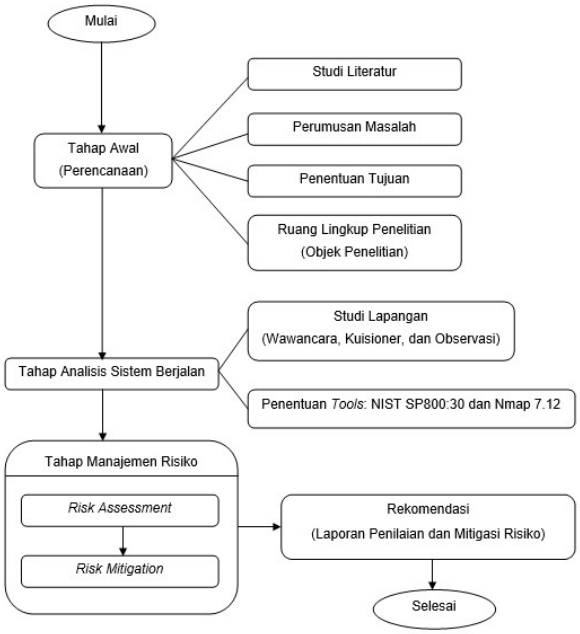
Berdasarkan permasalahan diatas serta menimbang kelebihan dan kekurangan dari penelitian sejenis sebelumnya maka penelitian ini membahas tentang analisis manajemen risiko pada SI pengarsipan di seksi sistem informasi melalui proses *risk assessment* dan *risk mitigation* menggunakan standar NIST SP800-30 dimana sistem yang diteliti adalah sistem yang bisa dikunjungi oleh siapapun melalui internet dengan pengujian keamanan sistem (*system security test*) pada langkah identifikasi kerentanan di proses *risk assessment* malalui *tool* NMap (*network mapper)* serta mengidentifikasi ancaman dan kerentanan mencakup risiko *cybercrime* (*human disaster*).

Dengan demikian, proses penilaian dan mitigasi risiko menghasilkan solusi berupa dokumen rekomendasi strategi manajemen risiko terkait penggunaan SI Pengarsipan di lingkungan kerja Kopertis Wilayah IV Bandung yang belum pernah dilakukan sebelumnya. Rekomendasi ini akan menjadi acuan untuk langkah perbaikan sistem dan prosedur kerja di masa mendatang.

2. METODE

Objek penelitian pada kasus ini adalah proses surat keluar, surat masuk dan pengarsipan surat yang digunakan oleh Staf, Kepala Sb Bagian/Seksi, kepala Bagian/Bidang, Sekretaris pelaksana, Sekretaris Sespel, koordinator, Sekretaris koordinator, Pengadministrasi Surat, dan Pemohon.

Metodologi penelitian sebagian besar didasarkan pada tahap-tahap dalam metode *risk asessment* dan *risk mitigation* NIST 800-30. Secara keseluruhan ada empat tahap yang dilakukan yaitu:



Gambar 1. Tahap Penelitian

Berdasarkan *Flowchart* kerangka metodologi pada Gambar 1 maka beberapa langkah yang dilakukan dalam penelitian ini antara lain:

1. Tahap Awal (Perencanaan)
   Tahap ini terdiri dari:
   a. Studi Literatur
      Studi kepustakaan dilakukan untuk mendalami berbagai teori yang relevan terkait manajemen risiko. Selain itu, dalam studi pustaka, didapatkan suatu konsep, teori, serta model yang mendukung masalah penelitian, sehingga dapat menghasilkan suatu kesimpulan untuk penerapan teoritisnya. Konsep NIST, COBIT, dan OCTAVE merupakan kerangka kerja yang dijadikan pembanding di dalam memahami proses manajemen risiko.
   b. Perumusan Masalah
      Menentukan tentang masalah apa saja yang akan dibahas dalam penelitian dengan cara mengamati kegiatan yang ada pada Seksi Sistem Informasi.
   c. Penentuan Tujuan
      Menentukan hasil-hasil seperti apakah yang hendak dicapai dari sebuah penelitian manajemen risiko SI pengarsipan.
   d. Ruang Lingkup Penelitian
      Menentukan bagian variabel-variabel yang diteliti, populasi atau subjek penelitian, dan lokasi penelitian.
2. Tahap Analisis Sistem Berjalan
   a. Studi Lapangan (Wawancara, Kuisioner dan Observasi)
      Pada tahap ini diadakan tanya lawab dengan beberapa staf/pegawai Seksi Sistem Informasi untuk memperoleh data yang akurat tentang ancaman dan kelemahan sistem informasi pengarsipan. Selain itu juga melakukan pengamatan untuk mendapatkan situasi dan informasi terkini mengenai objek yang diteliti, sehingga dapat ditentukan variabel-variabel dalam tahapan proses penelitian selanjutnya.

https://doi.org/10.25077/TEKNOSI.v9i2.2023.208-217

b. Penentuan *Tools*
Tool yang digunakan dalam manajemen risiko adalah NIST SP800-30. NIST seri ini akan menjadi pedoman untuk memanajemen risiko pada sistem informasi pengarsipan. Sedangkan Nmap 7.12 dijadikan sebagai *tool* penguji keamanan Sistem Informasi Pengarsipan dari sebuah/beberapa kerentanan.

3. Tahap Manajemen Risiko
Tahap Manajemen risiko mengacu pada pedoman NIST SP800-30 yaitu *risk assessment dan risk mitigation.*
a. *Risk Assessment* (Penilaian Risiko)
Pada penilaian risiko ada 9 tahap yang harus dilakukan secara berurutan[14]:
1) S*ystem Characterization* (Karakterisasi Sistem)
Langkah pertama adalah menentukan ruang lingkup usaha dari Kopertis Wilayah IV Terkait dengan SI Pengarsipan. Untuk melakukan hal ini, perlu adanya identifikasi menggunakan teknik pengumpulan informasi, batasan sistem, sumber daya dan informasi yang merupakan bagian dari SI Pengarsipan. *Output* dari langkah ini adalah Karakterisasi dari SI Pengarsipan gambaran dari lingkungannya, dan batasan sistemnya.
2) *Threat Identification* (Identifikasi Ancaman)
Pada langkah ini, potensi ancaman pada SI Pengarsipan diidentifikasi dan didokumentasikan. Sumber ancaman bisa berasal dari alam, manusia, teknologi atau pertimbangan lingkungan. *Output* dari langkah ini adalah sebuah pernyataan ancaman yang berisi daftar ancaman beserta sumbernya yang dapat mengeksploitasi kerentanan SI Pengarsipan.
3) *Vulnerability Identification* (Identifikasi Kerentanan)
Pada langkah ini dilakukan proses identifikasi kerentanan berdasarkan sumber ancaman dengan cara menganalisis kerentanan/kelemahan yang dimiliki SI Pengarsipan dan berpotensi terjadi dimasa depan. Kerentanan yang didapat tidak hanya berasal dari wawancara, kuisioner dan observasi tetapi juga dengan penggunaan *tool* penguji keamanan sistem yaitu aplikasi Nmap. Dengan adanya aplikasi ini potensi kerentanan terhadap serangan *cracker/hacker* dapat diidentifikasi.
Output dari langkah ini berupa daftar kerentanan SI Pengarsipan yang dapat dieksekusi oleh sumber ancaman-potensial**.**
4) *Control Analysis* (Analisis Pengendalian)
Pada langkah ini dilakukan pendokumentasian dan menilai efektivitas pengendalian teknis maupun non-teknis yang telah atau akan dilaksanakan oleh manajemen Kopertis Wilayah IV untuk meminimalkan atau menghilangkan kemungkinan (probabilitas) dari sumber ancaman yang mengeksploitasi kerentanan SI Pengarsipan. *Output* dari langkah ini berupa daftar kontrol (kebijakan, prosedur, pelatihan, mekanisme teknis, asuransi, dan lain-lain) yang digunakan untuk mengurangi kemungkinan kerentanan dan mengurangi dampaknya.
5) *Likelihood Determination* (Pengenalan Kecenderungan)
Pada langkah ini ditentukan nilai keseluruhan kemungkinan yang menunjukkan kemungkinan bahwa kerentanan sistem dapat dimanfaatkan oleh sumber ancaman yang diberikan kontrol keamanan yang ada atau yang direncanakan. *Output* dari langkah ini adalah *rating* kemungkinan mulai dari *rating* rendah, menengah, atau tinggi.
6) *Impact Analysis* (Analisis Dampak)
Pada langkah ini ditentukan tingkat dampak negatif yang akan dihasilkan dari ancaman yang berhasil mengeksploitasi kerentanan sistem. *Output* dari langkah ini adalah besaran peringkat dampak rendah, sedang, atau tinggi.
7) *Risk Determination* (Penentuan Risiko)
Pada langkah ini dilakukan pengalian peringkat dari penentuan kemungkinan dan analisis dampak untuk menentukan tingkat risiko. *Output* dari langkah ini berupa risiko tingkat rendah, menengah atau tinggi.
8) *Control Recommendation* (Rekomendasi Kontrol)
Pada langkah ini akan diidentifikasi kontrol yang dapat mengurangi atau menghilangkan risiko yang telah ditentukan pada langkah 7 dan disesuaikan dengan operasi Kopertis Wilayah IV. *Output* dari langkah ini berupa rekomendasi kontrol dan solusi alternatif untuk mengurangi risiko SI Pengarsipan.
9) *Result Documentation* (Dokumentasi Hasil)
Pada langkah ini, hasil dari penilaian risiko didokumentasikan dalam laporan dan diberikan kepada manajemen koperti Wilayah IV. Laporan ini nantinya bermanfaat untuk membantu manajemen membuat keputusan tentang kebijakan, prosedur, anggaran, dan sistem perubahan operasional dan manajemen. *Output* langkah ini berupa laporan penilaian risiko yang menggambarkan ancaman, kerentanan, tingkat risiko, dan rekomendasi pelaksanaan kontrol.
b. *Risk Mitigation* (Pengurangan Risiko)
Pada proses mitigasi risiko ada 2 tahap yang harus diperhatikan agar strategi mitigasi berjalan lancar antara lain:
1) *Risk Mitigation Option*
Ada enam opsi pengurangan risiko yang dapat diambil diantaranya[15]:
a. *Risk Assumption*
b. *Risk Avoidance*
c. *Risk Limitation*
d. *Risk Planning*
e. *Research and Acknowledgment*
f. *Risk Transference*

2) *Approach For Control Implementation*
Setelah memutuskan *risk mitigation option*, selanjutnya membuat strategi mitigasi melalui pendekatan implementasi kontrol dengan langkah berikut ini.
   a) Pemprioritasan Aksi *(Prioritize Action)*
   Pada langkah ini, pemprioritasan dilakukan dengan mengamati tingkatan risiko dari laporan risk assessment kemudian meletakan risiko tersebut berdasarkan *ranking* aksi mulai dari tingkat tinggi ke tingkat rendah.
   b) Mengevaluasi Opsi Kontrol yang Direkomendasikan *(Evaluate Recomended Control Option)*
   Pada langkah ini, evaluasi opsi pengendalian dapat merujuk pada kemungkinan-kemungkinan terbaik dan keefektifannya. *Output* dari langkah ini berupa daftar kemungkinan pengendalian
   c) Pilih Kontrol *(Select Controls)*
   Setelah melakukan analisis biaya-manfaat maka pengendalian dapat dipilih sesuai dengan aksi mitigasinya. *Output* dari langkah ini berupa pilihan kontrol.
   d) Menetapkan Tanggung Jawab *(Assign Responsibility)*
   Penunjukan personil yang tepat untuk kontrol yang diterapkan, *input*-nya adalah kontrol yang terpilih sementara *output* adalah penugasan atau pemilihan penanggung jawab terhadap kontrol yang dilaksanakan.
   e) Mengembangkan Rencana Pelaksanaan Keamanan *(Develop Safeguard Implementation Plan)*
   Pada langkah ini, pengembangan rencana dilakukan dengan memanfaatkan informasi dari langkah 1 sampai dengan 5. Dalam rencana ini sudah tertulis prioritas aksi yang telah disortir, kontrol yang dipilh, penanggung jawab pelaksanaan, penentuan tanggal mulai, kebutuhan, dan target pelaksanaan.

4. Rekomendasi
Pada tahap ini dihasilkan rekomendasi berdasarkan hasil penilaian dan mitigasi risiko. Rekomendasi ini nantinya dapat memberi bantuan kepada manajemen Kopertis Wilayah IV Bandung untuk membuat keputusan suatu kebijakan keamanan, memperbaharui prosedur, anggaran, dan sistem operasionalnya.

3. HASIL

3.1. Analisis Sistem Berjalan

3.1.1. Penentuan Sampel untuk Studi lapangan

Penerapan manajemen risiko SI harus memperhatikan situasi sosial yang terdiri atas tiga elemen yaitu tempat, pelaku, dan aktivitas yang berinteraksi secara sinergis. Situasi sosial tersebut merupakan kesatuan dalam organisasi dengan berbagai aktivitas dari orang-orang yang berinteraksi secara langsung dengan SI Pengarsipan.

Penentuan sumber data pada orang yang diwawancarai dipilih sesuai pertimbangan dan tujuan**.** Narasumber diambil sebanyak 7 orang dari 18 populasi yang ada di Kopertis Wilayah IV terkait pengguna ataupun sebagai admin SI pengarsipan. 18 populasi ini berasal dari setiap bagian dengan akun yang dibagikan berbeda-beda tingkat otoritasnya. Otoritas *full access* dimiliki oleh koordinator, sekretaris, kepala dan staf seksi sistem informasi. Batas toleransi kesalahan (*error tolerance*) yang digunakan adalah sebesar 30%.

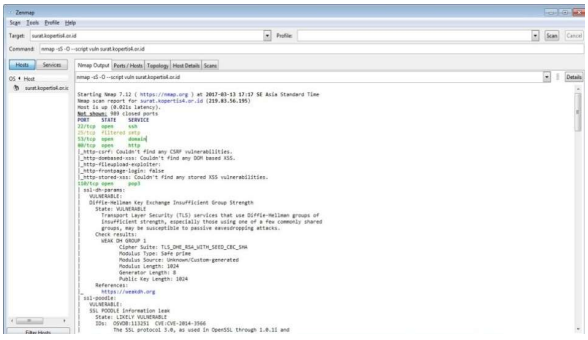
Pemilihan jumlah sampel sebanyak 7 narasumber sesuai dengan rumus perhitungan sampel Slovin[16] sebagai berikut:

$$n = \frac{\mathrm{N}}{1+\mathrm{Ne}^2} \quad (1)$$

$$n = \frac{18}{1+18\,.0{,}3^2} = \frac{18}{2{,}62} = 6{,}87 \approx 7 \quad (2)$$

3.1.2. Vulnerability System Test

Nmap adalah aplikasi keluaran insecure.Com LLC yang dapat mencari *vulnerability* melalui pemindaian jaringan suatu sistem[17]. SI Pengarsipan Kopertis IV dapat diuji dengan cara mengetik "*surat.kopertis4.or.id"* pada kolom target. Kemudian memasukkan *command "Nmap -sS -sS -O --script=vuln surat.kopertis4.or.id*" sebelum mengklik tombol *scan* di aplikasi Nmap. Gambar 2 menunjukkan hasil keluaran Nmap setelah memindai surat.kopertis4.or.id.



Gambar 2. Nmap *Output* (*Vulnerability Scanning*)

3.2. Risk Management

3.2.1. Risk Assessment (Penilaian Risiko)

Proses penilaian risiko memiliki sembilan tahap utama dengan hasil akhirnya berupa nilai risiko. Tujuan dari langkah ini adalah untuk menentukan tingkatan risiko pada sistem IT. Suatu *risk*

https://doi.org/10.25077/TEKNOSI.v9i2.2023.208-217

scale dan *risk-level matrix* harus dibuat untuk menentukan risiko. Tabel 1 menunjukan matriks level risiko yang didapat berdasarkan perkalian tingkat/level dampak dengan tingkat/level kemungkinan terjadinya ancaman.

Output dari langkah ini adalah berupa tingkat risiko rendah, menengah atau tinggi seperti yang terlihat pada Tabel 2.

Tabel 1. *Risk-Level Matrix*

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

Sumber: NIST SP800-30:25

Tabel 2. Level Risiko pada SI Pengarsipan Kopertis

No.	*Vulnerability*	Tingkatan Dampak	*Likelihood*	Level Risiko
1.	Penangkal petir yang sudah usang sehingga perlu diganti	*High (100)*	*Medium (0.5)*	*Medium (50)*
2.	1. Alat pemadaman kebakaran kurang optimal karena belum didukung dengan sistem proteksi kebakaran seperti *Emergency Power Off* dan *gaseous suppressant* yang tidak akan merusak server. 2. Masih adanya bahan bangunan disekitar server yang mudah terbakar 3. Pengamanan *Mini Circuit breaker* (MCB) kurang optimal karena hanya bisa memutuskan arus listrik bila melampaui batas yang tertera pada MCB	*High (100)*	*Low (0.1)*	*Low (10)*
3.	1. Konstruksi bangunan yang telah mengalami penyusutan sehingga perlu direnovasi. 2. Belum ada sensor pendeteksi gempa. 3. Belum ada prosedur untuk menyelamatkan sistem saat terjadi gempa 4. Belum memasang jalur evakuasi 5. Posisi letak *server* pada daerah yang rawan bencana.	*High (100)*	*Low (0.1)*	*Low (10)*
4.	Ketidaktersedian alat pengatur kelembaban dan alat pencegah konsletting listrik.	*Medium (50)*	*Low (0.1)*	*Low (5)*
5.	Posisi letak kabel yang dekat dengan pohon.	*Medium (50)*	*Medium (0.5)*	*Medium (25)*
6.	1. Kabel perangkat jaringan yang longgar 2. Perangkat jaringan yang sinyalnya mudah di interferensi oleh sinyal lain. *3.* Kecepatan layanan internet yang kecil sehingga terjadinya *overload traffic* saat penggunanya banyak. 4. *Setting* dan konfigurasi perangkat jaringan yang belum sesuai dengan standar *provider* 5. Belum ada pengaturan pembatasan maksimal kecepatan unduh dan unggah bagi *client* yang konek 6. Kualitas perangkat jaringan yang kurang bagus	*Low (10)*	*High (1.0)*	*Low (1)*
7.	Beberapa *Hardware* sudah mulai rusak dan beberapanya lagi sudah terlalu tua.	*Low (10)*	*Low (0.1)*	*Low (1)*
8.	1. Kualitas Material selang pembuangan kurang bagus 2. Posisi AC terlalu dekat dengan *rack server*	*Medium (50)*	*Medium (0.5)*	*Medium (25)*
9.	Daya UPS (*Uninterruptible power supply)* terlalu kecil.	*Medium (50)*	*High (1.0)*	*Medium (50)*
10.	1. Prosedur pemakaian *stop* kontak yang belum ada 2. *Stop* kontak yang digunakan tidak memiliki teknologi pencegah kelebihan panas	*High (100)*	*Low (0.1)*	*Low (10)*
11.	1. Stabilizer yang digunakan sudah terlalu tua 2. *Stop* kontak yang digunakan tidak memiliki teknologi anti *interferance* dan anti *spike*	*Medium (50)*	*High (1.0)*	*Medium (50)*
12.	AC (*Air Conditioner*) yang sudah uzur dan tidak terawat.	*Medium (50)*	*High (1.0)*	*Medium (50)*
13.	1. Pembersihan dan perawatan ruangan jarang dilakukan 2. Belum ada metode yang digunakan untuk mencegah Tikus, semut, dan laba-laba masuk ke lingkungan sistem	*Medium (50)*	*Medium (0.5)*	*Medium (25)*
14.	*Rack server* belum optimal memproteksi komponen dari debu.	*Medium (50)*	*High (1.0)*	*Medium (50)*
15.	1. Menu *help* pada sistem belum ada 2. Buku petunjuk penggunaan yang belum diperbaharui 3. *Training* yang dilakukan belum maksimal 4. Sanksi untuk staf yang mengakses sistem dengan akun staf lain belum ada 5. Fitur verifikasi 2 langkah belum dimiliki oleh sistem. 6. *Website* belum *mobile-friendly*	*Low (10)*	*High (1.0)*	*Low (10)*
16.	1. CCTV untuk memantau keadaan lingkungan luar kantor belum ada 2. Alarm pembobolan pintu ruangan server belum ada 3. Rack server yang digunakan belum menggunakan pintu dan kunci digital	*Medium (50)*	*Low (0.1)*	*Low (5)*
17.	1. Belum ada *Smoke detector* yang terpasang disekitar ruangan.	*Medium (50)*	*Low (0.1)*	*Low (5)*

No.	*Vulnerability*	Tingkatan Dampak	*Likelihood*	Level Risiko
	2. Belum ada penunjukan tanggung jawab pengawasan untuk mengawasi staf yang merokok di area sistem.			
18.	1. Masih ada *router* dan *access point* yang menggunakan *password default* manufaktur 2. Sistem tidak memiliki teknologi realtime alerting seperti fitur yang bisa mengirimkan pesan langsung ke koordinator, sekretaris dan/atau kepala bagian via teknologi sms gateway yang telah terintegrasi 3. Antivirus yang tidak diperbaharui	*Medium (50)*	*High (1.0)*	*Medium (50)*
19.	1. Sistem belum memiliki verifikasi akun 2 langkah. 2. Diffie-Hellman Key Exchang Insufficient Group Strength 3. SSL POODLE information leak 4. SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497) *5.* Service regsvc in systems vulnerable to denial of service	*Medium (50)*	*High (1.0)*	*Medium (50)*
20.	1. Sistem belum memiliki verifikasi akun 2 langkah. 2. Sistem operasi linux yang terpasang pada server telah usang/tua. 3. Beberapa Port masih terbuka.	*Low (10)*	*Medium (0.5)*	*Low (5)*

3.2.2. Risk Mitigation (Mitigasi Risiko)

Pada mitigasi risiko ada 2 tahap yang harus diperhatikan agar strategi mitigasi berjalan lancar diantaranya:

1. *Risk Mitigation option*

   Ada 6 opsi pengurangan risiko yang dapat diambil oleh manajemen Kopertis diantaranya:

   a. *Risk Assumption:* Menerima potensi risiko dan melanjutkan operasional SI Pengarsipan atau menerapkan pengendalian untuk menurunkan risiko menjadi suatu tingkatan yang dapat diterima.

   b. *Risk Avoidance*: Menghindari risiko dengan melakukan penghapusan penyebab risiko dan konsekuensinya yaitu membatalkan fungsi tertentu pada SI Pengarsipan atau menutup sistemnya ketika terdapat risiko yang dikenali.

   c. *Risk Limitation*: Membatasi risiko dengan menerapkan pengendalian untuk memperkecil dampak yang kurang baik dari efek ancaman suatu *vulnerability* dengan cara *preventive controls* dan *detective controls*.

   d. *Risk Planning*: Mengatur risiko dengan mengembangkan suatu rencana *risk mitigation*, yang implementasinya diprioritaskan dan pengendalian dalam pemeliharaan.

   e. *Research and Acknowledgment*: Menurunkan risiko kerugian dengan cara mengetahui *vulnerability*/kelemahan dan meneliti pengendaliannya untuk memperbaiki *vulnerability* tersebut.

   f. *Risk Transference*: Memindahkan risiko dengan menggunakan suatu pilihan, untuk mengganti kerugian, seperti pengambilan asuransi.

   Opsi mitigasi yang direkomendasikan untuk diambil oleh Manajemen Kopertis adalah *Risk Assumption, Risk Avoidance, Risk Limitation, Risk Planning,* dan *Research and Acknowledgment* serta *Risk transference.* Jika semua opsi ini diambil maka kemungkinan risiko untuk berkurang lebih besar daripada memilih salah satu atau beberapa diantaranya.

2. *Approach For Control Implementation*

   Setelah memilih opsi *risk mitigation*, selanjutnya manajemen senior Kopertis dapat membuat strategi mitigasi melalui pendekatan implementasi control. Tabel 3 adalah tabel tabulasi dari hasil strategi mitigasi risiko berdasarkan berdasarkan langkah-langkah mitigasi risiko (metodologi *risk mitigation*) dengan *Selected Plan Control* merujuk pada NIST *Security Control Catalog* SP800-53A.

Tabel 3. Strategi Mitigasi Risiko pada Sistem Pengarsipan

No	*Action Priority*	*Selected Controls*		*Required Resources*	*Responsible*
		Control No.	*Control Name*		
1.	*Medium*	PE-9(2)	*Power Equipment And Cabling-Automatic Voltage Controls*	*Surge Protector/Surge Arrester* minimal memiliki *surge current* 93.000A	Bagian Umum Kopertis Wilayah IV
2.	*Low*	PE-10	*Emergency Shutoff*	1. *Emergency Shutoff* harus dekat dengan pengelola / pengawas pada ruangan server. *gaseous suppressant* minimal ada 1 khusus ruangan server dan terisi penuh. 2. *ELCB* (*Earth Leakage Circuit Breakers*) minimal sudah berstandar SNI.	Bagian Umum Kopertis Wilayah IV
		PE-13	*Fire Protection*		
		PE-10	*Emergency Shutoff*		
3.	*Low*	PM-8	*Critical Infrastructure Plan*	1. Pemasangan *Quake Alarm Detector* pada lantai 1 dan 2. 2. Waktu 1 bulan untuk perancangan SOP. 3. Maksimal 1 hari untuk pemasangan rute evakuasi darurat.	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi
		SI-5	*Security Alerts, Advisories, And Directives*		
		CP-10	*Information System Recovery And Reconstitution*		
		PL-1	*Security Planning Policy And Procedures*		

 https://doi.org/10.25077/TEKNOSI.v9i2.2023.208-217

No	Action Priority	Selected Controls		Required Resources	Responsible
		Control No.	Control Name		
4.	*Low*	PE-14	*Temperature And Humidity Controls*	1. Minimal ada 1 *Digital Air Humidity Controller* disetiap sisi. 2. *ELCB* (*Earth* Leakage *Circuit Breakers*) minimal sudah berstandar SNI.	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi
		PE-10	*Emergency Shutoff*		
5.	*Medium*	SA-15(10)	*Development Process, Standards, And Tools- Incident Response Plan*	Ahli jaringan listrik dan jaringan komputer.	Bidang Kelembagaan dan Sistem Informasi
		PE-9	*Power Equipment And Cabling*		
6.	*Low*	MA-1	*System Maintenance Policy And Procedures*	Ahli jaringan komputer dan Layanan ISP Bersangkutan	Bidang Kelembagaan dan Sistem Informasi
		SC-40	*Wireless Link Protection*		
		CP-8	*Telecommunications Services*		
		CM-6	*Configuration Setting*		
7.	*Low*	CP-1	*Contingency Planning Policy And Procedures*	1. Harddisk minimal kecepatan 7200 RPM dan clock speed processor minimal 3 Ghz dengan 8 core. 2. Waktu 1 bulan untuk membuat jadwal dan SOP	Bidang Kelembagaan dan Sistem Informasi
		MA-1	*System Maintenance Policy And Procedures*		
8.	*Medium*	IR-1	*Incident Response Policy And Procedures*	1. Ahli AC dan Teknisi Komputer 2. *rack server* yang digunakan minimal terstandarisasi IP65	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi
		PE-15	*Water Damage Protection*		
9.	*Medium*	MA-1	*System Maintenance Policy And Procedures*	1. Waktu 1 bulan untuk membuat jadwal dan SOP. 2. Genset minimal 40000 watt.	Bidang Kelembagaan dan Sistem Informasi
		PE-11	*Emergency Power*		
10.	*Low*	PE-14	*Temperature And Humidity Controls*	1. Stop kontak yang sudah berstandar SNI. 2. Waktu 1 bulan untuk membuat peraturan dan SOP.	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi
		PL-1	*Security Planning Policy And Procedures*		
11.	*Medium*	PE-9(2)	*Power Equipment And Cabling-Automatic Voltage Controls*	1. Stop kontak yang sudah berstandar SNI. 2. Waktu 1 bulan untuk membuat jadwal dan SOP. 3. Ahli Kelistrikan	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi
		MA-1	*System Maintenance Policy And Procedures*		
12.	*Medium*	MA-1	*System Maintenance Policy And Procedures*	1. Minimal ada 1 *thermohygrometer* untuk menampilkan suhu dan kelembaban yang dapat dimonitor dari luar. 2. Waktu 1 bulan untuk membuat jadwal dan SOP.	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi
		PE-14	*Temperature And Humidity Controls*		
13.	*Medium*	MA-1	*System Maintenance Policy And Procedures*	1. Waktu 1 bulan untuk membuat jadwal dan SOP. 2. Minimal ada 1 *Riddex Plus Pest Repelling Aid* yang dipasang disetiap sisi ruang *server*.	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi.
		IR-1	*Incident Response Policy And Procedures*		
14.	*Medium*	PE-15	*Water Damage Protection*	*rack server* yang digunakan minimal tersertifikasi IP65	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi.
15.	*Low*	SA-5	*Information System Documentation*	1. Waktu 1 bulan untuk membuat peraturan dan SOP. 2. Analis Sistem, *Web Programmer / designer* dan *mobile app programmer.*	Bidang Kelembagaan dan Sistem Informasi.
		SA-5	*Information System Documentation*		
		AT-1	*Security Awareness And Training Policy And Procedures*		
		AT-1	*Security Awareness And Training Policy And Procedures*		
		AC-3(2)	Access Enforcement-Dual Authorization		
		AC-2	*Account Management*		
		SC-18	*Mobile Code*		
16.	*Low*	PE-1	*Physical And Environmental Protection Policy And Procedures*	1. CCTV yang digunakan minimal sudah *night vision* dan berkualitas HD. 2. CCTV *Specializer.* 3. Ahli Kunci.	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi.
		AC-1	*Access Control Policy And Procedures*		
17.	*Low*	SI-5	*Security Alerts, Advisories, And Directives*	*Smoke detector* tipe *Photoelectric* dibutuhkan sekitar 2 buah.	Bagian Umum dan Bidang Kelembagaan dan Sistem Informasi.
		PL-1	*Security Planning Policy And Procedures*		
18.	*Medium*	IA-5	*Authenticator Management*	1. *Password* yang digunakan harus dikombinasikan dengan huruf besar/ kecil, dan angka dengan minimal 8 karakter.	Koordinator, Bagian Umum dan Bidang
		SI-3	*Malicious Code Protection*		
		AC-8	*System Use Notification*		

No	Action Priority	Selected Controls		Required Resources	Responsible
		Control No.	Control Name		
				2. *Software antivirus* resmi yang selalu mengeluarkan *update definition virus* setiap minggunya. 3. Analis Sistem dan *Web programmer*.	Kelembagaan dan Sistem Informasi.
19.	*Medium*	AC-3(2)	*Access Enforcement-Dual Authorization*	1. IT *Consultant*, *Hacker*, Ahli jaringan komputer, Analis Sistem, *Web Programmer* dan *Web Designer.* 2. *Password* yang digunakan harus dikombinasikan dengan huruf besar/ kecil, dan angka dengan minimal 8 karakter. 3. *Tools scanning* yang dapat mengidentifikasi kerentanan seperti Aplikasi NMAP 4. DBA *(Database administrator)*	Bidang Kelembagaan dan Sistem Informasi.
		PL-3	*System Security Plan Update*		
		SC-5	*Denial Of Service Protection*		
		PM-14	*Testing, Training, And Monitoring*		
		PL-3	*System Security Plan Update*		
		PL-1	*Security Planning Policy And Procedures*		
20.	*Low*	AC-3(2)	*Access Enforcement-Dual Authorization*	1. IT *Consultant*, *hacker*, Ahli jaringan komputer, Analis Sistem, *Web Programmer* dan *Web Designer.* 2. *Password* yang digunakan harus dikombinasikan dengan huruf besar/ kecil, dan angka dengan minimal 8 karakter. 3. *Tools scanning* yang dapat mengidentifikasi kerentanan seperti Aplikasi NMAP 4. DBA *(Database administrator).*	Bidang Kelembagaan dan Sistem Informasi.
		PL-3	*System Security Plan Update*		
		PM-14	*Testing, Training, And Monitoring*		
		PL-3	*System Security Plan Update*		
		PM-14	*Testing, Training, And Monitoring*		
		SC-41	*Port And I/O Device Access*		
		PM-15	*Contacts With Security Groups And Associations*		

4. PEMBAHASAN

Setelah hasil mitigasi diketahui, langkah terakhir adalah implementasi kontrol yang akan dilakukan oleh manajemen Kopertis Wilayah IV Bandung. Implementasi kontrol tersebut berkaitan dengan jadwal pengendalian serta perhitungan biaya dan manfaatnya. Kegiatan ini biasa dilakukan oleh Sub Bagian Keuangan yang berkoordinasi dengan Seksi Sistem Informasi. Tidak hanya itu, Hasil proses *risk assessment* dan hasil *risk mitigation* pada Tabel 2 dapat digunakan sebagai acuan dalam kegiatan *evaluation and risk assessment* nanti.

Evaluation and risk assessment suatu saat akan dilakukan karena risiko tidak dapat sepenuhnya dihilangkan. Implementasi kontrol berdasarkan Hasil proses *risk assessment* dan hasil *risk mitigation* pasti menghasilkan risiko-risiko kecil yang perlu diidentifikasi melalui kegiatan evaluasi.

Dari hasil *risk assessment* dan *risk mitigation* maka dapat direkomendasi bahwa:

1. Manajemen Kopertis Wilayah IV Bandung perlu meningkatkan keamanan SI Pengarsipannya terutama pada sumber ancaman yang bernilai terbesar yaitu *medium (50)* hingga yang bernilai terkecil yaitu *Low* (5). Hal ini perlu dilakukan untuk mencegah terjadinya risiko kerusakan dengan cara mengimplementasikan kontrol yang tersedia pada hasil *risk mitigation.*
2. Manajemen Kopertis Wilayah IV Bandung perlu meningkatkan perawatan berkala pada sistem informasi pengarsipannya dengan mengimplementasikan kontrol yang dipilih.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka disimpulkan bahwa terdapat 20 isu risiko dalam penggunaan SI/TI di Kopertis Wilayah IV Badung. 10 diantaranya berlevel *medium* dan selebihnya berlevel *low*. Terdapat 5 terbesar dari 20 isu risiko dalam penggunaan SI/TI berdasarkan sumber ancamannya yaitu Mati Listrik (*Medium*(50)), Stabilitas Daya Listrik (*Medium*(50)), Penurunan Kinerja AC (*Medium*(50)), Renovasi Ruangan (*Medium*(50)), *Insiders* (*Medium*(50)), dan *Cracker (Medium(50)).* Aksi ancaman dari sumber ancaman *Cracker* adalah potensi serangan yang paling banyak terjadi pada SI Pengarsipan yaitu sebanyak 6 aksi.

DAFTAR PUSTAKA

[1] Y. Megasyah and A. A. Arifnur, "Academic Information System Security Audits Using COBIT 5 Framework Domains APO12, APO13 AND DSS05," *Journal of Applied Engineering and Technological Science (JAETS)*, vol. 1, no. 2, pp. 124–135, 2020.

[2] G. I. Belo, L. H. Atrinawati, and Y. T. Wiranti, "Perancangan Tata Kelola Teknologi Informasi Menggunakan Cobit 2019 Pada PT Telekomunikasi Indonesia Regional VI Kalimantan," *Jurnal Sistem Informasi dan Ilmu Komputer Prima (JUSIKOM PRIMA)*, vol. 4, no. 1, pp. 23–30, 2020.

[3] M. Pasaribu and A. Widjaja, *Strategi dan Transformasi Digital*. Kepustakaan Populer Gramedia, 2021.

[4] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 2, pp. 129–146, 2020.

[5] A. A. Putro, A. Ambarwati, and E. Setiawan, "Analisa Manajemen Risiko E-Learning Edlink Menggunakan

 https://doi.org/10.25077/TEKNOSI.v9i2.2023.208-217

Metode NIST SP 800-30 Revisi 1," *Jurnal Teknologi dan Informasi*, vol. 11, no. 2, pp. 125–136, 2021.

[6] S. Meharanjunisa and S. Baker, "Implementation and role of risk management in an organization," Jun. 2020.

[7] A. Elanda and D. Tjahjadi, "Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute Of Standards And Technology) Sp 800-30.(Studi Kasus: Disinfolahtaau Mabes Tni Au)," *Infoman's: Jurnal Ilmu-ilmu Manajemen dan Informatika*, vol. 12, no. 1, pp. 1–13, 2018.

[8] D. Suhartono and K. N. Isnaini, "Strategi Recovery Plan Teknologi Informasi di Perguruan Tinggi Menggunakan Framework NIST SP 800-34," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, pp. 261–272, 2021.

[9] A. Kurniati, L. E. Nugroho, and M. N. Rizal, "Manajemen risiko teknologi informasi pada e-government: ulasan literatur sistematis (Information Technology Risk Management on e-Government: Systematic Literature Review)," *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, vol. 22, no. 2, pp. 207–222, 2020.

[10] 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: Jurnal Elektronika dan Komputer*, vol. 14, no. 1, pp. 141–151, 2021.

[11] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "Analisis risiko teknologi informasi pada aplikasi sap di pt serasi autoraya menggunakan iso 31000," *Sebatik*, vol. 23, no. 1, pp. 36–43, 2019.

[12] E. Pujastuti and A. Nasiri, "Analisis Manajemen Resiko Pada Penggunaan Sistem Informasi 'Smart Pmb' Di Stmik Amikom Yogyakarta," *SEMNASTEKNOMEDIA ONLINE*, vol. 4, no. 1, p. 1, 2016.

[13] I. Masyhuri and F. Samopa, "Pengembangan Manajemen Resiko Teknologi Informasi Pada Sistem Penerimaan Peserta Didik Baru (Ppdb Online) Kemdikbud Menggunakan Framework Nist Sp800-30," *Pros. Semin. Nas. Manaj. Teknol. XVIII*, pp. 1–7, 2015.

[14] R. S. Ross, "Guide for conducting risk assessments," 2012.

[15] A. P. Putra and B. Soewito, "Integrated Methodology for Information Security Risk Management using ISO 27005: 2018 and NIST SP 800-30 for Insurance Sector," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, 2023.

[16] D. Yadewani and R. Wijaya, "Pengaruh e-Commerce terhadap minat berwirausaha," *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, vol. 1, no. 1, pp. 64–69, 2017.

[17] N. Nazwita and S. Ramadhani, "Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata," in *Seminar Nasional Teknologi Informasi Komunikasi dan Industri*, 2017, pp. 308–317.

NOMENKLATUR

n	arti dari jumlah sampel
N	arti dari jumlah populasi
e	arti dari batas toleransi kesalahan (*error tolerance*)

BIODATA PENULIS

Adi Arga Arifnur, M.Kom
Lahir pada 20 Agustus 1992 di Kota Pekanbaru Riau. Pendidikan Terakhir berasal dari STMIK LIKMI Bandung dengan gelar Magister Komputer. Saat ini bekerja sebagai dosen bidang sistem informasi.

Hery Heryanto, Ph.D
Seorang dosen dari Institut Teknologi Harapan Bangsa dan IT Manager STMIK LIKMI. Pendidikan Terakhir berasal dari ITB dengan gelar *Doctor of Philosophy* dalam bidang *Electrical Engineering and Informatics*

Yoga Megasyah, M.Kom,
Seorang dosen dari Universitas Nasional Pasim. Pendidikan Terakhir berasal dari STMIK LIKMI Bandung dengan gelar Magister Komputer dalam bidang sistem informasi.