Prosiding Seminar Nasional Teknologi Komputer dan Sains
Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

PENILAIAN RISIKO KEAMANAN INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAKAD) DENGAN MENGGUNAKAN FRAMEWORK NIST-SP 800 30

Hena Sulaeman1[1], Hadi Prasetyo Utomo [1], Agus Iim Suryana [2,*]

[1] Fakultas, Program St, Nama Institusi, Kota, Indonesia
[2] Teknik Informatika, Magister Teknik Informatika, Universitas Langlangbuana, Bandung, Indonesia
Email: [1]henasulaeman@sttbandung.ac.id, hadi@informatika.unla.ac.id[2], [3,*]pamupus@email.com
Email Penulis Korespondensi: henasulaeman@sttbandung.ac.id

Abstrak− Sistem keamanan informasi seperangkat kebijakan, prosedur, teknologi, dan praktik yang dirancang untuk melindungi, mengamankan, dan menjaga kerahasiaan, integritas, dan ketersediaan data dan informasi dalam suatu organisasi.
Penggunaan Framework NIST-SP 800-30 sebagai panduan dalam manajemen risiko keamanan informasi bertujuan untuk mengidentifikasi, mencegah, dan mengelola potensi risiko yang dapat membahayakan organisasi. Dengan demikian, organisasi dapat mengurangi kemungkinan terjadinya kerugian yang signifikan. Tujuan akhirnya adalah melindungi proses bisnis organisasi dari berbagai ancaman keamanan, meminimalkan potensi kerugian, dan mencegah terjadinya gangguan serius terhadap sistem dan teknologi informasi yang digunakan oleh organisasi.
Penelitian ini berfokus pada penilaian risiko aset system informasi yang terkait dengan system informs akademik (SIAKAD) yang didasarkan pada panduan NIST-SP 800-30. Penilaian risiko bertujuan untuk mengidentifikasi dan mengevaluasi tingkat kerentanan dari aset Teknologi Informasi (TI) yang dapat mempengaruhi proses bisnis. Hasil dari evaluasi risiko digunakan sebagai landasan untuk merencanakan langkah-langkah pengamanan yang disesuaikan dengan tingkat risiko yang telah diidentifikasi dan kontrol yang direkomendasikan. Dengan demikian, penelitian ini bertujuan untuk memastikan bahwa rekomendasi kontrol keamanan yang di sarankan akan efektif dalam mengurangi risiko yang mungkin timbul dari aset TI yang berdampak pada proses bisnis.

Kata Kunci: Keamanan informasi, Keamanan Database, NIST-SP 800-30 , Risk Assesment

1. PENDAHULUAN

STT Bandung (Sekolah Tinggi Teknologi Bandung) merupakan kampus swasta yang sudah menerapkan Teknologi Informasi dan Komunikasi (TIK) di dalamnya. STT Bandung memiliki 5 misi salah satu misi yang berkaitan dengan teknologi yaitu Menyelenggarakan pendidikan tinggi yang dinamis dan kreatif di bidang sosial, seni budaya, dan teknologi berbasis kewirausahaan, Menyelenggarakan layanan Pengabdian Masyarakat secara profesional dalam rangka memberi solusi kreatif terhadap permasalahan di masyarakat terutama dalam bidang sosial, seni budaya, dan teknologi.
Sesuai dengan hasil wawancara yang sudah dilakukan dengan kepala divisi PUSDATIN (Pusat Data dan Informasi), secara umum kampus STT Bandung mempunyai misi yang berkaitan erat kaitanya dengan teknologi informasi yaitu Menyelenggarakan pendidikan tinggi yang dinamis dan kreatif di bidang sosial, seni budaya, dan teknologi berbasis kewirausahaan dan menyelenggarakan layanan pengabdian masyarakat secara profesional dalam rangka memberi solusi kreatif terhadap permasalahan di masyarakat terutama dalam bidang sosial, seni budaya, dan Teknologi. Pada misi tersebutlah perlu peran dari teknologi dan informasi untuk bisa merealisasikan atau mewujudkan nilai yang ada pada misi tersebut.

Berdasarkan salah satu jawaban dari pertanyaan wawancara ada beberapa dampak potensial yang bisa mempengaruhi nilai dari misi kampus STT Bandung adalah ancaman keamanan cyber yang sering terjadi, menurut pendapat narasumber terkait dengan ancaman keamanan cyber terhadap data yang ada di database siakad yaitu melihat karena data yang di proses oleh sistem siakad sangat sensitive dan penting sekali bagi kampus STT Bandung sudah tentu sangat dibutuhkan pengamanan terhadap data tersebut karena data yang diolah oleh sistem siakad harus valid dan perlu di laporkan ke PDDIKTI (Pangkalan Data Pendidikan Tinggi).

Dari banyaknya permasalahan yang sudah di jelaskan, munculah ide penelitian yang akan di angkat. Tujuan utama dari penelitian ini adalah mengidentifikasi kelemahan yang ada dalam sistem saat ini dengan melakukan penilaian risiko, merancang kontrol keamanan database dan mengimplementasikan hasil dari perancangan kontrol keamanan yang sudah dirancang. Penelitian ini akan melibatkan analisis mendalam terhadap arsitektur keamanan yang ada, serta evaluasi risiko terhadap potensi ancaman, langkah-langkah konkret yang akan diambil termasuk konfigurasi ulang firewall, pembaruan rutin untuk kredensial login, pengaturan hak akses yang lebih ketat, dan managemen pencadangan database atau replikasi database yang baik. Pada Penelitian ini memfokuskan pada penilaian risiko untuk mendapatkan rekomendasi kontrol keamananan yang bisa digunakan pada sistem informasi akademik (SIAKAD).

Peneliti sudah melakukan studi literatur terhadap penelitian terdahulu yang berkaitan dengan proses penilaian risiko untuk sistem keamanan informasi, ada beberapa praktik yang direkomendasikan pada penelitian dahulu diantaranya adalah menggunakan metode DREAD (Damage Potential, Reproducibilty, Exploitability, Affected User, Discoverability) dan ISO 27005:2018. Metode DREAD bisa digunakan untuk melakukan proses penilaian risiko dimulai dari langkah identifikasi ancaman, dokumentasi ancaman, penilaian risiko dan rekomendasi perbaikan sedangkan framework ISO 27005:2018 bisa di jadikan sebagai pelengkap dari proses identifikasi ancaman (Utami et al., 2023).

Prosiding Seminar Nasional Teknologi Komputer dan Sains
Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

Rekomendasi yang lain adalah menggunakan framework ISO/IEC 31000 merupakan standar international mengenai pedoman penerapan manajemen risiko dalam praktiknya bisa melakukan identifikasi ancaman, menentukan dampak risiko , menentukan level risiko dan perlakukan risiko terhadap kemungkinan-kemungkinan risiko tersebut (Christian & Sitokdana, 2022).

Selain itu rekomendasi selanjutnya bisa menggunakan framework NIST (National Institute of Standars and Technology) SP 800 30, dalam praktiknya NIST-SP 800 30 memiliki 9 langkah untuk melakukan anlisa risiko diantarnya identifikasi karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, analisa kontrol, penentuan kemungkinan, analisa dampak, penilaian risiko, rekomendasi kontrol dan dokumentasi hasil (Stoneburner & Goguen, n.d.) (Elanda & Buana, 2021).

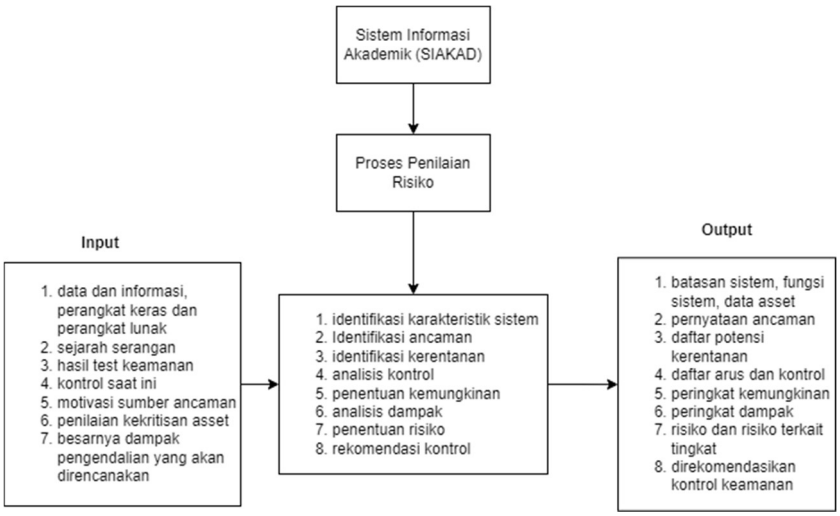
Rekomendasi selanjutnya menggunakan metode Octave Allegro menggunakan 4 fase yang dikelompokan untuk proses identifikasi risiko diantarnya define drivers or guidelines, profile asset, identify threats, identify and Mitigate. Metodelogi ini berfokus pada pengumpulan kebutuhan bisnis dan bisa menyesuaikan risiko sesuai dengan kebutuhan prioritas (Deva & Jayadi, 2022).

Dari ke empat rekomendasi yaitu metode DREAD (Damage Potential, Reproducibilty, Exploitability, Affected User, Discoverability), ISO/IEC 31000, NIST (National Institute of Standars and Technology) SP 800 30 dan metode Octave Allegro. Peneliti memutuskan memilih menggunakan framework NIST (National Institute of Standars and Technology) SP 800 30 dikarenakan sudah terbukti banyak kelebihan jika menggunakan framewok NIST-SP 800 30 diantaranya mudah dipahami, konsisten dan komprehensif bagi pengambil kebijakan, langkah-langkah penilaian risiko lebih terstruktur, mudah dalam melakukan identifikasi ancaman, perhitungan tingkat risiko yang mudah dipahami oleh orang awam dan lebih fleksible karena proses yang ada bisa disesuaikan dengan kebutuhan organisasi (Stoneburner & Goguen, n.d.).

2. METODE PENELITIAN

2.1 Kerangka Dasar Penelitian

Penelitian ini dilakukan di STT Bandung, dan metode yang digunakan adalah metode kualitatif deskriptif. Data-data primer diperoleh melalui wawancara dan observasi, sedangkan data sekunder diperoleh dari studi literatur yang mengkaji penelitian terdahulu yang relevan dengan topik ini. Penelitian ini menggunakan teknik analisis penilaian risiko yang mengacu pada framework NIST-SP 800-30 sebagai dasar metodologi. Berikut kerangka pemikirian pada penelitian ini



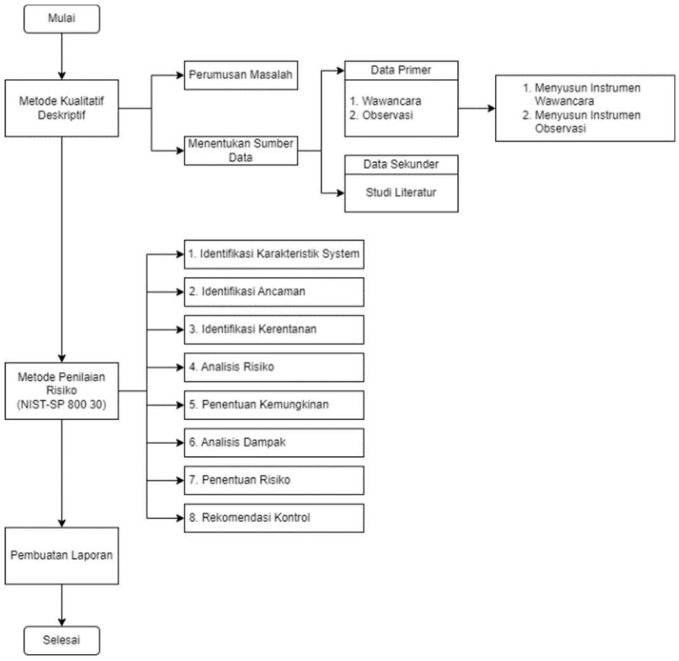
Gambar 1. Kerangka pemikiran

Dalam konteks kerangka pemikiran yang telah disebutkan sebelumnya, terdapat delapan tahapan dalam evaluasi risiko yang masing-masing memiliki input dan output data yang spesifik. Tujuan dari langkah-langkah ini adalah untuk mempermudah pelaksanaan penilaian risiko.

2.2 Tahapan Penelitian

Tahapan pada penelitian ini di dasari dengan pendekatan pada langkah-langkah yang ada di framework NIST-SP 800 30, guna untuk memperoleh gambaran dan analisa mendalam mengenai analisa risiko dan kontrol keamanan yang digunakan. Berikut merupakan tahapan penelitian yang digunakan dalam penelitian ini.

Prosiding Seminar Nasional Teknologi Komputer dan Sains
Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks



Gambar 2. Tahapan Penelitian

a. Metode kualitatif deskriptif

Dalam tahap ini peneliti sudah mengumpulkan beberapa pertanyaan dan sudah di kategorikan kedalam perumusan masalah, kemudian untuk pengumpulan data dilakukan melalui dua sumber data utama, yaitu data primer dan data sekunder. Data primer yang diperoleh dari penelitian ini berasal dari beberapa sumber, termasuk hasil wawancara dengan narasumber, survei, dan pengamatan langsung. Data sekunder data yang diperoleh bersumber dari studi pustaka yang melibatkan pencarian informasi yang sudah ada, serta kutipan dari berbagai sumber seperti internet, berita, jurnal, penelitian-penelitian terdahulu dan buku terbaru yang relevan dengan topik penelitian.

b. Metode penilaian risiko

Tahapan ini dilaksanakan dengan maksud melakukan evaluasi dan klasifikasi risiko yang ada, melalui pendekatan mengidentifikasi potensi ancaman, kerentanan, serta dampak yang timbul dari setiap ancaman terhadap kerentanan yang terjadi. Selain itu. Dalam melakukan penilaian risiko, peneliti mengacu pada panduan yang disajikan oleh framework NIST-SP 800 30. Framework ini mencakup sembilan tahapan dalam penilaian risiko (Stoneburner & Goguen, n.d.), tetapi dalam konteks penelitian ini, hanya delapan tahapan yang akan diadopsi, disesuaikan dengan keperluan penelitian.

c. Pembuatan laporan

Langkah terkahir adalah pembuatan laporan. Laporan yang dibuat berisi ringkasan dari seluruh proses implementasi kontrol keamanan database, pengujian fungsionalitas kontrol dan hasil dari verifikasi keamanan. Laporan ini akan menjadi dokumen penting yang dapat digunakan untuk dokumentasi, evaluasi dan sebagai referensi di masa yang akan datang.

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini yaitu hasil dari penilaian risiko dan kontrol keamanan pada sistem informasi akademik yang direkomendasikan berdasarkan temuan asset yang di dapat pada hasil penilaian risiko.

a. Penilaian Risiko

1. Identifikasi karakteristik system

Sistem Informasi Akademik (SIAKAD) merupakan aplikasi yang memungkinkan terjadinya transaksi atau aktivitas kegiatan akademik yang ada di lingkungan kampus atau di instansi pendidikan. Berdasarkan hasil wawancara yang dilakukan dengan kepala Pusat Data dan Informasi (PUSDATIN) STT Bandung memiliki 4 kelompok asset TI yang digunakan untuk kebutuhan proses bisnis pada aplikasi SIAKAD diantaranya adalah perangkat keras (Hardware), Perangkat Lunak (Software), Perangkat Virtual (Cloud), Sumber daya Manusia (SDM).

Prosiding Seminar Nasional Teknologi Komputer dan Sains
Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

Tabel 1. Daftar Asset

No	Kelompok	Asset	Jumlah	Proses Bisnis	ID Asset
1	Perangkat Virtual (Cloud)	Server Virtual Aplikasi	1 unit	Melayani permintaan dari client dan menyediakan resource untuk digunakan secara Bersama, login, logout, download dan upload data	SV-01
		Server Virtual Database	1 unit	Menyimpan semua data utama	SV-02
2	Perangkat Keras (Hardware)	PC Server Storage File Siakad	1 unit	Melayani penyimpanan data file upload client	HD-01
		Perangkat Jaringan	4 unit	Konektivitas internet server	HD-02
		PC Pengguna (Staff Akademik)	6	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di oraganisasi	HD-03
		PC Pengguna (Staff Perpustakaan)	1	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di oraganisasi	HD-04
		PC Pengguna (Staff Prodi)	1	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di oraganisasi	HD-05
		PC Pengguna (Staff Bimbingan Konseling)	1	Karyawan menggunakan komputer untuk	HD-06

No	Kelompok	Asset	Jumlah	Proses Bisnis	ID Asset
				berbagai keperluan administrasi di oraganisasi	
		PC Pengguna (Staff Admin PDDIKTI)	1	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di oraganisasi	HD-07
		PC Pengguna (Staff Kemahasiswaan)	1	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di oraganisasi	HD-08
3	Perangkat Lunak (Software)	Sistem Informasi Akademik (SIAKAD)	1	Digunakan untuk administrasi akademik secara online seperti pengelolaan data mahasiswa, data dosen , pembuatan jadwal perkuliahan , rekap nilai mahasiswa , rekap kehadiran dosen dan lain-lain	SW-01
		Online Akademik System (OASIS)	1	Digunakan untuk penyimpanan informasi-informasi akademik pengguna mahasiswa	SW-02
		Elektronic Learning (E-Learning)	1	Digunakan untuk kegiatan pembelajaran Online, pengguna mahasiswa dan dosen	SW-03
4	Karyawan	Divisi Akademik	6	Mengelola semua akses dari fitur Siakad (super admin)	SDM-01

No	Kelompok	Asset	Jumlah	Proses Bisnis	ID Asset
		Divisi Program Studi (PRODI)	6	Akses terbatas hanya bisa membuatan kurikulum, melihat daftar seminar sidang, cek file skripsi dan KP	SDM-02
		Divisi Perpustakaan	1	Akses terbatas hanya bisa acc penjadwalan sidang skripsi dilihat dari sisa buku yang belum dikembalikan.	SDM-03
		Divisi Bimbingan Konseling	2	Akses terbatas hanya bisa melihat data mahasiswa aktif dan tidak aktif dari status mahasiswa untuk di tindak lanjuti	SDM-04
		Divisi Kemahasiswaan	2	Akses terbatas hanya bisa acc penjadwalan sidang skripsi dilihat dari sisa SKKM yang sudah terpenuhi	SDM-05
		Admin WK 1	3	Akses terbatas hanya bisa mengecek kesesuaian data mahasiswa yang dilaporkan mahasiswa, diperbaiki oleh admin WK 1 di system akademik	SDM-06

2. Identifikasi ancaman

Data ancaman ini bersumber dari riwayat kejadian masa lalu serta kemungkinan terjadinya kembali di masa yang akan datang. Dalam konteks ini, dilakukan identifikasi ancaman yang berpotensi menggangu proses bisnis yang terjadi terhadap aset Teknologi Informasi (TI) yang ada di STT Bandung. Identifikasi tersebut telah disesuaikan dengan informasi yang diperoleh melalui wawancara yang telah dilaksanakan.

Tabel 2. Identifikasi Ancaman

No	Sumber Ancaman	Motivasi	Tindakan Ancaman	Kode
1	Hacker, cracker	1. Tantangan 2. Uang	1. DDoS Attack 2. Deface Website	IA-1

Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

No	Sumber Ancaman	Motivasi	Tindakan Ancaman	Kode
		3. Status Ketenaran	3. Vulenerability File upload	
2	Orang dalam (karyawan yang kurang terlatih, tidak puas, berbahaya, lalai, tidak jujur atau dipecat	1. Keuntungan 2. Kesalahan dan kelalaian yang tidak disengaja (seperti entri data, kesalahan program) 3. Ketidak puasan karyawan terhadap aturan	1. Penyalah gunaan komputer 2. Kecurangan dan pencurian 3. Penyuapan informasi 4. Input data dipalsukan, data yang rusak 5. Penjualan informasi pribadi 6. Sistem akses yang tidak sah	IA-2
3	Serangan Virus Malware	informasi pribadi, keuangan, atau bisnis	Mencuri data penting yang ada di dalam PC yang terinveksi malware	IA-3
4	Human Error	1. Ketidak sengajaan oleh pihak system administrator saat melakukan maintenance 2. Kesalahan oleh staff admin saat input data ke sistem	1. Konfigurasi instalasi aplikasi pada server yang salah yang dilakukan oleh system administrator 2. Data yang di input ke sistem tidak valid	IA-4
5	Pemadaman Listrik	Pemadaman dilakukan karena keperluan untuk maintenance dari PLN	1. Gangguan operasional dan produktivitas TI 2. Kehilangan data dan Kerusakan perangkat keras	IA-5

Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

No	Sumber Ancaman	Motivasi	Tindakan Ancaman	Kode
			3. Rentan terhadap serangan 4. Ketidak mampuan untuk mengakses data 5. Kerusakan perangkat pendingin pada ruang server	
6	Developer yang masih bisa mengakses database production dengan mudah	Diperlukan pembaruan data dengan melakukan injeksi langsung ke dalam database karena terdapat kebutuhan mendesak untuk mengubah data.	1. Pencurian data sensitive 2. Perubahan data yang tidak valid jika terjadi kesalahan 3. Pembocoran informasi penting 4. Kegagalan pengamanan	IA-6
7	Single point database failure/Down	Ketidaksengajaan	1. Kehilangan data karena adanya kegagalan Software package instalasi database 2. Kehilangan data karena human error 3. Tidak siap dalam kasus bencan alam 4. Ketergantungan pada perbaikan manual	IA-7
8	Debu dan Korosi	Ketidaksengajaan	1. Hardware Komputer failure error blue screen 2. Processore over heate 3. HDD storage tidak terbaca	IA-8

No	Sumber Ancaman	Motivasi	Tindakan Ancaman	Kode
			4. Data pada PC hilang	
9	Kesalahan fungsional pada perangkat lunak (Software)	Ketidaksengajaan	Software yang sedang digunakan tiba-tiba not responds , over close dan tidak akan bisa di gunakan	IA-9
10	Kebakaran (*Fire*)	Ketidaksengajaan	Terjadinya konselting listrik yang mengakibatkan terjadi kebakaran dan kehilangan asset TI yang penting serta akan menggangu proses bisnis yang sedang berlangsung	IA-10

3. Identifikasi kerentanan

Tujuan dari langkah ini adalah untuk menghasilkan daftar kerentanan sistem yang mungkin dapat dieksploitasi oleh potensi sumber ancaman. Dalam proses identifikasi kerentanan, terdapat beberapa langkah yang akan dijalankan. Pertama, akan mencari sumber-sumber kerentanan yang ada.

Tabel 3. Identifikasi Kerentanan

No	Letak Vulnerability (kerentanan)	Sumber Ancaman	Aksi Ancaman	Kode
1	kelemahan pada code program aplikasi	Adanya Hacker, cracker yang dengan sengaja mencari celah keamanan pada sistem	1. DDoS *Attack* 2. Deface Website 3. Vulenerability File upload	IK-1
2	Tidak Ada Kontrol Pengawasan atau dokumentasi	Tidak ada acuan untuk maintenance aplikasi jika terjadi kesalahan program	1. DDoS Attack 2. Deface Website 3. Vulenerability File upload	IK-2
3	Tidak dlakukan Pentesting	Adanya kelemahan code program yang	1. DDoS Attack 2. Deface Websit	IK-3

No	Letak Vulnerability (kerentanan)	Sumber Ancaman	Aksi Ancaman	Kode
		lolos pada saat launch ke production server	3. Vulenerability File upload	
4	Kurangnya pelatihan dan kesadaran karyawan tentang keamanan informasi	Orang dalam (karyawan yang kurang terlatih, tidak puas, berbahaya, lalai, tidak jujur atau dipecat	Tidak terdapat Standard Operating Procedure (SOP) yang menguraikan perjanjian untuk menjaga keamanan data Siakad. Pengamanan hanya bergantung pada kepercayaan masing-masing unit.	IK-4
5	Pembaharuan rutin pada komputer pengguna tidak di lakukan	Serangan Virus Malware	Ancaman ini memiliki potensi untuk mencuri data berharga yang ada di dalam komputer yang terinfeksi malware. Selain itu, pelaku juga dapat mengancam pengguna untuk membayar agar file penting yang terkunci oleh malware bisa diakses kembali.	IK-5
6	Kesalahan konfigurasi server yang terjadi saat instalasi atau maintenance oleh administrator sistem.	Human Error	Pengaturan keamanan yang lemah, pembaruan tidak rutin, tidak menerapkan patch keamanan kurangnya pemantauan dan logging yang mencurigakan pada sistem	IK-6
7	Rusaknya UPS yang digunakan pada PC server	Pemadaman Listrik	1. Gangguan operasional dan produktivitas TI	IK-7

Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

No	Letak Vulnerability (kerentanan)	Sumber Ancaman	Aksi Ancaman	Kode
			2. Kehilangan data dan Kerusakan perangkat keras 3. Rentan terhadap serangan 4. Ketidak mampuan untuk mengakses data 5. Kerusakan perangkat pendingin pada ruang server	
8	Role akses database yang belum di konfigurasi dengan baik.	Developer yang masih bisa mengakses database production dengan mudah	1. Pencurian data sensitive 2. Perubahan data yang tidak valid jika terjadi kesalahan 3. Pembocoran informasi penting 4. Kegagalan pengamanan	IK-8
9	Regulasi terkait akses user database yang belum di terapkan	Tidak ada SOP yang mengarah ke role akses user pada sistem database		IK-9
10	Tidak ada keamanan replikasi database, masih mengandalkan single server	Database server yang belum menerapkan Teknik keamanan replikasi	1. Kehilangan data karena adanya kegagalan hardware 2. Down Time Database Server 3. Kehilangan data karena human error 4. Tidak siap dalam kasus bencan alam 5. Ketergantungan pada perbaikan manual	IK-10
11	Kehilangan sumber data utama			IK-11
12	Kurang terkontrolnya maintenance yang dilakukan	Debu dan Korosi	1. Hardware Komputer failure error blue screen	IK-12

Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

No	Letak Vulnerability (kerentanan)	Sumber Ancaman	Aksi Ancaman	Kode
			2. Processore over heat 3. HDD storage tidak terbaca 4. Data pada PC hilang	
13	Software usang dan terbaca virus oleh anti virus	Kesalahan fungsional pada perangkat lunak (Software)	Software yang sedang digunakan tiba-tiba not responds , over close dan tidak akan bisa di gunakan	IK-13
14	Kurang terkontrolnya instalasi kelistrikan	Kebakaran (*Fire*)	Terjadinya konselting listrik yang mengakibatkan terjadi kebakaran dan kehilangan asset TI yang penting serta akan menggangu proses bisnis yang sedang berlangsung	IK-14

4. Analisis kontrol

tujuan pada analisis kontrol adalah untuk meninjau kontrol yang sudah ada yang telah di terapkan oleh STT Bandung untuk mengurangi potensi ancaman dan kelemahan pada sistem informasi akademik.

Tabel 4. Analisis Kontrol

Ancaman	**Penyebab ancaman**	**Risiko**	**Kontrol Saat Ini**	**Rencana Kontrol**
Hacker, cracker	kelemahan pada code program aplikasi	system tidak dapat diakses, proses bisnis tidak bisa berjalan pada aplikasi yang terdampak	Memperbaiki setelah kejadian diketahui	Membuat system monitoring secara realtime untuk mengetahui jika ada serangan dari luar
Orang dalam (karyawan yang kurang terlatih, tidak puas, berbahaya, lalai, tidak jujur atau dipecat	Kurangnya pelatihan dan kesadaran karyawan tentang keamanan informasi	Pelanggaran keamanan data, kehilangan data, kebocoran data, risiko hukum	dilakukan pelatihan maksimal 1 kali dalam setahun	Membuat kontrol untuk karyawan yang belum melakukan atau mengajukan pelatihan
Serangan Virus Malware	Pembaharuan rutin pada komputer	Pencurian data, kerusakan data, pemerasan	Install antivirus	Pembatasan hak akses, pengguna diberikan akses ke

Ancaman	Penyebab ancaman	Risiko	Kontrol Saat Ini	Rencana Kontrol
	pengguna tidak di lakukan			aplikasi yang dibutuhkan untuk bekerja, update database antivirus secara rutin
Human Error	Kesalahan konfigurasi server yang terjadi saat instalasi atau maintenance oleh administrator sistem.	gangguan pada proses bisnis akademik jika terjai kesalahan pada server	dilakukan pelatihan maksimal 1 kali dalam setahun	menerapkan Principle of least Privilege – PoLP untuk hak akses sysadmin.
Pemadaman Listrik	Adanya maintenance Kelistrikan	Kerusakan pada hardware komputer dan jaringan, proses bisnis akan terhenti	Tidak ada	Melakukan pengadaan genset listrik dan UPS
Developer yang masih bisa mengakses database production dengan mudah	Role akses database yang belum di konfigurasi dengan baik.	Mengancam Integritas data, mengancam kerahasiaan data	Tidak ada	Membuat Teknik keamanan database Role Base Access Control (RBAC) untuk database siakad
Single point database failure/Down	Tidak ada keamanan replikasi database, masih mengandalkan single server	Mengancam ketersediaan data	Tidak ada	Membuat Teknik keamanan database menggunakan Replikasi Database Master-Slave
Debu dan Korosi	Kurang terkontrolnya maintenance yang dilakukan	Mengancam kerusakan pada hardware komputer, processore over heat	Maintenance komputer berdasarkan permintaan	Melakukan maintenance rutin tanpa menunggu permintaan agar lebih terkontrol
Kesalahan fungsional pada perangkat lunak (Software)	Software usang dan terbaca virus oleh anti virus	Software over close dan tidak bisa digunakan	Tidak ada	Melakukan update patch software secara rutin
Kebakaran (*Fire*)	Kurang terkontrolnya instalasi kelistrikan	Kerusakan ada hardware, kehilangan asset TI yang berharga, proses bisni akan terhenti	Tidak ada	Pengecekan rutin pada tegangan listrik untuk memastikan listrik aman, membuat sistem sensore berbasis IoT untuk mendeteksi kebakaran secara dini

Prosiding Seminar Nasional Teknologi Komputer dan Sains
Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

5. Menentukan Kemungkinan / *Likelihood*

Langkah ini bertujuan untuk menganalisis kondisi saat ini dari masing-masing aset yang terkait dengan manajemen keamanan informasi akademik di STT Bandung.

Tabel 5. Menentukan kemungkinan

Kategori Asset	Nama Aset	Kode Asset	Nilai Kemungkinan	Level Kemungkinan
SDM	Divisi Akademik	SDM-01	0	Sangat Jarang
	Divisi Program Studi (PRODI)	SDM-02	0	Sangat Jarang
	Divisi Perpustakaan	SDM-03	0	Sangat Jarang
	Divisi Bimbingan Konseling	SDM-04	0	Sangat Jarang
	Divisi Kemahasiswaan	SDM-05	0	Sangat Jarang
	Admin WK 1	SDM-06	0	Sangat Jarang
Perangkat Virtual Server (Cloud)	Server Virtual Aplikasi siakad	SV-01	1	Sangat Jarang
	Server Virtual Database	SV-02	28	Mungkin
Perangkat Keras (Hardware)	PC Server Storage File Siakad	HD-01	10	Jarang
	Perangkat Jaringan	HD-02	6	Jarang
	PC Pengguna (Staff Akademik)	HD-03	23	Mungkin
	PC Pengguna (Staff Perpustakaan)	HD-04	31	Mungkin
	PC Pengguna (Staff Prodi)	HD-05	21	Mungkin
	PC Pengguna (Staff Bimbingan Konseling)	HD-06	21	Mungkin
	PC Pengguna (Staff Admin PDDIKTI)	HD-07	20	Mungkin
	PC Pengguna (Staff Kemahasiswaan)	HD-08	21	Mungkin
	Sistem Informasi Akademik (SIAKAD)	SW-01	12	Jarang

Prosiding Seminar Nasional Teknologi Komputer dan Sains
Vol 1, No 1, November 2023, page 414 - 432
ISSN 3030-8011 (Media Online)
Website https://prosiding.seminars.id/prosainteks

Kategori Asset	Nama Aset	Kode Asset	Nilai Kemungkinan	Level Kemungkinan
Perangkat Lunak (Software)	Online Akademik System (OASIS)	SW-02	12	Jarang
	Elektronic Learning (E-Learning)	SW-03	12	Jarang

6. Analisis dampak

Tujuan dari langkah ini adalah untuk menetapkan tingkat dampak negatif yang dapat dihasilkan oleh sumber ancaman yang ada dalam Sistem Informasi Akademik (SIAKAD) terhadap aset-aset Teknologi Informasi (TI). Tingkat dampak dan pemetaan dampak yang di ambil yaitu berdasarkan tabel berikut:

Tabel 6. Tingkat Dampak/Impact
Sumber: (Joint Task Force Transformation Initiative, 2012)

Skor	Tingkat Dampak	Definisi Dampak
96-100	Sangat besar	Hampir pasti akan menimbulkan dampak buruk yang sangat besar
80-95	Besar	Kemungkinan besar ancaman tersebut akan menimbulkan dampak buruk
21-79	Sedang	Kemungkinan ancaman tersebut akan menimbulkan dampak buruk
5-20	Kecil	Kemungkinan besar ancaman tersebut tidak akan menimbulkan dampak buruk
0-4	Sangat kecil	Kecil kemungkinana dampak buruk akan terjadi

Tabel . Peta penentuan risiko
Sumber : (Joint Task Force Transformation Initiative, 2012)

Kemungkinan	Dampak				
	Sangat kecil	Kecil	Sedang	Besar	Sangat besar
Sangat sering	Low	Moderate	High	Very High	Very High
Sering	Low	Moderate	Moderate	High	Very High
Mungkin	Low	Low	Moderate	Moderate	High
Jarang	Very Low	Low	Low	Moderate	Moderate
Sangat jarang	Very Low	Very Low	Low	Low	Low

7. Penentuan risiko

Tujuan dari tahapan ini adalah untuk mengidentifikasi aset-aset TI yang memiliki dampak risiko yang lebih signifikan terhadap kelancaran proses bisnis di STT Bandung.

Tabel 8. Penentuan Risiko

Kategori Asset	Nama Aset	Kode Aset	Kemungkinan	Dampak	Level
1	Perangkat Virtual Server (Cloud)	SV-01	Sangat Jarang	Besar	Low
		SV-02	Mungkin	Sangat Besar	High
2	Perangkat Keras (Hardware)	HD-01	Jarang	Sedang	Low
		HD-02	Jarang	Sedang	Low
		HD-03	Mungkin	Kecil	Low
		HD-04	Mungkin	Kecil	Low
		HD-05	Mungkin	Kecil	Low
		HD-06	Mungkin	Kecil	Low
		HD-07	Mungkin	Kecil	Low
		HD-08	Mungkin	Kecil	Low
3	Perangkat Lunak (Software)	SW-01	Jarang	Sedang	Low
		SW-02	Jarang	Sedang	Low
		SW-03	Jarang	Sedang	Low
4	Karyawan	SDM-01	Sangat Jarang	Sangat kecil	Very low
		SDM-02	Sangat Jarang	Sangat kecil	Very low
		SDM-03	Sangat Jarang	Sangat kecil	Very low
		SDM-04	Sangat Jarang	Sangat kecil	Very low
		SDM-05	Sangat Jarang	Sangat kecil	Very low
		SDM-06	Sangat Jarang	Sangat kecil	Very low

8. Rekomendasi kontrol

Berikut adalah rekomendasi kontrol yang disarankan untuk mengurangi atau menghilangkan risiko yang telah teridentifikasi pada langkah sebelumnya.

Tabel 9. Rekomendasi Kontrol

No	Sumber Ancaman	Tindakan Ancaman	Rekomendasi Kontrol
1	Hacker, cracker	1. DDoS Attack 2. Deface Website 3. Vulenerability File upload	1. Konfigurasi firewall atau file2ban pada server untuk memfilter lalulintas jaringan masuk dan keluar, blokir otomatis jika ada request loop ke server yang mencurigakan. 2. Melakukan filter input untuk mencegah sql injection atau cross-site-scripting (XSS) 3. Membuat filterisasi extension file atau pembatasan jenis file pada file yang di upload melalui web atau server, hal ini untuk

No	Sumber Ancaman	Tindakan Ancaman	Rekomendasi Kontrol
			menghindari penyerang untuk upload backdoor ke server.
2	Orang dalam (karyawan yang kurang terlatih, tidak puas, berbahaya, lalai, tidak jujur atau dipecat	1. Penyalah gunaan komputer 2. Kecurangan dan pencurian data atau perangkat 3. Penyuapan informasi 4. Input data dipalsukan, data yang rusak 5. Penjualan informasi pribadi 6. Sistem akses yang tidak sah	Melakukan pelatihan terkait kebijakan keamanan sistem informasi kepada seluruh karyawan pengguna sistem, untuk meningkatkan pemahaman terhadap pentingnya keamanan informasi.
3	Serangan Virus Malware	Mencuri data penting yang ada di dalam PC yang terinveksi malware	Melakukan pembaruan dan patch rutin antivirus dan membatasi hak akses pengguna, karyawan hanya boleh memiliki akses ke data dan aplikasi sesuai dengan pekerjaan mereka bisa menggunakan sistem *active directory*.
4	Human Error	1. Konfigurasi instalasi aplikasi pada server yang salah yang dilakukan oleh system administrator 2. Data yang di input ke sistem tidak valid	Melakukan pelatihan tersertifikasi untuk sysadmin, dan menerapkan Principle of least Privilege – PoLP untuk hak akses sysadmin.
5	Pemadaman Listrik	1. Gangguan operasional dan produktivitas TI 2. Kehilangan data dan Kerusakan perangkat keras 3. Rentan terhadap serangan 4. Ketidak mampuan untuk mengakses data	Instalasi sumber daya cadangan (UPS) pada server, dan menyediakan alat genset serta terapkan kebijakan penyimpanan data yang aman. Pastikan data penting secara teratur disimpan dan dilakukan backup dalam kasus pemadaman yang tidak terduga.

No	Sumber Ancaman	Tindakan Ancaman	Rekomendasi Kontrol
		5. Kerusakan perangkat pendingin pada ruang server	
6	Developer yang masih bisa mengakses database production dengan mudah	1. Pencurian data sensitive 2. Perubahan data yang tidak valid jika terjadi kesalahan 3. Pembocoran informasi penting 4. Kegagalan pengamanan	Memberikan least privilege kepada developer, hanya untuk tugas-tugas tertentu yang diperlukan dalam Pengembangan dan pemeliharaan aplikasi. memberikan akses database cloning kepada developer dan melakukan audit Log untuk pemantauan aktivitas audit secara berkala untuk mendeteksi tindakan yang mencurigakan atau tidak sah
7	Single point database failure/Down	1. Kehilangan data karena adanya kegagalan Software package instalasi database 2. Kehilangan data karena human error 3. Tidak siap dalam kasus bencan alam 4. Ketergantungan pada perbaikan manual	Implementasi replikasi database dengan metode master-slave atau cluster, ini akan membantu untuk menjaga ketersediaan data bahkan jika satu server database mengalami gangguan.
8	Debu dan Korosi	1. Hardware Komputer failure error blue screen 2. Processore over heat 3. HDD storage tidak terbaca 4. Data pada PC hilang	Tempatkan komputer pada lingkungan yang bersih, pembersihan atau maintenance komputer yang rutin dan kontrol kelembaban udara pada ruangan.
9	Kesalahan fungsional pada perangkat lunak (Software)	Software yang sedang digunakan tiba-tiba not responds , over close dan tidak akan bisa di gunakan	Melakukan pembaharuan perangkat lunak yang rutin, patch ulang jika perangkat lunak (software) berlisensi free. Membuat sistem ticketing pelaporan kesalahan (Bug Reporting) untuk pengguna agar bisa lebih cepat di tindak lanjuti.
10	Kebakaran (*Fire*)	Terjadinya konselting listrik yang mengakibatkan terjadi	Memasang sistem berbasis IoT untuk mendeteksi kebakaran secara dini jika ada asap dan panas pada ruangan, dan melakukan pemeliharaan secara rutin

No	Sumber Ancaman	Tindakan Ancaman	Rekomendasi Kontrol
		kebakaran dan kehilangan asset TI yang penting serta akan menggangu proses bisnis yang sedang berlangsung	

3.1 Pembahasan

Hasil yang di dapatkan pada penilaian risiko adalah telah teridentifikasi 20 asset yang terkait dengan Sistem Informasi Akademik (SIAKAD), satu diantaranya mempunyai tingkat risiko yang tinggi (HIGH) jika terjadi sebuah ancaman yaitu asset dengan kode SV-02 (server database), 12 asset mempunyai tingkat risiko Low, 6 asset mempunyai tingkat risiko very low. Untuk asset yang mempunyai tingkat risiko tinggi (HIGH) agar segera membuat keamanan database menggunakan Teknik replikasi database master-slave, untuk menjaga ketersediaan data pada sistem informasi akademik jika terjadi kerusakan hardware atau software dan melakukan pengujian keberfungsian dari Teknik replikasi database. Sedangkan untuk asset yang mempunyai tingkat risiko Low dan very Low risiko tersebut masih bisa di terima, sehingga tidak perlu adanya tindakan.

4. KESIMPULAN

Ancaman yang membahayakan database siakad berdasarkan hasil penilaian risiko yaitu Human Error, Tidak ada aturan yang khusus kepada developer untuk mengakses ke database production, Tidak dikonfigurasi replikasi database, Kesalahan konfigurasi server yang terjadi saat instalasi atau maintenance oleh administrator sistem.

Penilaian risiko dilakukan dengan 8 tahap : identifikasi karakateristik sistem, identifikasi ancaman, identifikasi kerentanan, analisis kontrol, penentuan kemungkinan, analisis dampak, penentuan risiko dan rekomendasi kontrol. hasil dari penilaian risiko ada 20 asset yang terkait dengan system siakad terbagi menjadi 4 kelompok yaitu perangkat lunak(software), perangkat keras(hardware), virtual server (cloud) dan SDM (Sumber Daya Manusia) dan salah satu dari asset tersebut mempunyai tingkat risiko yang tinggi yaitu kode asset SV-02 dengan nama asset server virtual database.

REFERENCES

Christian, H. C., & Sitokdana, M. N. N. (2022). *Analisis Risiko Teknologi Informasi pada BANK ABC Menggunakan Framework ISO 31000*. *9*(1).

Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi dan Informasi*, *12*(2), 106–117. https://doi.org/10.34010/jati.v12i2.6829

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*, *14*(1), 141–151. https://doi.org/10.51903/elkom.v14i1.387

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST SP 800-30r1; 0 ed., p. NIST SP 800-30r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Stoneburner, G., & Goguen, A. (n.d.). *Panduan Manajemen Risiko untuk Sistem Teknologi Informasi*.

Utami, G. C., Supramaji, A. B., & Isnaini, K. N. (2023). *Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018*. *8*(1).