NARATIF : Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika
Vol. 05 No. 02 Desember 2023
P-ISSN: 2656-7377 || E-ISSN: 2714-8467

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

Hena Sulaeman[1], Hadi Prasetyo Utomo[2], Agus Iim Suryana[3]
Program Studi Teknik Informatika [1, 2, 3]
Universitas Langlangbuana[1,2,3]
henasulaeman@sttbandung.ac.id[1,] hadi@informatika.unla.ac.id[2,] pamupus@gmail.com[3]

Abstrak

Seiring dengan perkembangan teknologi banyak kejahatan *cyber* yang sangat meresahkan terhadap data yang ada di suatu organisasi atau perusahaan, hal penting yang harus menjadi *focus* utama terhadap data dan informasi adalah melindungi informasi yang bersifat rahasia agar tidak bocor ke *public* atau segelintir orang yang tidak berkepentingan. Dengan meningkatnya insiden keamanan *cyber* berupa perusakan situs web (*web defacement*), peretasan (*hacking*) dan perangkat lunak berbahaya keamanan informasi harus menjadi fokus utama yang harus di selesaikan terutama di sector pendidikan hal ini merujuk pada Peraturan Sekretaris Jenderal Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Nomor 11 Tahun 2022 tentang Sistem Manajemen Keamanan Informasi pada Sistem Pemerintahan Berbasis Elektronik Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi.

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 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 *Database*, NIST-SP 800-30, *Risk Assesment*

Abstract

With the rapid advancement of technology, numerous cybercrimes have posed significant concerns for the data within organizations or companies. A crucial focal point regarding data and information is to safeguard confidential information, preventing its exposure to the public or unauthorized individuals. As incidents of cyber security breaches like website defacement, hacking, and harmful software continue to increase, information security becomes a primary focus, particularly within the education sector. This aligns with Secretary General Regulation of the Ministry of Education, Culture, Research, and Technology Number 11 of 2022 concerning the Information Security Management System within the Ministry's Electronic Government-Based Systems.

Information security is a set of policies, procedures, technologies, and practices designed to protect, secure, and maintain the confidentiality, integrity, and availability of data and information within an organization. The use of the NIST-SP 800-30 framework as a guide in information security risk management aims to identify, prevent, and manage potential risks that could threaten an organization. Thus, organizations can reduce the likelihood of significant losses. The ultimate goal is to protect the organization's business processes from various security threats, minimize potential losses, and prevent serious disruptions to the systems and information technology used by the organization. This research focuses on the risk assessment of information system assets related to the academic information system (SIAKAD) based on the NIST-SP 800-30 guidelines. The risk assessment aims to identify and evaluate the vulnerability level of Information Technology (IT) assets that can affect business processes. The results of the risk assessment are used as a basis for planning security measures tailored to the identified and recommended risk levels. Thus, this research aims to ensure that the recommended security controls will be effective in reducing the risks associated with IT assets that impact business processes.

Keywords : Database Security, NIST-SP 800-30, Risk Assesment

I. 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 dalam 30 hari terakhir rata-rata 3 ancaman yang pernah terjadi. Melihat 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). 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 diguanakan 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 [1]. 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 [2]. 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 [3]

Dari banyaknya permasalahan yang sudah di jelaskan, munculah ide penelitian yang akan di angkat. Ide penelitian ini akan berfokus pada sistem keamanan pada *database* yang komprehensif yang digunakan pada SIAKAD (Sistem Informasi Akademik) di lingkungan STT Bandung dari ancaman yang beragam. 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 keamanan informasi pada system informasi akademik (SIAKAD) dengan didasari dari hasil penilaian risiko.

II. TINJAUAN PUSTAKA

1. Sistem Informasi

Menurut [4] sistem informasi adalah kegiatan perencanaan dan pengendalian yang terdiri dari manusia dan sumber daya di dalam suatu organisasi yang bertanggung jawab mengumpulkan dan mengolah data untuk menghasilkan informasi yang berguna. Menurut [5] istem informasi adalah suatu sistem yang mendukung operasi, manajemen dalam suatu organisasi dan sudah terintegrasi antara manusia-mesin dan mampu menyediakan informasi yang bermanfaat bagi penggunanya. Berdasarkan beberapa pengertian di atas, penulis menyimpulkan bahwa sistem informasi merujuk pada serangkaian kegiatan dan operasi manajemen yang terdapat di dalam suatu organisasi. Sistem ini melibatkan interaksi antara manusia dan komputer, dengan fokus pada aspek manajerial yang bertujuan untuk menyediakan pelaporan dan informasi yang memiliki manfaat bagi pihak eksternal.

2. Sistem Informasi Akademik

Menurut [6] sistem akademik atau sistem informasi akademik (SIAKAD) adalah suatu kegiatan akademik kampus secara online seperti proses Penerimaan Mahasiswa Baru (PMB), pembuatan jadwal kuliah, pengisian Kartu Studi (KRS), pengisian nilai, perwalian, pengelolaan data dosen dan mahasiswa. Mengacu pada beberapa pengertian di atas, penulis menyimpulkan bahwa sistem informasi akademik merujuk pada rangkaian kegiatan yang terjadi di lingkungan kampus, yang berkaitan dengan pengelolaan data akademik. Tujuan dari sistem ini adalah untuk memberikan bantuan dan kemudahan kepada staf, dosen, dan mahasiswa dalam hal administrasi akademik.

3. Cybercrime

Dikutip dari [7] sebuah Lembaga pencegahan kejahatan di Havana, Kuba pada tahun 1999 dan di Wina, Australia pada tahun 2000, menyebutkan terdapat dau pengertian cybercrime yang terbagi secara garis sempit dan luas. *Cybercrime* dalam arti sempit, yaitu aktivitas mencurigakan ilegal atau melanggar hukum secara langsung menyerang sistem keamanan komputer dan data yang diproses oleh komputer.

4. Teknik Serangan

Menurut [8] ada beberapa Teknik serangan yang biasa dilakukan untuk menyerang sistem keamanan pada *website* yaitu *SQL Injection* adalah penyisipan injeksi *query SQL* melalui inputan data dari client ke aplikasi, *Cross Site Scripting* adalah teknik injeksi dari sisi klien, *Broken Access Control* adalah celah keamanan yang memungkinkan peretas untuk masuk ke Admin *Dashboard* ataupun ke file lain tanpa memerlukan autentikasi terlebih dahulu, menurut [9] *Broken Access Control* aplikasi yang memungkinkan setiap pengguna untuk melihat atau mengedit data sensitif tanpa mengautentikasi terlebih dahulu.

5. Rekomendasi Metode Penilaian Risiko

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 [1].
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 [2].

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 [10] [11]. 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 [12].

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 *framework* 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 [10]. Karena *framework* ini sangat fleksible maka dari itu proses penilaian risiko akan di ambil sesuai dengan kebutuhan pada penelitian. Tahapan penilaian risiko yang diambil yaitu identifikasi karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, menentukan *likelihood*, analisis dampak dan penentuan risiko

III. ANALISIS DAN PERANCANGAN

1. Karakteristik System

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). Asset yang tergolong *hardware* adalah komputer, server dan UPS. Asset yang tergolong *software* adalah Sistem Informasi Akademik, *Online Akademik System* (OASIS), *Elektronic Learning* (*E-learning*). Asset yang tergolong SDM adalah pengguna dari Sistem Informasi Akademik (SIAKAD). Berikut adalah asset yang sudah dikelompokkan berdasarkan penjelasan sebelumnya.

TABEL I.
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

No	Kelompok	Asset	Jumlah	Proses Bisnis	ID Asset
		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 organisasi	HD-03
		PC Pengguna (Staff Perpustakaan)	1	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di organisasi	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 berbagai keperluan administrasi di oraganisasi	HD-06
		PC Pengguna (Staff Admin PDDIKTI)	1	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di organisasi	HD-07
		PC Pengguna (Staff Kemahasiswaan)	1	Karyawan menggunakan komputer untuk berbagai keperluan administrasi di organisasi	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

No	Kelompok	Asset	Jumlah	Proses Bisnis	ID Asset
		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
		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 II.
IDENTIFIKASI ANCAMAN

No	Sumber Ancaman	Motivasi	Tindakan Ancaman	Kode
1	*Hacker, cracker*	1. Tantangan 2. Uang 3. Status Ketenaran	*1. DDoS Attack* *2. Deface Website* *3. Vulenerability File upload*	IA-1
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 3. Rentan terhadap serangan	IA-5

No	Sumber Ancaman	Motivasi	Tindakan Ancaman	Kode
			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 4. Data pada PC hilang	IA-8

No	Sumber Ancaman	Motivasi	Tindakan Ancaman	Kode
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

Dari hasil analisis ancaman yang telah dilakukan, teridentifikasi berbagai kerentanan yang dapat memungkinkan terjadinya ancaman tersebut. Berikut adalah daftar kerentanan yang berhasil diidentifikasi berdasarkan pengamatan terhadap sistem Siakad. Kerentanan tersebut terkait dengan manajemen sistem, yang melibatkan proses pengenalan dan penilaian terhadap potensi kelemahan dalam aspek keamanan secara teknis. Berikut ini adalah daftar kerentanan pada manajemen dalam aspek pengelolaan sistem, yang didasarkan pada hasil diskusi dengan pemangku kepentingan terkait.

TABEL III
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 system	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 di lakukan *Pentesting*	Adanya kelemahan *code* program yang lolos pada saat *launch* ke *production server*	1. *DDoS Attack* 2. *Deface Websit* 3. *Vulenerability File upload*	IK-3

No	Letak *Vulnerability* (kerentanan)	Sumber Ancaman	Aksi Ancaman	Kode
4	Kesalahan pada regulasi di organisasi	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 system	IK-6
7	Rusaknya UPS yang digunakan pada PC server	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 5. Kerusakan perangkat pendingin pada ruang server	IK-7

No	Letak *Vulnerability* (kerentanan)	Sumber Ancaman	Aksi Ancaman	Kode
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* *2.* *Processore over heat* 3. HDD *storage* tidak terbaca 4. Data pada PC hilang	IK-12
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	IK-14

No	Letak *Vulnerability* (kerentanan)	Sumber Ancaman	Aksi Ancaman	Kode
			menggangu proses bisnis yang sedang berlangsung	

4. Hasil Penelitian
   1. Penentuan Risiko

Penentuan tingkat risiko ini mengacu pada peta risiko yang telah dibuat dalam Tabel 3 mengenai Penentuan Tingkat Risiko. Langkah ini penting untuk memandu peneliti dalam memilih kontrol keamanan yang paling sesuai untuk diterapkan pada sistem TI di STT Bandung. Penentuan risiko di dasari dengan peta penentuan risiko sebagai berikut:

TABEL IV
PETA PENENTUAN RISIKO
Sumber : [13]

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*

Berdasarkan hasil dari penilianan risiko yang dilakukan, berikut adalah hasil dari penentuan tingkat level risiko asset TI yang terkait dengan sistem informasi akademik (SIAKAD) yang ada di STT Bandung.

TABEL V
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		SW-01	Jarang	Sedang	*Low*

Kategori Asset	Nama Aset	Kode Aset	Kemungkinan	Dampak	Level
	Perangkat Lunak (*Software*)	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*

2. Rekomendasi Kontrol

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

TABEL VI
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 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	Melakukan pelatihan terkait kebijakan keamanan sistem informasi kepada seluruh karyawan pengguna sistem, untuk meningkatkan pemahaman terhadap pentingnya keamanan informasi.

No	Sumber Ancaman	Tindakan Ancaman	Rekomendasi Kontrol
		6. Sistem akses yang tidak sah	
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 5. Kerusakan perangkat pendingin pada ruang server	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.
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

No	Sumber Ancaman	Tindakan Ancaman	Rekomendasi Kontrol
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 kebakaran dan kehilangan asset TI yang penting serta akan menggangu proses bisnis yang sedang berlangsung	Memasang sistem berbasis IoT untuk mendeteksi kebakaran secara dini jika ada asap dan panas pada ruangan, dan melakukan pemeliharaan secara rutin

IV. KESIMPULAN

Berdasarkan hasil analisis, penilaian risiko, hasil perancangan dan hasil pengujian yang telah di paparkan, maka dapat di tarik kesimpulan sebagai berikut:

1. 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.

2. 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*.

REFERENSI

[1] G. C. Utami, A. B. Supramaji, and K. N. Isnaini, "Penilaian Risiko Keamanan Informasi pada *Website* dengan Metode DREAD dan ISO 27005:2018," vol. 8, no. 1, 2023.
[2] H. C. Christian and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi pada BANK ABC Menggunakan *Framework* ISO 31000," vol. 9, no. 1, 2022.
[3] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems :: recommendations of the National Institute of Standards and Technology," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30, 2002. doi: 10.6028/NIST.SP.800-30.
[4] N. Husin, "Perancangan Sistem Informasi Akademik Berbasis Web pada SDN Jatisampurna X," *J. Esensi Infokom J. Esensi Sist. Inf. Dan Sist. Komput.*, vol. 3, no. 2, pp. 13–17, Feb. 2022, doi: 10.55886/infokom.v3i2.331.
[5] I. Irawan, "PENGEMBANGAN SISTEM INFORMASI AKADEMIK UNIVERSITAS PAHLAWAN TUANKU TAMBUSAI RIAU," *J. Teknol. DAN OPEN SOURCE*, vol. 1, no. 2, pp. 55–66, Dec. 2018, doi: 10.36378/jtos.v1i2.21.
[6] F. Sevima, "Pengertian dan Manfaat Sistem Informasi Akademik Bagi Perguruan Tinggi & Mahasiswa," Sevima. Accessed: Jul. 13, 2023. [Online]. Available: https://sevima.com/manfaat-sistem-informasi-akademik-bagi-perguruan-tinggi-mahasiswa/
[7] D. Chirzah and R. A. Ramadhan, "CYBER WAR: ANCAMAN PADA KEAMANAN NASIONAL," vol. 01, 2023.
[8] N. F. Saragih, "Analisis Keamanan dan Implementasi secure code pada Pengembangan Keamanan *website* fikom-methodist.com Menggunakan Penetration Testing dan CVSS," vol. 7, no. 1, 2023.
[9] K. OWASP, "SQl Injection," OWASP. Accessed: Aug. 14, 2023. [Online]. Available: https://owasp.org/www-community/attacks/SQL_Injection
[10] G. Stoneburner and A. Goguen, "Panduan Manajemen Risiko untuk Sistem Teknologi Informasi".
[11] 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.*, vol. 14, no. 1, pp. 141–151, Jul. 2021, doi: 10.51903/elkom.v14i1.387.
[12] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *J. Teknol. Dan Inf.*, vol. 12, no. 2, pp. 106–117, Sep. 2022, doi: 10.34010/jati.v12i2.6829.
[13] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.