DIFFUSION
JOURNAL OF SYSTEM AND INFORMATION TECHNOLOGY

Volume 5, No. 1, January 2025 P-ISSN: 2809-9028 E-ISSN: 2827-7864

Analisis Manajemen Risiko dan Keamanan Sistem Informasi Akademik Terpadu (SIAT) Universitas Negeri Gorontalo Menggunakan Framework NIST SP 800-30

I Putu Jovano[a*], Indhitya R. Padiku[b], Budiyanto Ahaliki[c]

[abc] Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Gorontalo
Email: [a]putujovano07@gmail.com, [b]indypadiku@ung.ac.id, [c]Budiyanto@ung.ac.id

Abstract

Intergrated Academic Information System (SIAT) is an information system developed by State University of Gorontalo that has been used to simplify academic processes. Developed since 2005, this information system has faced various risks in which their likelihood and impact need to be identified. This study aimed to ascertain means of risk and security management analysis of Intergrated Academic Information System (SIAT) in State University of Gorontalo using NIST SP 800-30. This study used qualitative analysis technique with descriptive approach. The results of this study disclosed that: (1) 4 moderate level risk, 12 low level risk, and 10 very low level risk has been discovered, the four moderate risks are: phising attacks, the sending of malware to the information system, the exploit of zero-day attacks, and brute-force attacks (2) The exploit of zero-day attacks, and brute-force attacks have very high likelihood; phising attacks and the sending of malware to the information system have high likelihood. These four risks have moderate level impact, (3) the proposed risk control recommendations are: providing training, counseling, socialization related to IT Security to SIAT' personnel/admins to prevent phising and malware attacks, providing informations about links that potentially be a phising links in SIAT main page, performing security assessment periodically, performing log activity checking periodically to detect anomaly activities, reducing the wrong password inputs limits to three, and locking the user's account if the login attempt has exceed the limit.

Keywords : *Risk and Security Management Analysis*; *NIST SP 800-30*; *Intergrated Academic Information System*; *Risk*.

Abstrak

Sistem Informasi Akademik Terpadu (SIAT) merupakan sistem informasi yang dikembangkan oleh Universitas Negeri Gorontalo yang digunakan untuk mempermudah proses bidang akademik. Sejak dikembangkannya SIAT sejak 2005, sistem informasi ini menghadapi berbagai risiko yang perlu diidentifikasi kemungkinan terjadi dan dampak dari risiko tersebut. Penelitian ini bertujuan untuk mengetahui cara analisis manajemen risiko dan keamanan Sistem Informasi Akademik Terpadu (SIAT) menggunakan NIST SP 800-30. Penelitian ini menggunakan Teknik kualitatif dengan pendekatan deskriptif. Hasil penelitian ini menunjukkan bahwa: (1) ditemukan 4 risiko dengan tingkat risiko menengah, 12 risiko dengan tingkat risiko rendah, dan 10 risiko dengan tingkat risiko sangat rendah, 4 risiko menengah tersebut berupa adanya serangan phishing, pengiriman malware ke dalam sistem informasi organisasi, dimanfaatkannya kelemahan menggunakan zero-day attack, dan Serangan percobaan login brute force. (2) dimanfaatkannya kelemahan menggunakan zero-day attack, dan Serangan percobaan login brute force memiliki kemungkinan yang sangat tinggi; dan adanya serangan phishing, dan pengiriman malware ke dalam sistem informasi organisasi memiliki kemungkinan yang tinggi. Keempat risiko memiliki tingkat dampak menengah (3) peneliti merekomendasikan kontrol risiko berupa memberikan pelatihan, penyuluhan, atau sosialiasi terkait keamanan TI kepada personil/admin SIAT untuk mencegah serangan phishing dan malware, menyediakan informasi terkait tautan yang berpotensi phishing pada halaman utama SIAT, melakukan asesmen keamanan SIAT secara berkala, melakukan pengecekan log aktivitas secara

berkala untuk pendeteksian aktivitas anomali, memperkecil batas kesalahan penginputan password menjadi 3, dan mengunci akun pengguna jika percobaan login melewati batas.

Kata kunci : Analisis manajemen risiko dan keamanan, NIST SP 800-30, Sistem Informasi Akademik Terpadu, Risiko.

1. **Pendahuluan**

Dalam menjalankan suatu sistem informasi, integritas, kerahasiaan, dan ketersediaan data serta informasi sangat diperlukan. Adanya gangguan ataupun kelemahan terkait ketiga hal tersebut dapat sangat berdampak pada berjalannya. Sistem informasi akademik seperti SIAT tak terhindar dari risiko ini.

Pada lembaga pendidikan Universitas Negeri Gorontalo, sekarang ini hampir semua pekerjaan yang berkaitan dengan bidang akademik sudah menggunakan sistem informasi berupa Sistem Informasi Akademik Terpadu (SIAT) dalam membantu pekerjaan. Penggunaan sistem informasi dalam melakukan pekerjaan ini berakibat pada ketergantungan sehingga adanya risiko dan ancaman keamanan dapat menggangu berjalannya kegiatan akademik sehingga perlu dilakukan analisis manajemen risiko dan keamanan.

Menurut Latifiana (Muharam, R. 2022) Risiko adalah sebuah kemungkinan kejadian atau peristiwa yang merugikan perusahaan atau bisnis, dimana kejadian tersebut tidak dapat diprediksi. Menurut Djohanputro (Binus University Business School, 2020) Manajemen resiko adalah proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan risiko dan memonitor dan mengendalikan penanganan risiko. Menurut Zakiyul (2019). Keamanan merupakan topik yang berhubungan kepada kejahatan, segala bentuk kecelakaan, dan lain-lain. Menurut IBM (2020) manajemen risiko merupakan proses mengidentifikasi, menilai, dan mengontrol keuangan, legalitas, strategi, dan risiko keamanan terhadap kapita dan pendapatan organisasi. Ancaman atau risiko tersebut dapat berakar dari berbagai sumber, seperti ketidakpastian finansial, kelabilan legalitasm kesalahan strategi manajemen, kecelakaan, dan bencana alam.

Menurut NIST (2012), NIST (*National Institute of Standarts and Technology*) SP (Special Publication) 800-30 adalah kerangka kerja manajemen risiko untuk sistem informasi yang terstandarisasi oleh pemerintah amerika serikat. Kerangka kerja ini bertujuan sebagai alat (tool) yang digunakan dalam asesmen atau penilaian risiko dalam sebuah sistem informasi yang kemudian dapat menjadi sumber data dan informasi dalam melakukan analisis manajemen risiko yang kemudian dapat menjadi acuan dalam penyusunan strategi dalam menghadapi risiko tersebut.

NIST SP 800-30 telah banyak digunakan telah banyak digunakan pada penelitian sebelumnya untuk menganalisis manajemen risiko dan keamanan pada suatu sistem informasi, Diantaranya adalah penelitian yang dilakukan oleh Elanda & Buana (2021), penelitian oleh Murniati, dkk (2021), dan penelitian oleh Wahdah, dan Soewito (2022).

2. **Metode**

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif. Menurut Fai (2022), metode penelitian kualitatif adalah sebuah cara atau metode penelitian yang lebih menekankan analisa atau deskriptif. Dalam sebuah proses penelitian kualitatif hal hal yang bersifat perspektif subjek lebih ditonjolkan dan andasan teori

dimanfaatkan oleh peneliti sebagai pemandu, agar proses penelitian sesuai dengan fakta yang ditemui di lapangan ketika melakukan penelitian. Menurut Nana dan Sukmadinata (2006), penelitian deskriptif adalah suatu bentuk penelitian yang ditujukan untuk mendeskripsikan fenomena-fenomena yang ada, baik fenomena alamiah maupun fenomena buatan manusia. Fenomena itu bisa berupa bentuk, aktivitas, karakteristik, perubahan, hubungan, kesamaan, dan perbedaan antara fenomena yang satu dengan fenomena yang lainnya. Metode penelitian kualitatif dengan pendekatan deskriptif ini bertujuan untuk menganalisis manajemen risiko dan keamanan Sistem Informasi Akademik Terpadu (SIAT) menggunakan framework NIST SP 800-30. Sumber data primer pada penelitian ini adalah wawancara dan observasi terhadap pengelola SIAT di Biro Akademik Kemahasiswaan dan Perencanaan, dan sumber data sekunder pada penelitian ini adalah studi kepustakaan, dokumentasi, buku, dan majalah, koran, serta arsip tertulis yang berhubungan dengan objek yang akan di teliti pada penelitian ini.

3. Hasil dan Pembahasan

3.1 System Characterization

Perangkat keras, perangkat lunak, data dan informasi serta sumber daya manusia merupakan komponen krusial dari berjalannya SIAT Universitas Negeri Gorontalo, perangkat keras yang digunakan berupa PC untuk pengelola SIAT yang berupa Badan Pengelola Usaha, serta PC atau laptop bagi admin jurusan dari setiap fakultas. Sistem SIAT dihosting dan dikembangkan menggunakan layanan Google Cloud di region Jakarta (asia-southeast2). Layanan Google Cloud yang digunakan oleh SIAT adalah:

1) Compute Engine: SIAT menggunakan compute engine series E2. Menurut Google Cloud (2024), Compute series jenis ini 0,25 hingga 32 virtual core (vCPU) dengan memori hingga 128 GB dengan maksimal 8 GB per vCPU, prosesor yang digunakan adalah prosesor Intel atau prosesor AMD EPYC™ Rome generasi kedua.
2) Cloud Run: SIAT menggunakan layanan Cloud Run untuk menjalankan layanan front-end dan back-end, tugas batch, hosting LLM, dan workload pemrosesan antrian tanpa memerlukan infrastruktur TI tambahan sehingga pengelolaan SIAT menjadi lebih fleksibel.
3) Cloud Storage: Menurut Google Cloud (2024), Cloud Storage menyediakan layanan penyimpanan tak terbatas dengan akses tanpa batas, penyimpanan data tanpa adanya ukuran objek minimum, aksesibilitas dan lokasi penyimpanan diseluruh dunia, latensi rendah (time to first byte dalam puluhan milidetik), Ketahanan tinggi (ketahanan tahunan sebesar 99,999999999%), Redundan di seluruh region jika data disimpan dalam multi-region atau dual-region, dan Pengalaman yang setara dengan fitur, keamanan, alat, dan API Cloud Storage.
4) Cloud Build: Google Build digunakan oleh pengelola SIAT untuk pengembangan, pengujian dan deploy pada platform CI/CD serverless Google Cloud menggunakan Google Cloud Compute Engine.
5) Cloud Deploy: Menurut Google Cloud (2024), Cloud Deploy adalah layanan terkelola yang mengotomatiskan pengiriman aplikasi ke serangkaian lingkungan target dalam urutan promosi yang ditentukan. Jika ingin men-deploy aplikasi yang telah di-update, pengguna harus membuat release, yang lifecycle-nya dikelola oleh pipeline pengiriman.

3.2 Threat Identification

Ancaman yang dihadapi oleh SIAT dinilai berdasarkan amcaman, sumber ancaman, dan relevansi dari ancaman tersebut terhadap SIAT.

Setelah dilakukan wawancara terhadap pengelola SIAT dan observasi pada SIAT, sumber ancaman adversarial dan ancaman non-adversarial yang dapat mengganggu berjalannya SIAT telah teridentifikasi, yaitu *hacker*, orang dalam, dan pencurian sebagai sumber ancaman *adversarial,* dan ketidaksengajaan personil, gangguan sinyal, *server error*, kurangnya pemeliharaan *hardware*, suhu dan voltase tidak stabil, *server* tidak dapat menyanggupi permintaan akses, kehilangan data, manajemen password buruk, tidak adanya kebijakan pengaturan hak akses *hardware*, dan bencana Alam

Berdasarkan identifikasi tersebut, diketahui *event* ancaman yang dapat dihadapi SIAT, yaitu: pemantauan atau pemindaian perimeter jaringan, pemantauan menggunakan *malware*, serangan *phising*, pengiriman *malware* ke dalam sistem informasi organisasi, dimasukkannya perangkat keras palsu atau rusak ke rantai persediaan, dimanfaatkannya akses fisik dari pegawai berijin untuk mendapatkan akses ke fasilitas organisasi, dimanfaatkannya kelemahan menggunakan zero-day attack, serangan *Distributed Denial of Service* (*DDoS*), serangan percobaan *login brute force*, serangan yang menargetkan perangkat pribadi dari pegawai penting, adanya pencurian hardware yang terdapat pada situs TI, pencurian hardware yang digunakan pengelola namun tidak berlokasi di situs TI, dan didapatkannya akses tanpa ijin sebagai *event* ancaman *adversarial;* dan kebocoran informasi sensitive, kesalahan penginputan data, kerusakan *hardware* akibat suhu tidak stabil, kerusakan *hardware* akibat voltase tidak stabil, kerusakan *hardware* akibat usia, *hardware* yang digunakan tidak mampu menyanggupi kinerja yang diharapkan, *website* SIAT tidak dapat diakses, terjadi kehilangan data akun pengguna (*username* dan *password*), terjadi kehilangan data akademik, jeda pergantian *password* terlalu lama, pegawai tidak berwenang dapat menggunakan *hardware* pengelola SIAT, kesalahan pemberian hak akses pengguna, dan terjadi bencana alam pada fasilitas TI sebagai *event* ancaman non *adversarial*.

3.3 Vurnerability Identification

Setelah dilakukan pengumpulan data berupa wawancara terhadap pihak pengelola SIAT dan observasi pada SIAT, ditemukan beberapa kelemahan atau kerentanan yang dihadapi oleh SIAT. Kelemahan ini dapat dimanfaatkan oleh sumber ancaman adversarial atau dapat memperparah ancaman yang disebabkan non-adversarial. Kelemahan SIAT yang telah teridentifikasi adalah: media penyimpanan data kurang memadai, *hardware* rentan terhadap suhu tinggi, *hardware* rentan terhadap voltase tidak stabil, kurangnya mekanisme otentikasi pengguna, batas kesalahan penginputan *password* terlalu tinggi, tidak adanya *server backup*, kurangnya perlindungan fisik pada situs TI (Gedung, pintu, atau jendela), manajemen kabel yang buruk, ketidakhadiran pegawai/admin saat dibutuhkan, kurangnya prosedur formal untuk penghapusan akun pengguna, kurangnya audit berkala, tidak adanya dokumentasi terhadap perubahan yang dilakukan pengelola terhadap SIAT, kurangnya mekanisme pemantauan yang diterapkan, dan kurangnya mekanisme pelaporan kelemahan keamanan secara formal. Kelemahan-kelemahan ini berpotensi untuk mengganggu integritas informasi dan operasional SIAT.

3.4 Control Analysis

Berdasarkan hasil observasi dan wawancara kepada pengelola SIAT, dilakukan identifikasi kontrol risiko yang dilakukan oleh pengelola SIAT untuk mengatasi atau memitigasi ancaman yang dihadapi oleh SIAT. Tindakan control risiko yang dilakukan adalah: penanganan oleh personal *network security*, penyesuaian kriteria rekrutmen pegawai yang memadai terkait *cybersecurity*, pencatatan inventaris, adanya pengawasan personil *security* dan *CCTV* pada situs TI, penambahan penyimpanan *cloud*, pengawasan melalui *log* aktivitas, penggantian atau pemeliharaan *hardware*, penanganan oleh personil pengelola, pemulihan data, kriteria *password* yang rumit, evakuasi *hardware* pada situs TI, dan pemanggilan personil melalui kontak yang dimiliki pengelola.

3.5 Likelihood Identification

Pada tahap ini dilakukan identifikasi kemungkinan event ancaman yang telah teridentifikasi pada SIAT berdasarkan kemungkinan terjadinya event ancaman dan kemungkinan adanya dampak kerugian yang disebabkan oleh event ancaman tersebut. Berikut adalah identifikasi kemungkinan dari event ancaman SIAT:

Tabel 1. Keseluruhan kemungkinan *event* ancaman

No.	*Event* ancaman	Keseluruhan Kemungkinan
Adversarial		
1.	Pemantauan atau pemindaian perimeter jaringan	Sangat Rendah
2.	Pemantauan menggunakan malware	Sangat Rendah
3.	Serangan phising	Tinggi
4.	Pengiriman malware ke dalam sistem informasi organisasi	Rendah
5.	Dimasukkannya perangkat keras palsu atau rusak ke rantai persediaan	Rendah
6.	Dimanfaatkannya akses fisik dari pegawai berijin untuk mendapatkan akses ke fasilitas organisasi	Sangat Rendah
7.	Dimanfaatkannya kelemahan menggunakan *zero-day attack*	Menengah
8.	Serangan Distributed Denial of Service (DDoS)	Sangat Tinggi
9.	Serangan percobaan login brute force	Sangat Tinggi
10.	Serangan yang menargetkan perangkat pribadi dari pegawai penting	Menengah
11.	Adanya pencurian hardware yang terdapat pada situs TI	Rendah
12.	Pencurian hardware yang digunakan pengelola namun tidak berlokasi di situs TI (Contoh: Laptop atau smartphone)	Rendah
13.	Didapatkannya akses tanpa ijin	Rendah
Non-Adversarial		
1.	Kebocoran informasi sensitif	Rendah
2.	Kesalahan penginputan data	Rendah
3.	Kerusakan hardware akibat suhu tidak stabil	Sangat Rendah
4.	Kerusakan hardware akibat voltase tidak stabil	Sangat Rendah
5.	Kerusakan hardware akibat usia	Sangat Rendah
6.	Hardware yang digunakan tidak mampu menyanggupi permintaan yang diharapkan	Menengah
7.	*Website* SIAT tidak dapat diakses	Rendah
8.	Terjadi kehilangan data akun pengguna (*username* dan *password*)	Rendah
9.	Terjadi kehilangan data akademik	Rendah
10.	Jeda pergantian *password* terlalu lama	Rendah
11.	Pegawai tidak berwenang dapat menggunakan *hardware* pengelola SIAT	Rendah

12.	Kesalahan pemberian hak akses pengguna	Rendah
13.	Terjadi bencana alam pada fasilitas TI	Rendah

Teridentifikasi 2 event ancaman dengan kemungkinan sangat tinggi, 1 event ancaman dengan kemungkinan tinggi, 3 event ancaman dengan kemungkinan menengah, 14 event ancaman dengan kemungkinan rendah, dan 6 event ancaman dengan kemungkinan sangat rendah yang dihadapi oleh SIAT.

3.6 Impact Analysis

Pada tahap ini dilakukan analisis dampak dari event ancaman yang telah teridentifikasi pada SIAT berdasarkan asset yang terdampak oleh event ancaman dan besarnya dampak yang disebabkan oleh event ancaman tersebut. Berikut adalah hasil analisis dampak dari event ancaman SIAT. Berikut adalah identifikasi dampak event ancaman SIAT:

Tabel 2. Identifikasi dampak *event* ancaman SIAT

No.	*Event* ancaman	Aset yang terdampak	Besarnya Dampak
Adversarial			
1.	Pemantauan atau pemindaian perimeter jaringan	Kerugian terhadap operasi	Sangat Rendah
2.	Pemantauan menggunakan malware	Kerugian terhadap operasi	Rendah
3.	Serangan phising	Kerugian terhadap operasi	Menengah
4.	Pengiriman malware ke dalam sistem informasi organisasi	Kerugian terhadap operasi	Menengah
5.	Dimasukkannya perangkat keras palsu atau rusak ke rantai persediaan	Kerugian terhadap operasi, kerugian pada aset	Rendah
6.	Dimanfaatkannya akses fisik dari pegawai berijin untuk mendapatkan akses ke fasilitas organisasi	Kerugian terhadap operasi	Rendah
7.	Dimanfaatkannya kelemahan menggunakan *zero-day attack*	Kerugian terhadap operasi	Menengah
8.	Serangan Distributed Denial of Service (DDoS)	Kerugian terhadap operasi	Rendah
9.	Serangan percobaan login brute force	Kerugian terhadap operasi	Menengah
10.	Serangan yang menargetkan perangkat pribadi dari pegawai penting	Kerugian terhadap operasi	Rendah
11.	Adanya pencurian hardware yang terdapat pada situs TI	Kerugian pada aset	Menengah
12.	Pencurian hardware yang digunakan pengelola namun tidak berlokasi di situs TI (Contoh: Laptop atau smartphone)	Kerugian pada aset	Menengah
13.	Didapatkannya akses tanpa ijin	Kerugian terhadap operasi	Rendah
Non-Adversarial			
14.	Kebocoran informasi sensitif	Kerugian terhadap operasi	Rendah
15.	Kesalahan penginputan data	Kerugian terhadap operasi	Sangat Rendah
16.	Kerusakan hardware akibat suhu tidak stabil	Kerugian pada aset	Sangat Rendah
17.	Kerusakan hardware akibat voltase tidak stabil	Kerugian pada aset	Sangat Rendah
18.	Kerusakan hardware akibat usia	Kerugian pada aset	Sangat Rendah
19.	Hardware yang digunakan tidak mampu menyanggupi permintaan yang diharapkan	Kerugian terhadap operasi	Sangat Rendah
20.	*Website* SIAT tidak dapat diakses	Kerugian terhadap operasi	Rendah

21.	Terjadi kehilangan data akun pengguna (*username* dan *password*)	Kerugian terhadap operasi	Rendah
22.	Terjadi kehilangan data akademik	Kerugian terhadap operasi	Rendah
23.	Jeda pergantian *password* terlalu lama	Kerugian terhadap operasi	Rendah
24.	Pegawai tidak berwenang dapat menggunakan *hardware* pengelola SIAT	Kerugian terhadap operasi	Rendah
25.	Kesalahan pemberian hak akses pengguna	Kerugian terhadap operasi	Sangat Rendah
26.	Terjadi bencana alam pada fasilitas TI	Kerugian terhadap operasi, kerugian terhadap aset	Sangat Rendah

3.7 Risk Determination

Berdasarkan hasil pengukuran kemungkinan dan dampak yang ditimbulkan dari terjadinya event ancaman, berikut adalah hasil penilaian risiko dari event ancaman yang dihadapi oleh SIAT:

Tabel 3. Hasil penilaian risiko SIAT

No.	***Event* ancaman**	**Tingkat Risiko**
Adversarial		
1.	Pemantauan atau pemindaian perimeter jaringan	Sangat Rendah
2.	Pemantauan menggunakan malware	Sangat Rendah
3.	Serangan phising	Menengah
4.	Pengiriman malware ke dalam sistem informasi organisasi	Menengah
5.	Dimasukkannya perangkat keras palsu atau rusak ke rantai persediaan	Rendah
6.	Dimanfaatkannya akses fisik dari pegawai berijin untuk mendapatkan akses ke fasilitas organisasi	Sangat Rendah
7.	Dimanfaatkannya kelemahan menggunakan *zero-day attack*	Menengah
8.	Serangan Distributed Denial of Service (DDoS)	Rendah
9.	Serangan percobaan login brute force	Menengah
10.	Serangan yang menargetkan perangkat pribadi dari pegawai penting	Rendah
11.	Adanya pencurian hardware yang terdapat pada situs TI	Rendah
12.	Pencurian hardware yang digunakan pengelola namun tidak berlokasi di situs TI (Contoh: Laptop atau smartphone)	Rendah
13.	Didapatkannya akses tanpa ijin	Rendah
Non-Adversarial		
14.	Kebocoran informasi sensitif	Rendah
15.	Kesalahan penginputan data	Sangat Rendah
16.	Kerusakan hardware akibat suhu tidak stabil	Sangat Rendah
17.	Kerusakan hardware akibat voltase tidak stabil	Sangat Rendah
18.	Kerusakan hardware akibat usia	Sangat Rendah
19.	Hardware yang digunakan tidak mampu menyanggupi permintaan yang diharapkan	Sangat Rendah
20.	*Website* SIAT tidak dapat diakses	Rendah
21.	Terjadi kehilangan data akun pengguna (*username* dan *password*)	Rendah
22.	Terjadi kehilangan data akademik	Rendah
23.	Jeda pergantian *password* terlalu lama	Rendah
24.	Pegawai tidak berwenang dapat menggunakan *hardware* pengelola SIAT	Rendah

25.	Kesalahan pemberian hak akses pengguna	Sangat Rendah
26.	Terjadi bencana alam pada fasilitas TI	Sangat Rendah

Berdasarkan hasil penilaian risiko yang dihadapi SIAT, diketahui bahwa terdapat 4 risiko dengan tingkat risiko menengah, 12 risiko dengan tingkat risiko rendah, dan 10 risiko dengan tingkat risiko sangat rendah.

3.8 Control Reccomendation

Berdasarkan hasil analisis risiko yang telah dilakukan, hanya terdapat 4 risiko dengan tingkat risiko menengah dan tidak ada risiko dengan tingkat risiko diatas menengah, hal ini menunjukkan efektifitas manajemen risiko dan keamanan SIAT. Berikut adalah rekomendasi kontrol terhadap risiko yang dihadapi SIAT:

Tabel 4. Rekomendasi kontrol risiko

No.	Risiko	Tingkat Risiko	Rekomendasi Kontrol
1.	Adanya serangan *phishing*	Menengah	1. Memberikan pelatihan, penyuluhan, atau sosialiasi terkait keamanan TI kepada personil/admin SIAT untuk mencegah serangan *phising*. 2. Menyediakan informasi terkait tautan yang berpotensi *phishing* pada halaman utama SIAT.
2.	Pengiriman malware ke dalam sistem informasi organisasi	Menengah	Memberikan pelatihan, penyuluhan, atau sosialisasi terkait keamanan TI kepada personil/admin SIAT untuk mencegah serangan *malware*.
3.	Dimanfaatkannya kelemahan menggunakan *zero-day attack*	Menengah	1. Melakukan asesmen keamanan SIAT secara berkala. 2. Melakukan pengecekan *log* aktivitas secara berkala untuk pendeteksian aktivitas anomali.
4.	Serangan percobaan login brute force	Menengah	1. Memperkecil batas kesalahan penginputan *password* menjadi 3. 2. Mengunci akun pengguna jika percobaan *login* melewati batas.

4. Kesimpulan

Setelah dilakukan analisis risiko dan keamanan terhadap SIAT, ditemukan 4 risiko dengan tingkat risiko menengah, 12 risiko dengan tingkat risiko rendah, dan 10 risiko

dengan tingkat risiko sangat rendah, empat risiko menengah tersebut berupa adanya serangan phishing, pengiriman malware ke dalam sistem informasi organisasi, dimanfaatkannya kelemahan menggunakan zero-day attack, dan Serangan percobaan login brute force.

Berdasarkan hasil analisis, dimanfaatkannya kelemahan menggunakan zero-day attack, dan Serangan percobaan login brute force memiliki kemungkinan yang sangat tinggi (adversarial hampir dipastikan melakukan serangan); dan adanya serangan phishing, dan pengiriman malware ke dalam sistem informasi organisasi memiliki kemungkinan yang tinggi (adversarial berkemungkinan untuk melakukan serangan). Keempat risiko memiliki tingkat dampak menengah (Event ancaman diperkirakan dapat berdampak serius terhadap operasi SIAT).

Setelah dilakukan analisis risiko, peneliti merekomendasikan kontrol risiko berupa memberikan pelatihan, penyuluhan, atau sosialiasi terkait keamanan TI kepada personil/admin SIAT untuk mencegah serangan phishing dan malware, menyediakan informasi terkait tautan yang berpotensi phishing pada halaman utama SIAT, melakukan asesmen keamanan SIAT secara berkala, melakukan pengecekan log aktivitas secara berkala untuk pendeteksian aktivitas anomali, memperkecil batas kesalahan penginputan password menjadi 3, dan mengunci akun pengguna jika percobaan login melewati batas.

Hasil dari analisi ini adalah peneliti menyimpulkan bahwa penerapan manajemen risiko dan keamanan Sistem Informasi Akademik Terpadu (SIAT) Universitas Negeri Gorontalo telah berjalan dengan baik, namun diharapkan dapat meningkatkan kualitas keamanan sistem yang sudah ada.

Ucapan Terima Kasih

Ucapan terima kasih kepada Ibu Indhytia R. Padiku, S.Kom., M.Kom selaku Ketua Jurusan Teknik Informatika dan Pembimbing I, Bapak Muchlis Polin, S.Kom., M.Kom selaku Ketua Program Studi Sistem Informasi, dan Budiyanto Ahaliki, S.Si, M.Kom Pembimbing II yang telah memberikan arahan serta saran untuk kesempurnaan penelitian ini.

Daftar Pustaka

Binus University Business School. (2020). Definisi Manajemen Risiko, dalam https://bbs.binus.ac.id/business-creation/2020/04/definisi-manajemen-risiko/, diakses pada 17 agustus 2023.

Fai. (2022). Metode Penelitian Kualitatif Adalah, dalam https://umsu.ac.id/metode-penelitian-kualitatif adalah/#:~:text=Metode%20Penelitian%20Kualitatif%20Adalah&text=Metode%20kualitatif%20lebih%20mengutamakan%20pengamatan,kata%20dan%20kalimat%20yang%20digunakan, diakses pada 30 Juli 2023.

Google Cloud. (2024). Compute Engine | Google Cloud., dalam https://cloud.google.com/products/compute?hl=en, diakses pada 1 september 2024.

IBM. (2020). Why is risk management important, dalam https://www.ibm.com/topics/risk-management, diakses pada 17 agustus 2023.

Muharam, R. (2022). Analisis Penerapan Audit Internal Berbasis Risiko Dengan Mengadopsi ISO 27001 dan COBIT 5 (studi kasus pada industry Business Process Outsourcing PT Metis). Tesis. Jakarta: Universitas Nasional.

Nana, dan Sukmadinata, S. (2006). Landasan Psikologi Proses Pendidikan, Bandung: PT. Remaja Rosdakarya.

National Institute of Standards and Technology. (2012). NIST Special Publication 800-30. Gaithensburg: National Institute of Standards and Technology.

Zakiyul, F. (2019). Tinjauan Terhadap Peranan Stasiun Meteorologi Dalam Menunjang Program Keselamatan Dan Keamanan Pelayaran Di Wilayah Kerja Pelabuhan Tanjung Mas Semarang. Karya Tulis. Semarang: Universitas Maritim AMNI.