

MANAJEMEN RISIKO PENERAPAN TEKNOLOGI INFORMASI PADA UNIVERSITAS BINA DARMA

Susanti¹, Dedy Syamsuar², Yesi Novaria Kunang³

Program Pascasarjana
Universitas Bina Darma

email : ¹susanti.harun12@gmail.com, ²dedy_syamsuar@binadarma.ac.id,
³yesinovariakunang@binadarma.ac.id

Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstrak

Hampir semua organisasi menggunakan Teknologi Informasi untuk menjalankan bisnisnya. Dengan menerapkan teknologi informasi diharapkan mampu meningkatkan efisiensi dan efektifitas dari kegiatan bisnis. Selain memberikan manfaat tentunya tidak bisa di pungkiri penerapan teknologi rentan terhadap risiko yang merugikan yang dapat mengganggu keberlangsungan proses bisnis bersangkutan begitu pula dengan penerapan teknologi informasi di perguruan tinggi. Maka dari itu, penelitian ini dilakukan untuk mengidentifikasi risiko yang mungkin terjadi pada Sistem Informasi Akademik (SISFO) dengan menggunakan metode *Octave Allegro* di Universitas Bina Darma. Data di peroleh dengan cara wawancara terhadap informan penelitian yang di anggap mengetahui objek penelitian. Hasil penelitian menunjukkan bahwa terdapat 3 area dampak risiko yaitu reputasi universitas, kepercayaan pengguna dan biaya operasional, serta terdapat 5 area yang menjadi perhatian ancaman pada Sistem Informasi Akademik (SISFO). Diantara 5 skenario ancaman tersebut terdapat 1 area dengan kemungkinan terjadi tinggi dengan skor risiko relatif yang tinggi juga yaitu ketersediaan data yang sering terganggu akibat mati lampu dan jaringan terputus. Pendekatan mitigasi yang dilakukan yaitu membuat redundan link internet dan meletakkan sistem di *cloud* (membuat *Secondary Server*). Hal ini diharapkan dapat mengurangi peluang terjadinya risiko terhadap ketersediaan data sistem informasi akademik (SISFO).

Kata Kunci : *Octave Allegro*, Sistem Informasi Akademik

1 PENDAHULUAN

Pada saat ini perkembangan Teknologi Informasi sedang menunjukkan kekuatannya. Hampir semua organisasi menggunakan Teknologi Informasi untuk menjalankan bisnisnya. Dengan menerapkan teknologi informasi diharapkan mampu meningkatkan efisiensi dan efektifitas dari kegiatan bisnis tersebut. Efisiensi dan efektifitas kerja menjadi hal utama yang harus diterapkan sebagai indikasi keberhasilan penerapan Teknologi Informasi di dalam perusahaan/organisasi tersebut. Penerapan Teknologi Informasi tentunya akan sangat bermanfaat apabila sesuai dengan visi, misi dan strategi perusahaan. Tujuan jangka panjang perusahaan menerapkan Teknologi Informasi adalah mampu bersaing di dalam dunia bisnis, begitu juga dengan perguruan tinggi yang memanfaatkan Teknologi Informasi (Nasution and Sari, 2014).

Perguruan tinggi merupakan sebuah institusi dengan salah satu tugas yang diembannya adalah memberikan pelayanan kepada masyarakat untuk menyiapkan Sumber Daya Manusia (SDM) dengan masa depan yang bermutu dan berdaya guna. Aktivitas utama dalam perguruan tinggi sesuai dengan fungsi utamanya yaitu sebagai penyelenggara pendidikan adalah layanan akademik. Dalam pelaksanaan layanan akademik ini perlu adanya penggunaan Teknologi informasi yang dapat mendukung tercapainya sasaran dari layanan akademik tersebut

(Jusuf, 2009). Hal ini juga berlaku penerapan teknologi informasi pada layanan akademik di Universitas Bina Darma yaitu Sistem Informasi Akademik (SISFO).

Sistem Informasi Akademik (SISFO) Universitas Bina Darma adalah salah satu aplikasi *web* yang digunakan untuk mendukung kegiatan operasional pendidikan, bukan hanya pelayanan terhadap mahasiswa yang menjadi lebih baik tetapi juga pelayanan untuk seluruh pihak terkait. Berdasarkan peranan sistem informasi akademik ini tidak bisa dipungkiri bahwa ketergantungan terhadap teknologi informasi sangat tinggi, hanya saja penerapan Teknologi Informasi pada suatu Perguruan Tinggi tidak selalu berjalan sesuai yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan Perguruan Tinggi.

Penelitian mengenai risiko teknologi informasi sudah pernah dilakukan sebelumnya oleh Jakaria and Dirgahayu (2013) yang menunjukkan bahwa beberapa sistem informasi beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (*natural disaster*), pencurian (*theft*), kebakaran (*fires*), lonjakan listrik (*power surge*) dan perusakan (*vandalism*). Risiko kerusakan logik mengacu kepada akses tidak sah (*unauthorized access*), kerusakan secara sengaja maupun tidak disengaja pada sistem informasi dan data untuk itu perlu dilakukan identifikasi ancaman dan analisis risiko untuk meningkatkan keamanan dan mengurangi risiko kerusakan sistem informasi. Dari penelitian sebelumnya, hampir semua sistem informasi dalam suatu organisasi rentan terhadap risiko yang merugikan yang dapat mengganggu keberlangsungan proses bisnis yang bersangkutan. Maka dari itu, Sistem Informasi Akademik (SISFO) di Universitas Bina Darma juga perlu melakukan manajemen risiko untuk mengetahui risiko apa saja yang mungkin bisa terjadi dan melakukan penilaian terhadap risiko serta penanganan terhadap risiko tersebut.

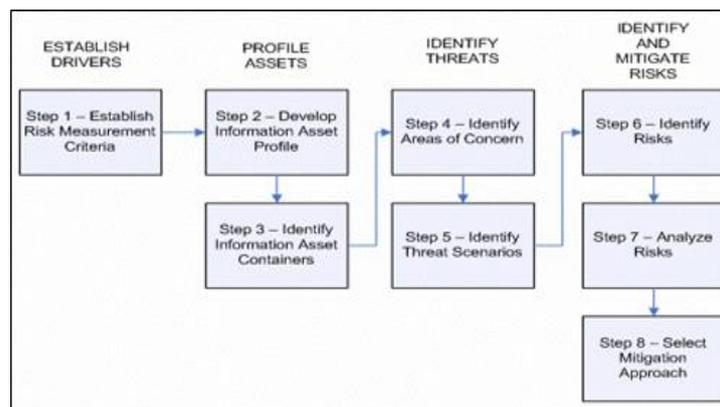
2 METODOLOGI PENELITIAN

Penelitian ini menggunakan metode *octave allegro* untuk mengidentifikasi risiko apa saja yang mungkin bisa terjadi dan melakukan pengukuran terhadap risiko tersebut serta penanganan terhadap risiko di sistem informasi akademik Universitas Bina Darma. Penelitian ini dilakukan selama 6 bulan dimulai dari Januari 2018 – Juli 2018. Teknik analisis data penelitian menggunakan analisis kuantitatif dan kualitatif, dimana pengumpulan data yang digunakan adalah wawancara dengan pihak yang dianggap mengetahui tentang objek penelitian yaitu kepada 4 orang informan.

Tabel 1. Informan Penelitian

No.	Bagian	Jumlah
1	Kepala Biro Penjaminan Mutu	1 Orang
2	Kepala UPT-SIM	1 Orang
3	Sub-Unit Pengembangan Sistem	1 Orang
4	Sub-Unit Perawatan dan Perbaikan	1 Orang
	Jumlah	4 Orang

Tujuan yang ingin dicapai oleh *OCTAVE Allegro* adalah penilaian yang luas terhadap lingkungan risiko operasional suatu organisasi dengan tujuan menghasilkan hasil yang lebih baik tanpa perlu pengetahuan yang luas dalam hal penilaian risiko. Pendekatan ini berbeda dari pendekatan *OCTAVE*, dimana *OCTAVE Allegro* lebih berfokus terhadap aset informasi dalam konteks bagaimana mereka digunakan, dimana mereka disimpan, dipindahkan, dan diolah, dan bagaimana mereka terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan. Langkah – langkah yang perlu dilakukan dalam menerapkan metode *octave allegro* seperti gambar berikut :



Gambar 1. Langkah - Langkah Octave Allegro (Caralli et al., 2007)

3 HASIL DAN PEMBAHASAN

Dalam penelitian ini akan menjelaskan hasil dari delapan tahapan sesuai dengan metode octave allegro yaitu membangun kriteria pengukuran risiko (*establish risk measurement criteria*), membangun profil aset informasi (*develop information asset profile*), mengidentifikasi *container* dari aset informasi (*identify information asset containers*), mengidentifikasi area yang diperhatikan (*identify areas of concern*), mengidentifikasi skenario ancaman (*identify threat scenarios*), mengidentifikasi risiko (*identify risks*), menganalisa risiko (*analyze risks*), dan memilih pendekatan pengurangan risiko (*select mitigation approach*).

3.1 Membangun Kriteria Pengukuran Risiko

Tahapan pertama yang dilakukan adalah membangun kriteria pengukuran risiko untuk melakukan penilaian risiko terhadap penggunaan Sistem Informasi Akademik (SISFO) di Universitas Bina Darma berdasarkan lembar kerja allegro. Hal ini dilakukan untuk mengenali area dampak risiko yang paling penting untuk meminimalisir risiko dapat terjadi.

Tabel 2. Impact Area

No	Area Dampak Resiko	Rendah (Low)	Sedang (medium)	Tinggi (high)
1.	Reputasi Universitas	Reputasi sedikit terpengaruh, hanya di internal.	Reputasi menjadi terpengaruh dan dapat menyebabkan citra buruk tersebar.	Reputasi terkena dampak yang sangat buruk dan tersebar ke eksternal.

Pada Tabel 2 diatas menunjukkan area dampak risiko yang dapat berpengaruh terhadap visi dan misi Universitas Bina Darma salah satunya yaitu reputasi Universitas. Setelah area dampak diidentifikasi, langkah selanjutnya memberikan nilai skala prioritas sebagai berikut :

Tabel 3. Skala Prioritas Impact Area

Prioritas	Area Dampak
3	Reputasi Universitas
2	Kepercayaan Pengguna
1	Biaya Operasional

3.2 Membangun Profil Aset Informasi

Tahapan ini dilakukan untuk mengetahui aset informasi apa yang dianggap paling penting pada Universitas Bina Darma dan mengetahui persyaratan keamanan dari aset informasi tersebut.

Tabel 4. Critical Information Asset Profile

Critical asset	Sistem informasi akademik (SISFO)	
Rationale for selection	Karena aset informasi ini digunakan untuk menyimpan semua data dan informasi baik di bidang akademik maupun di bidang keuangan.	
Description	Terdiri dari data di bidang akademik dan keuangan. Bidang akademik seperti data mahasiswa, data nilai, data matakuliah, data keaktifan mahasiswa, data dosen ngajar, data pembimbing, dan data lulusan. Bidang keuangan seperti data penggajian, data karyawan, data absensi karyawan, dan data pembayaran mahasiswa.	
Owner	Bagian akademik (Bidang akademik), dan Bagian keuangan (Bidang keuangan)	
Security requirement	Confidentiality	Data hanya bisa di akses oleh pengguna yang memiliki hak akses / proses bisnis.
	Integrity	Ada beberapa data tertentu yang tidak bisa di ubah / di modifikasi oleh pengguna yang memiliki hak akses kecuali bagian umum dan UPT, seperti kesalahan penginputan data yang telah di validasi.
	Availability	Informasi data harus selalu tersedia untuk pengguna yang mempunyai hak akses jika di butuhkan.
Most important security requirement	Integritas, karena semua data harus terjamin keakuratan dan konsistensinya. Tujuannya untuk memastikan bahwa setiap data yang diinputkan memiliki kesesuaian dengan data yang seharusnya.	

3.3 Mengidentifikasi *Container* dari Aset Informasi

Dari hasil penelitian diatas terdapat *container technical* dan *container people*. Pada *container technical internal* Sistem Informasi Akademik (SISFO) terdapat *server* SISFO, *client server*, media jaringan (kabel, *wireless*, nirkabel), media perantara (*switch*, *router*, *hotspot*), jaringan yang dikelola oleh UPT – SIM dan untuk *container technical external* terdapat pada sistem bank, forlap, feeder, sister, HRIS, dan internet. Sedangkan *container people internal* terhadap Sistem Informasi Akademik (SISFO) yaitu analisis dan programmer, penyimpanan hardisk *backup* oleh staff pengembangan sistem, pelaporan data ke forlap yang dilakukan oleh staff pengolahan data dan untuk *container people external* yaitu proses transaksi pembayaran di bank.

3.4 Mengidentifikasi Area yang Diperhatikan

Tahapan ini digunakan untuk mengetahui kondisi atau situasi yang memungkinkan yang dapat mengancam sistem informasi akademik (SISFO) melalui cara *brainstorming* dengan informan penelitian.

Tabel 5. Areas of Concern

No.	Areas of Concern
1.	Mengubah data nilai tanpa otoritas untuk tujuan tertentu
2.	Ketersediaan data sering terganggu karena sistem sering down yang disebabkan oleh beberapa hal seperti mati lampu dan jaringan putus.
3.	Hilang / rusaknya data yang disebabkan adanya kode berbahaya seperti virus.
4.	Kerusakan pada perangkat keras dan perangkat lunak.
5.	Terjadinya bencana alam yang tidak diinginkan seperti kebakaran.

3.5 Mengidentifikasi Skenario Ancaman

Pada tahapan ini *Area of Concern* yang telah di tetapkan di tahapan sebelumnya, dikembangkan kedalam skenario ancaman yang menjelaskan detail atribut dari sebuah risiko. Skenario ancaman ini dapat mempengaruhi aset informasi untuk masing-masing *container* yang telah ditetapkan dan mengidentifikasikan *actor*, *means*, *motive*, *outcome*, dan *security requirements* serta *probability*.

Tabel 6. Properties of Threat

Ketersediaan data sering terganggu karena sistem sering down yang disebabkan oleh beberapa hal seperti mati lampu, dan jaringan terputus.	1. <i>Actor</i>	Penyedia Jasa Layanan Internet (ISP) jika jaringan internet terputus.
	2. <i>Means</i>	Tidak di ketahui
	3. <i>Motive</i>	Tidak di ketahui
	4. <i>Outcome</i>	Interruption (terganggu)
	5. <i>Security Requirements</i>	Menghidupkan <i>link</i> internet dan menggunakan sarana dan prasarana seperti genset.
	6. <i>Probability</i>	Tinggi

3.6 Mengidentifikasi Risiko

Tahapan ini dilakukan untuk menentukan dampak dari skenario ancaman terhadap Universitas Bina Darma. Untuk setiap skenario yang telah dibuat, Universitas Bina Darma harus menentukan dampak atau konsekuensi yang akan timbul jika ancaman tersebut benar-benar terjadi.

Tabel 7. Identifikasi Risiko

Skenario Ancaman	Konsekuensi
Ketersediaan data sering terganggu karena sistem sering down yang disebabkan oleh beberapa hal seperti mati lampu dan jaringan terputus.	Menyebabkan data <i>corrupt</i> , pekerjaan yang di lakukan secara manual tanpa sistem, dan kerusakan alat dan perangkat keras serta dapat berdampak pada pendapatan Universitas.

3.7 Menganalisa Risiko

Tahapan ini dilakukan untuk mengukur seberapa besar dampak yang ditimbulkan dari sebuah *threat*/ancaman dengan menghitung skor area dampak pada setiap skenario ancaman. Nilai dampak yang di gunakan adalah nilai kuantitatif seperti berikut : Tinggi (3), Sedang (2), dan Rendah (1).

Tabel 8. Analisis Risiko

Skenario Ancaman	Konsekuensi
Ketersediaan data sering terganggu karena sistem sering down yang disebabkan oleh beberapa hal seperti mati lampu dan jaringan terputus.	Ketersediaan data terganggu akibat dari sistem yang sering down, pekerjaan yang di lakukan secara manual tanpa sistem, dan kerusakan alat dan perangkat keras serta dapat berdampak pada pendapatan Universitas.

Area Dampak	Ranking	Nilai Dampak	Skor
Reputasi Universitas	3	Tinggi (3)	9
Kepercayaan Pengguna	2	Sedang (2)	4
Biaya Operasional	1	Rendah (1)	1
		Total Skor	14

3.8 Memilih Pendekatan Pengurangan Risiko

Tahapan ini menentukan risiko mana yang bisa di mitigasi oleh Universitas Bina Darma berdasarkan perhitungan skor risiko relatif di tahapan sebelumnya. Adapun kategori skor risiko sebagai berikut :

Tabel 9. Relative Risk Matrix

Kemungkinan	Skor Risiko		
	13 – 18	7 – 12	0 - 6
Tinggi	POOL 1	POOL 2	POOL 2
Sedang	POOL 2	POOL 2	POOL 3
Rendah	POOL 3	POOL 3	POOL 4

Selanjutnya menetapkan pendekatan mitigasi untuk setiap risiko yang telah di analisis yaitu sebagai berikut :

Tabel 10. Mitigation Approach

<i>Pool</i>	<i>Mitigation Approach</i>
Pool 1	Mengurangi
Pool 2	Mengurangi / <i>Defer</i>
Pool 3	<i>Defer</i> / Menerima
Pool 4	Menerima

Sumber : (Caralli et al., 2007)

Berdasarkan perhitungan analisis skor risiko pada tahapan sebelumnya, maka skenario ancaman termasuk dalam kategori / *pool* 1 artinya harus dilakukan strategi mitigasi.

Tabel 11. Risk Mitigation

Area yang di perhatikan	Tindakan	Solusi
Ketersediaan data sering terganggu karena sistem sering down yang disebabkan oleh beberapa hal seperti mati lampu dan jaringan terputus	Mengurangi	Membuat redundan <i>link</i> internet dan meletakkan sistem di <i>cloud</i> (membuat <i>Secondary Server</i>).

4 KESIMPULAN

Sistem informasi akademik (SISFO) adalah aset informasi yang paling penting bagi Universitas Bina Darma karena sistem informasi ini digunakan universitas dalam proses atau pekerjaan baik di bidang akademik maupun keuangan. Dari aset informasi ini terdapat 5 area yang menjadi perhatian yang bisa menjadi ancaman pada universitas, baik area yang berdampak pada reputasi universitas, kepercayaan pengguna, dan biaya operasional. dari hasil penelitian diantara 5 skenario ancaman terdapat 1 area yang kemungkinan terjadi tinggi dengan skor risiko relatif yang tinggi juga yaitu ketersediaan data yang sering terganggu akibat mati lampu dan jaringan terputus. Pendekatan mitigasi yang dilakukan yaitu membuat redundan link internet dan meletakkan sistem di *cloud* (membuat *Secondary Server*). Hal ini diharapkan dapat mengurangi peluang terjadinya risiko terhadap ketersediaan data sistem informasi akademik (SISFO).

Referensi

- CARALLI, R. A., STEVENS, J. F., YOUNG, L. R. & WILSON, W. R. 2007. The octave allegro guidebook, v1. 0. *Software Engineering Institute*.
- JAKARIA, D. A. & DIRGAHAYU, R. T. Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2013.
- JUSUF, H. IT Governance pada layanan akademik on-line di universitas nasional menggunakan COBIT (control objectives for information and related technology) versi 4.0. Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2009.
- NASUTION, R. & SARI, A. P. 2014. Manajemen Resiko Sistem Informasi Ujian Online Pada Perguruan Tinggi. *Simposium Nasional Ilmu Pengetahuan dan Teknologi (SIMNASIPTEK)*, 1, 136-139.