yayuk

by Adelin Adelin

Submission date: 07-Oct-2020 12:30PM (UTC+1000)
Submission ID: 1387533977
File name: YayukIkeMeilani_3.doc (157K)
Word count: 3155
Character count: 21416

PENILAIAN RESIKO PADA SISTEM MONITORING KEGIATAN BELAJAR MENGAJAR DI PERGURUAN TINGGI SWASTA

Yayuk Ike Melani[1*], Mahmud[2]
[1]Sistem Informasi, STMIK PalComTech Palembang
[2]Informatika, STMIK PalComTech Palembang
email: [1]yayuk_ike@palcomtech.ac.id, [2]mahmud@palcomtech.ac.id

Abstract: The purpose of this study is to measure the likelihood of a threat and risk impact on the teaching and learning activity monitoring system and to provide recommendations for risk control of security problems that could become a threat that causes losses to universities. Some of the risks that are classified as dangerous are often ignored by users of the learning activity monitoring system at private universities so that there are several obstacles such as not being able to open the system because the system was hacked by irresponsible parties. The framework used as a tool to measure the level of threat and risk impact is to use the NIST Special Publication 800-30r-1 framework. The framework of the NIST Special Publication 800-30r-1 has nine phases in carrying out risk assessments, namely introduction of system characteristics, recognition of threats, recognition of vulnerabilities, analysis of handling systems, determining likelihood, determining consequences, risk determination, recommending control and determination of results. There are six risk assessment systems for monitoring learning activities at private universities, two of which are high so they are classified as very dangerous and the rest are moderate. The results of this study are used as a reference in making risk control standard documents as a form of improving the quality of a private university

Keywords: Monitoring System, Risk Assessment, NIST Spesial Publication 800-30r1.

Abstrak: Tujuan dari penelitian ini adalah mengukur seberapa besar kemungkinan terjadi ancaman dan dampak resiko terhadap sistem monitoring kegiatan belajar mengajar serta memberikan rekomendasi pengendalian resiko dari permasalahan keamanan yang bisa menjadi suatu ancaman yang menimbulkan kerugian pada perguruan tinggi. Beberapa resiko yang tergolong berbahaya sering tidak dihiraukan oleh pengguna dari sistem monitoring kegiatan belajar pada perguruan tinggi swasta sehingga terjadi beberapa kendala seperti tidak bisa membuka sistem karena sistem diretas oleh pihak yang tidak bertanggung jawab. Framework yang digunakan sebagai alat untuk mengukur tingkat ancaman dan dampak resiko adalah menggunakan kerangka kerja NIST Special Publication 800-30r-1. Kerangka kerja NIST Special Publication 800-30r-1 ini mempunyai sembilan fase dalam melakukan penilaian resiko yaitu pengenalan karakteristik sistem, pengenalan ancaman, pengenalan kerentanan, analisis penanganan sistem, menentukan kemungkinan terjadi (likelihood), menentukan dampak (impact), risk determination, merekomendasikan pengendalian dan penetapan hasil. Penilaian resiko sistem monitoring kegiatan belajar pada perguruan tinggi swasta ada enam resiko yang dua diantaranya termasuk tinggi sehingga digolongkan sangat berbahaya dan selebihnya termasuk sedang. Hasil dari penelitian ini digunakan sebagai acuan dalam pembuatan dokumen standar pengendalian resiko sebagai bentuk peningkatan mutu suatu perguruan tinggi swasta.

Kata kunci: Sistem Monitoring, Penilaian Resiko, NIST Spesial Publication 800-30r1.

PENDAHULUAN

Teknologi sebagai media informasi yaitu teknologi yang dapat dipergunakan untuk mengampuh data, seperti melakukan proses data, mendapatkan data, menata data, menyimpan data, serta memanipulasi data untuk memperoleh informasi yang berkualitas, yaitu informasi yang signifikan, saksama dan tepat waktu, yang dapat digunakan untuk keperluan personal, bisnis, dan pemerintahan dan memperoleh informasi yang strategis untuk pengambilan keputusan. Perkembangan teknologi yang luar biasa beberapa dekade membuat semua pekerjaan menjadi lebih cepat dan akurat. Salah satu yang menerapkan teknologi informasi adalah perguruan tinggi. Tidak hanya perguruan tinggi negeri tetapi perguruan tinggi swasta pun juga menerapakan teknologi informasi sebagai alat dalam proses pembelajaran.

Sistem informasi merupakan aset yang berharga. seiring perkembangannya Kebanyakan teknologi kerap kali dimanfaatkan pihak-pihak yang tidak bertanggung jawab sehingga menimbulkan beberapa ancaman serta resiko dari penggunaan teknologi. Permasalahan yang diakibatkan oleh keamanan sistem membuat kerugian.

Pemanfaatan teknologi dan sistem informasi seharusnya mendapatkan perhatian sehubungan dengan resiko yang kemungkinan akan muncul sehingga pemanfaatan sistem informasi dan teknologi yang kurang efektif. [1].

Penelitian ini difokuskan pada penilaian resiko terhadap penggunaan teknologi dari sistem monitoring kegiatan belajar mengajar yang ada pada salah satu perguruan tinggi swasta di Palembang. Setiap proses kegiatan belajar mengajar diperlukan pengawasan terhadap teknologi yang digunakan agar kegiatan belajar mengajar berjalan dengan lancar. Seiring berjalannya waktu dan penggunaan teknologi semakin besar, terdapat beberapa kejahatan komputer yang dilakukan oleh user. Kejahatan komputer digolongkan dari yang hanya mengesalkan sampai ke tahap sangat berbahaya.

Penelitian terdahulu pernah dilakukan oleh Mashuri yang berjudul "Pengembangan Manajemen Resiko Teknologi Informasi Pada Sistem Penerimaan Peserta Didik Baru (Ppdb Online) Kemdikbud Menggunakan Framework Nist Sp800-30" mengungkapkan bahwa yang dibuat merupakan sistem meliputi menyebabkan tidak keseragaman dalam aturan proses PPDB. Hal ini menyebabkan resiko yang cukup besar pula. Dengan adanya manajemen resiko, dapat mengatur dan mengelola segala sesuatu terkait dengan kegiatan penilaian resiko, mitigasi resiko dan evaluasi pelaksanaannya. [2].

Penelitian serupa juga pernah dilakukan oleh Agustinus dkk yang berjudul "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS", Hasil dari penelitian yang dilakukan, menganalisis resiko TI pada program Human Resource Management System (HRMS) menggunakan ISO 31000. Analisis ini menggunakan tahapan-tahapan seperti penilaian risiko yang terdiri dari tahap identifikasi, analisis, dan tahap evaluasi risiko hingga tahap perlakuan risiko [3].

Penelitian selanjutnya pernah dilakukan oleh Via Aprilia Prabawati dkk yang berjudul "Analisis Risiko Teknologi

Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya"mengungkapkan bahwa modal kritis yang melakukan pemahaman pada Unit Pengelola Sistem Informasi dan Kehumasan Fakultas Ilmu Komputer adalah FILKOM Apps dan Infrastruktur Data dan Jaringan. Hasil analisis risiko menggunakan kerangka kerja OCTAVE-S menunjukkan bahwa terdapat tiga area keamanan yang memiliki status stoplight kuning diantaranya adalah Pengendalian Akses Fisik, Autentikasi dan Otorisasi, serta Manajemen Kerentanan. Sedangkan area praktik keamanan yang berstatus stoplight merah adalah Manajemen Insiden [4].

Tujuan dari penelitian ini adalah mengukur seberapa besar kemungkinan terjadi ancaman dan dampak resiko terhadap sistem monitoring kegiatan belajar mengajar serta memberikan rekomendasi pengendalian resiko dari permasalahan keamanan yang bisa menjadi suatu ancaman yang menimbulkan kerugian pada perguruan tinggi.

METODE

Teknik Pengumpulan Data

Pengumpulan data yang dilakukan dalam penelitian ini adalah menggunakan wawancara dan observasi. Wawancara adalah teknik berkomunikasi atau beriinteraksi untuk mendapatkan informasi dengan cara bertanya dan menjawab yang dilakukan oleh peneliti dan informan atau subjek penelitian. Adanya kemajuan teknologi seperti membuat wawancara dapat dilakukan tanpa tatap muka, yakni melalui media elektronik. Pada dasarnya wawancara merupakan kegiatan untuk memperoleh informasi secara rinci tentang sebuah persoalan yang diangkat dalam penelitian. Atau, merupakan proses memberikan bukti terhadap informasi atau keterangan yang telah diperoleh lewat teknik yang lain sebelumnya [5]. Wawancara dilakukan dengan mewawancarai user yang yang bertanggung jawab atas aplikasi. Data yang didapat berupa informasi ancaman apa saja yang pernah menyerang aplikasi.

Pengumpalan data selanjutnya yang dilakukan adalah observasi. Observasi sebagai kegiatan mencatat suatu proses dengan bantuan data-data dan merekamnya dengan tujuan ilmiah atau tujuan lain. Observasi merupakan kumpulan data berdasarkan semua kemampuan daya tangkap pancaindera manusia [6]. Data yang didapat adalah informasi dari hardware dan software yang digunakan untuk scanning jika terjadi hacking dan phissing, informasi hardware yang dipakai, informasi bagaimana penanganan jika ada ancaman, serangan apa saja yang pernah terjadi.

Mekanisme Penilaian Resiko

Mekanisme penilaian resiko menggunakan menggunakan kerangka kerja NIST SP 800-30r-1. Kerangka kerja NIST SP 800-30r-1 merupakan pedoman untuk menjalankan data yang sangat sensitif. NIST Special Publication 800-30r-1 memiliki peran lebih dalam melakukan penilian resiko karena memberikan pengetahuan keamanan penjelasan yang bersifat konsisten dan mendalam bagi pengambilan kebijakan, bentuk sumber daya yang terstruktur, pengetahuan keamanan informasi dapat diterima oleh penerima resiko, penentuan ancaman dapat diketahui dengan mudah, pengam-

bilan keputusan untuk setiap resiko dan ancaman yang telah diperiksa [7]. Kerangka kerja NIST mengeluarkan rekomendasi melalui publikasi khusus 800-30r1 tentang *Risk Management Guide for Information Technology System*. Ada tiga proses dalam manajemen resiko yaitu *Risk Assessment, Risk Mitigation dan Evaluation and Assessment*. Tetapi, proses yang digunakan penulis dalam penelitian ini adalah membahas *risk assessment* dari sistem informasi akademik. *Risk assessment* atau penilaian risiko adalah proses awal yang dilakukan dalam metodologi manajemen risiko [8]. Beberapa organisasi menggunakan asessment untuk mengetahui seberapa banyak potensi ancaman dan risiko yang terkait dengan teknologi informasi di seluruh SDLC-nya. Keluaran dari proses ini membantu mengetahui pengendalian yang tepat mengurangi atau menghilangkan risiko selama proses mitigasi risiko. Penilaian resiko dari framework NIST 800-30r1 mempunyai sembilan fase yaitu :

Pengenalan Karakteristik Sistem

Sistem teknologi informasi mencakup perangkat keras, perangkat lunak, infrastrktur, data dan informasi user yang terlibat dalam pengelolaan dan penggunaan sistem.

Pengenalan Ancaman

Melakukan pengenalan bahaya terhadap kelemahan sistem teknologi informasi yang berasal dari dalam maupun luar organisasi serta lingkungan.

Pengenalan Kerentanan

Melakukan pengenalan kerentanan (*vulnerability*) pada mekanisme keamanan, desain, implementasi, pengendalian baik luar maupun dalam terhadap sistem sehingga menghasilkan kesalahan terhadap kebijakan keamanan sistem.

Analisis Penanganan Sistem

Menganalisis pengendalian-pengendalian yang sudah diimplementasikan atau direncanakan untuk direncanakan oleh organisasi untuk mengurangi atau menghilangkan kecenderungan (kemungkinan) dari suatu ancaman yang menyerang sistem.

Menentukan Kemungkinan Terjadi (*Likelihood*)

Menentukan kemungkinan terjadi (*likelihood*) bertujuan untuk mendapatkan penilaian terhadap keseluruhan keinginan yang mengisyaratkan kemungkinan adanya potensi penilaian kerentanan yang diserang oleh lingkungan sekitar. Penilaian skala untuk kemungkinan terjadi ada 4 tabel yaitu skala yang mengukur kemungkinan terjadi pada penyusup(adversarial), mengukur kemungkinan terjadi bukan karena penyusup(non-adversarial), mengukur kemungkinan terjadi yang mengakibatkan dampak buruk, dan yang terakhir itu skala keseluruhan dari kemungkinan terjadi. Tabel 1 menunjukan gambaran dari kemungkinan terjadi karena penyusup.

Tabel 1. Kemungkinan Terjadi Resiko

	Deskripsi Kemungkinan Terjadi Resiko
Tinggi	Sumber ancaman sangat mahir pencegahan yang dilakukan

	Deskripsi Kemungkinan Terjadi Resiko
	tidak efektif lagi
Sedang	Sumber ancaman mampu dapat menembus pertahanan sistem namun hanya sampai pada lapisan tengah dapat menghambat kerentanan
Rendah	Sumber ancaman tidak dapat menembus keamanan

Sumber: NIST SP 800-30 r1

Menganalisis Dampak Resiko

Melakukan analisis dampak negatif terhadap keberhasilan penyerangan vulnerability sistem TI. Seperti loss of integrity, loss of availability, dan loss of confidentiality. Pengukuran dampak dari risiko TI dapat dilakukan secara kualitatif. Dampak tersebut dapat diklasifikasikan menjadi tiga bagian yaitu: tinggi, sedang dan rendah. Dampak atau impact yang digunakan dalam melakukan penilaian resiko telah tersedia didalam kerangka kerja NIST SP 800-30r-1. Skala mengukur dampak resiko yang terlihat pada tabel 2.

Tabel 2. Skala Penilaian Dampak

	Deskripsi Dampak
Tinggi	(I) Menyebabkan kerusakan parah atau hilangnya kemampuan untuk meningkatkan misi dari lembaga yang mengakibatkan tidak dapat melakukan satu atau lebih dari fungsi utama sistem. (II) Mengakibatkan kerusakan yang besar terhadap aset lembaga. (III) Mengakibatkan kerugian finansial yang besar
Sedang	(I) Menyebabkan penurunan yang signifikan dalam meningkatkan misi dan lembaga yang mengakibatkan tidak dapat melakukan satu atau lebih dari fungsi utama sistem. (II) Menyebabkan kerusakan yang signifikan terhadap aset organisasi. (III) Menyebabkan kerugian finansial yang signifikan
Rendah	(I) Menyebabkan degradasi dalam meningkatkan misi lembaga tidak dapat melakukan satu atau lebih dari fungsi utama sistem, tetapi efektifitas

	Deskripsi Dampak
	fungsi berkurang. (II) Mengakibatkan kerusakan kecil terhadap aset organisasi. (III) Mengakibatkan kerugian finansial yang kecil

Sumber: NIST SP 800-30 r1

Risk Determinan

Penetapan tingkatan risiko dari sistem teknologi informasi yang merupakan pasangan ancaman merupakan suatu fungsi, yaitu keinginan suatu sumber ancaman menyerang vulnerability dari sistem teknologi informasi.

Matriks tingkat resiko yang digunakan adalah 3X3 yaitu untuk penentuan kemungkinan terjadi ancaman yang terdiri dari tinggi, sedang dan rendah. Kemudian untuk penentuan dampak ancaman terdiri dari tinggi, sedang dan rendah. Dari penentuan keseluruhan maka didapat hasil apakah termasuk kedalam level yang rendah atau yang tinggi. Kemungkinan terjadi ancaman mempunyai skala level yaitu 1 untuk tinggi, 0,5 untuk sedang, dan 0,1 untuk rendah.

Nilai dari dampak ancaman yaitu 100 untuk tinggi, 50 untuk medium dan 10 untuk rendah

Tingkat resiko kombinasi antara kemungkinan terjadi dan dampak dapat dilihat pada gambar 1.

Threat Likelihood	Impact		
			High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Sumber: NIST SP 800-30 r1

Gambar 1. Skala Penentuan Resiko

2

Merekomendasikan Pengendalian

Memberikan saran pencegahan untuk mengurangi tingkatan risiko sistem teknologi informasi serta data sehingga mencapai tingkatan yang dapat diterima.

Dokumen Hasil

HASIL DAN PEMBAHASAN

Untuk menganalisis resiko-resiko maka dilakukan melalui tahap wawancara dan penyebaran kuesioner untuk mendapatkan hasil tingkat resiko pada sistem monitoring kegiatan belajar mengajar pada perguruan tinggi swasta. Terdapat beberapa tahapan-tahapan yang dilakukan untuk mengantisipasi kemungkinan terjadinya resiko adalah sebagai berikut:

Karakteristik sistem

Perangkat keras yang digunakan berupa PC yang mempunyai server lokal dan server luar yaitu cloud untuk membackup data-data yang diolah didalam aplikasi sintana. Software yang digunakan berupa linux free BSD.

1. Pengenalan Ancaman

Ancaman terhadap sistem monitoring kegiatan belajar mengajar adalah orang dalam yang pernah mempunyai akses kedalam sistem, sistem operasi yang usang, kebakaran yang disebabkan human error, virus malware, jamming, serangan cyber, rusaknya media penyimpanan seperti

hardisk yang ada pada PC yang digunakan

2. Pengenalan Kerentanan

Setelah mengindentifikasi ancaman, tahap yang dilakukan selanjutnya adalah mengidentifikasi kerentanan yang terjadi pada sistem monitoring kegiatan belajar mengajar. pengenalan kerentanan dapat dilihat pada tabel 3.

Tabel 3. Indentifikasi Kerentanan

Tipe Resiko	Kerentanan
Pengguna sistem monitoring yang merupakan orang terpercaya melakukan penyerangan	- Salah satu penyerangan yang dilakukan yaitu menggunakan kata kunci secara paksa untuk melakukan pencurian data pada sistem
Sistem operasi yang digunakan sudah usang	- Teknologi yang digunakan untuk melakukan penyerangan sistem semakin kuat seiring berjalannya waktu
Kebakaran	- Pengamanan kabel yang membangun sistem E-University yang tidak benar akan membuat resiko kebakaran
Malware	- Keterlambatan dalam melakukan *update anti-virus* sehingga memungkinkan *malware* masuk kedalam sistem
Jamming	- jaringan wifi menggunakan wireless
Serangan *cyber*	- Penyusup menyesuaikan perilaku dalam menanggapi pengawasan dan langkah-langkah keamanan organisasi
Media penyimpanan data rusak	- Over heat pada pc - Penggunaan yang berlebihan pada pc yang digunakan - Mematikan pc dengan cara menekan tombol power bukan dari menu shutdown (mematikan paksa)

Analisis Penanganan Sistem

Pengendalian-pengendalian yang didapat dalam wawancara telah dituangkan kedalam arsip yang mencakup semua standar-standar dan mekanisme dalam pengoperasian sistem monitoring kegiatan belajar mengajar yaitu dokumen SOP (*Standard Operating Procedure)*.

Menentukan Kemungkinan Terjadi (*Likelihood*)

Setelah melakukan identifikasi kerentanan, selanjutnya menentukan bagaimana kemungkinan terjadi (*likelihood*) pada sistem monitoring kegiatan belajar mengajar. Kemungkinan terjadi ancaman pada sistem monitoring kegiatan belajar mengajardapat dilihat pada tabel 4.

Tabel 4. Kemungkinan Terjadi (*Likelihood*)

Tipe Resiko	Tingkat kemungkinan terjadi (Likelihood)

Tipe Resiko	Tingkat kemungkinan terjadi (Likelihood)
Pengguna sistem monitoring yang merupakan orang terpercaya melakukan penyerangan	Tinggi
Sistem operasi yang digunakan sudah usang	Tinggi
Kebakaran	Sedang
Malware	Tinggi
Jamming	Tinggi
Serangan *cyber*	Sedang
Media penyimpanan data rusak	Tinggi

Menganalisis Dampak Resiko

Setelah melakukan identifikasi kemungkinan terjadi (*likelihood)*, selanjutnya menentukan bagaimana dampak resiko yang akan terjadi pada sistem monitoring kegiatan belajar mengajar. Dampak resiko ancaman pada sistem monitoring kegiatan belajar mengajardapat dilihat pada tabel 5.

Tabel 5 Konsekuensi Resiko

Tipe Resiko	Dampak	Tingkat dampak resiko
Pengguna sistem monitoring yang merupakan orang terpercaya melakukan penyerangan	Penyusup yang masuk dapat melakukan pencurian data	Tinggi
Sistem operasi yang digunakan sudah usang	Kerusakan parah pada sistem yang mengakibatkan beberapa atau semua fungsi pada sistem tidak dapat dioperasikan,	Tinggi
Kebakaran	Rusaknya hardware dan software yang digunakan untuk mendukung sistem monitoring kegiatan belajar mengajar	Tinggi
Malware	- Merubah tampilan pada sistem monitoring kegiatan belajar mengajar - Memunculkan iklan-iklan spam pada sistem monitoring kegiatan belajar mengajar -	Sedang
Jamming	Penyusup mengganggu jaringan yang digunakan oleh sistem monitoring kegiatan	Sedang

Tipe Resiko	Dampak	Tingkat dampak resiko
	belajar mengajar	
Serangan *cyber*	- Mengunci sistem komput-er dan data yang diserang	Sedang
Media penyimpanan data rusak	Kehilangan data penting yang ada pada sistem	Tinggi

Risk Determination

Setelah melakukan identifikasi kemungkinan terjadi (*likelihood)* dan dampak resiko, selanjutnya dilakukan pengukuran seberapa tinggi atau seberapa rendahkah tingkat resiko yang terjadi pada sistem monitoring kegiatan belajar mengajar menggunakan skala pada matriks resiko. Hasil dari risk determination dapat dilihat pada tabel 6.

Tabel 6. Penetapan Resiko

Tipe Resiko	Nilai peluang Terjadi (vulnerability)	Nilai dampak	Nilai Resiko	Tingkat Resiko
Pengguna sistem monitoring yang merupa-kan orang terpercaya melakukan penyerangan	Tinggi (1,0)	Tinggi (1,0)	100	Tinggi
Sistem operasi yang digunakan sudah usang	Tinggi (1,0)	Tinggi (1,0)	100	Tinggi
Kebakaran	Sedang (0,5)	Tinggi (1,0)	50	Sedang
Malware	Tinggi (1,0)	Sedang (0,5)	50	Sedang
Jamming	Tinggi (1,0)	Sedang (0,5)	50	Sedang
Serangan *cyber*	Sedang (0,5)	Sedang (0,5)	25	Sedang
Media penyimpanan data rusak	Tinggi (1,0)	Tinggi (1,0)	100	Tinggi

Rekomendasi Pengendalian

Dari hasil penentuan tingkat resiko maka peneliti memberikan rekomendasi pengendalian bagaimana cara menghadapi ancaman-ancaman atau serangan-serangan yang dilakukan oleh hacker terhadap sistem monitoring kegiatan belajar mengajar. Rekomendasi pengendalian dapat dilihat pada tabel 7.

Tabel 7. Rekomendasi Pengendalian

No.	Jenis Resiko	Tingkat Resiko	Rekomedasi Pengendalian
1	Pengguna sistem monitoring yang merupakan orang ter-percaya melakukan penyerangan	Tinggi	Memperkuat firewall yang digunakan
2	Sistem operasi yang digunakan sudah usang	Tinggi	Lakukan update berkala untuk sistem operasi yang digunakan
3	Kebakaran	Sedang	Gunakan pelindung kabel yang aman dan instalasi kabel dengan benar
4	*Malware*	Sedang	Update plug in, update antivirus, update versi software
5	Jamming	Sedang	Gunakan teknik spread spectrum
6	Serangan *cyber*	Sedang	Memberikan password yang kuat dan rahasia kepada semua pengguna, firewall diperkokoh, backup data berkala
7	Media penyimpanan data rusak	Tinggi	- Gunakan kipas untuk menstabilkan suhu didalam pc - Batasi waktu penggunaan pc agar pc mempunyai waktu "istirahat" untuk mendinginkan suhu - Selalu gunakan menu shutdown untuk mematikan pc

Penetapan Hasil

Dari hasil penilaian resiko sistem monitoring kegiatan belajar mengajar pada perguruan tinggi swasta dibuatlah tata cara bagaimana penanganan resiko-resiko dari penyerangan terhadap sistem yang dibuat berdasarkan rekomendasi bagaimana cara pengendalian terhadap ancaman-ancaman yang menyerang sistem. Dokumen hasil ini dapat berupa standar prosedur penanganan dari ancaman-ancaman dan resiko-resiko yang menyerang sistem.

SIMPULAN

Dalam proses penialain resiko pada penelitian ini menggunakan kerangka kerja NIST Special Publication 800-30r-1 yang terdiri dari penilaian resiko yaitu pengenalan karakteristik sistem, pengenalan ancaman, pengenalan kerentanan, analisis penanganan sistem, menentukan kemungkinan terjadi (likelihood), menentukan konsekuensi (impact), risk determination, merekomendasikan pengendalian dan penetapan hasil. Untuk mengetahui resiko, peneliti melakukan wawancara kepada pengguna sistem. Dari hasil penilaian resiko terdapat delapan jenis resiko yang terjadi pada sistem monitoring kegiatan belajar mengajar. Resiko-resiko yang terjadi adalah orang dalam yang pernah mempunyai akses kedalam sistem, sistem operasi yang usang, kebakaran yang disebabkan human error, virus malware, jamming, serangan cyber, rusaknya media penyimpanan seperti hardisk yang ada pada PC yang digunakan. Saran dari peneliti, pengendalian yang dilakukan terhadap sistem monitoring kegiatan belajar

mengajar pada perguruan tinggi swasta telah tertuang kedalam SOP yang ada pada perusahaan, namun ada baiknya jika membuat dokumen pemulihan setelah bencana yang terjadi *(Disaster Recovery Planning*). Untuk penelitian selanjutnya, peneliti menyarankan dilakukan Teknik penilaian resiko yang lebih mendalam dan beragam untuk penilaian resiko pada sistem monitoring kegiatan belajar mengajar pada perguruan tinggi swasta.

UCAPAN TERIMA KASIH

Terima kasih saya ucapkan kepada keluarga saya yang sudah mendukung dan membantu dalam menyelesaikan penelitian ini..

DAFTAR PUSTAKA

[1] B. Suzanto and I. Sidharta, "Pengukuran end-user computing satisfaction atas penggunaan sistem informasi akademik," *Jurnal Ekonomi, Bisnis & Entrepreneurship,* vol. 9, no. 1, pp. 16-28, 2015.

[2] I. Mashuri, "Pengembangan Manajemen Resiko Teknologi Informasi Pada Sistem Penerimaan Peserta Didik Baru (Ppdb Online) Kemdikbud Menggunakan Framework Nist Sp800-30," *Surabaya: Theses Manajemen Teknologi Informasi-S2 Mmt, Its,* 2015.

[3] S. Agustinus, A. Nugroho, and A. D. Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi),* vol. 1, no. 3, pp. 250-258, 2017.

[4] V. A. Prabawati, A. Rachmadi, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN,* vol. 2548, p. 964X, 2018.

[5] M. Rahardjo, "Metode pengumpulan data penelitian kualitatif," 2011.

[6] H. Hasanah, "Teknik-teknik observasi (sebuah alternatif metode pengumpulan data kualitatif ilmu-ilmu sosial)," *At-Taqaddum,* vol. 8, no. 1, pp. 21-46, 2017.

[7] Y. I. Meilani, D. Syamsuar, and Y. N. Kunang, "Assessment Resiko Teknologi Pada Implementasi Sistem Informasi Akademik E-university," *Jurnal Bina Komputer,* vol. 1, no. 1, pp. 54-60, 2019.

[8] S. NIST, "800-30, Revision 1," *Guide for Conducting Risk Assessments,* 2012.

yayuk

ORIGINALITY REPORT

18%	%	%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	media.neliti.com Internet Source	4%
2	es.scribd.com Internet Source	3%
3	Submitted to Universitas Brawijaya Student Paper	2%
4	j-ptiik.ub.ac.id Internet Source	1%
5	eprints.iain-surakarta.ac.id Internet Source	1%
6	nanditobryan.blogspot.com Internet Source	1%
7	Submitted to Universitas Kristen Satya Wacana Student Paper	1%
8	digilib.unila.ac.id Internet Source	1%
9	ejournal.poltektegal.ac.id Internet Source	1%

10	jurnal.iaii.or.id Internet Source	1%
11	Submitted to Sriwijaya University Student Paper	1%
12	id.123dok.com Internet Source	1%
13	www.neliti.com Internet Source	1%

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	On		