Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Audit Keamanan dan Manajemen Risiko pada *e-Learning* Universitas Sangga Buana

Sandy[1], **Hanhan Hanafiah Solihin**[2]
[1,2]Program Studi Sistem Informasi, Universitas Sangga Buana, Bandung, Indonesia
e-mail: [1]sandydy231096@gmail.com, [2]hanhan.hanafiah@usbypkp.ac.id

Abstrak

Universitas Sangga Buana merupakan lembaga pendidikan yang terus berkembang mengikuti kemajuan teknologi, dengan membuat sistem e-Learning bagi mahasiswanya untuk memudahkan pembelajaran jarak jauh. Sistem ini terbilang baru dan masih terus dikembangkan, yang memungkinkan masih banyak celah yang bisa dimanfaatkan oleh orang lain, terutama pada sisi keamanan sistem. Untuk mengurangi kerentanan pada keamanan sistem serta mengurangi risiko kemungkinan kehilangan data, maka perlu dilakukannya audit pada sistem e-Learning Universitas Sangga Buana. Tahapan yang digunakan untuk mengetahui kerentanan sistem keamanan serta manajemen risiko pada sistem e-Learning yaitu menggunakan framework NIST, serta aplikasi Acunetix sebagai alat pengujian keamanan sistem. Hasil akhir dari audit sistem e-Learning adalah sistem e-Learning Universitas Sangga Buana berada pada level yang sudah baik dengan tidak ditemukannya kerentanan sistem yang tinggi dan manajemen risiko yang diimplementasikan sudah baik.

Kata kunci: *Audit, e-Learning, Framework NIST, Keamanan, Manajemen Risiko*

Abstract

Universitas Sangga Buana is an educational institution that continues to develop the following technological advances by creating an e-Learning system for students to facilitate distance learning. This system is relatively new and still being developed, allowing there are still many gaps that others can exploit, especially on the security side of the system. To reduce system security vulnerabilities and data loss risks, it is necessary to conduct an audit of the e-Learning system at the Universitas Sangga Buana. The stages used to determine security system vulnerabilities and risk management in e-Learning systems use the NIST framework and the Acunetix application as a system security testing tool. The final result of the e-Learning system audit is that the e-Learning system of the University of Sangga Buana is at a reasonable level with no high system vulnerabilities found and well-implemented risk management.

Keywords: *Audit, e-Learning, NIST Framework, Risk Management, Security*

1. Pendahuluan

Saat ini sudah banyak perguruan tinggi yang melakukan inovasi pembelajaran menggunakan teknologi informasi dan komunikasi. Kemudahan akses internet dan murahnya perangkat untuk mengakses internet membuat pengguna untuk membuat sistem *e-Learning* terus bertambah. Dengan pembelajaran dilakukan secara *online* yang harus difasilitasi dengan menggunakan komputer yang terhubung ke internet maka materi pembelajaran tidak lagi terbatas oleh jarak, ruang dan waktu, serta bisa dimana saja dan kapan saja.

Seiring berkembangnya antara Sistem Informasi (SI) dan Teknologi Informasi maka kebutuhan audit Sistem Informasi bertambah diberbagai lembaga, yang mana audit SI berfungsi untuk mengetahui dan memperbaiki sistem keamanan agar mengurangi jumlah risiko kehilangan data dan aset lembaga tersebut serta menjadi rujukan pengembangan

Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

sistem yang ada. Pengelolaan yang kurang baik akan mempengaruhi kinerja dan pandangan dari pengguna. Maka dari itu, manajemen risiko memegang peranan penting dalam menjaga keamanan data dan aset [1] seperti mengatur bila terjadi kesalahan yang disebabkan oleh masalah data, dengan meningkatkan kemanan sistem yang digunakan.

Framework NIST adalah suatu kerangka kerja yang dipublikasikan oleh *National Institute of Standard and Technology* (NIST). Yang dilakukan NIST, yaitu pengukuran, menetapkan standar dan teknologi agar mampu mengoptimalkan fungsi dari infrastruktur institusi, khususnya dalam bidang *Information Technology* (IT). Versi dan topik yang dimiliki NIST sangat banyak, tetapi saling memiliki keterkaitan. "*NIST Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems*" merupakan salah satu versi dari NIST yang berfungsi untuk melakukan audit keamanan sistem informasi. NIST 800-26 memiliki *self-asessment* yang bertujuan untuk mengetahui status program keamanan informasi saat ini [2]. Kerangka kerja NIST tersebut diharapkan dapat meningkatkan kemampuan sebuah lembaga dalam mengatasi permasalah keamanan komputer, baik pada saat ini maupun masa yang akan datang[3][4], Dengan menggunakan NIST lembaga pendidikan akan mengetahui sejauh mana tingkat keamanan, serta mengurangi terjadi kerusakan pada aset lembaga pendidikan. Untuk itu perlu dilakukan identifikasi ancaman dan analisis risiko untuk meningkatkan keamanan dan mengurangi resiko kerusakan sistem informasi[5]. Dengan banyaknya lembaga baik nasional maupun internasional yang menggunakan *Framework* NIST sebagai alat audit dan manajemen risiko, serta kejelasan setiap bagian dari NIST baik itu pertanyaan kepada responden dan tahapannya, maka NIST layak digunakan pada penelitian ini.

Universitas Sangga Buana merupakan salah satu lembaga pendidikan yang sudah menggunakan sistem *e-Learning* dengan berbasis website untuk dapat memudahkan mahasiswanya dalam pembelajaran online dengan memerlukan Nomor Pokok Mahasiswa (NPM) dan *password* agar dapat tersambung pada sistem *e-Learning* tersebut. Sistem website ini digunakan sebagai pengganti pembelajaran tatap muka pada umumnya seperti memberikan materi perkuliahan, memberikan tugas dan kuis, Ujian Tengah Semester (UTS) maupun Ujian Akhir Semester (UAS) yang diberikan oleh dosen. Sistem ini terbilang baru dan belum diketahui sampai sejauh mana sistem keamanan sudah berjalan. Oleh karena itu diperlukannya audit keamanan sebagai sarana untuk mengembangkan dan memperbaiki masalah sistem yang ada agar menjadi lebih baik lagi. Jika keamanan dan manajemen risiko dilakukan terhadap sistem informasi *e-Learning*. Maka akan dapat mengurangi masalah pada sistem kuliah online, khususnya di Universitas Sangga Buana, diantaranya data menjadi tidak valid, akurasi data menjadi tidak dapat dipercaya, dan sistem informasi tersebut terhindar dari ancaman, baik itu ancaman secara internal maupun external. Peran NIST sebagai alat yang tepat pada penelitian ini dikarenakan belum adanya penelitian sebelumnya yang berkaitan dengan audit keamanan dan menajemen risiko pada sistem kuliah *online* Universitas Sangga Buana.

Berdasarkan uraian diatas, rumusan masalah-masalah yang akan dibahas, yaitu: (1) Bagaimana dampak yang terjadi saat ini dengan menggunakan sistem *e-Learning* yang berlaku sekarang, (2) Apa pendapat dan pandangan para pengguna *e-Learning* dengan fitur sistem yang berlaku saat ini, (3) Bagaimana sistem keamanan yang diterapkan dalam sistem *e-Learning* di Universitas Sangga Buana, (4) Bagaimana sistem manajemen risiko yang telah dilakukan dalam sistem *e-Learning* yang ada di Universitas Sangga Buana, (5) Bagaimana memberikan rekomendasi yang tepat untuk meningkatkan pemecahan masalah sistem keamanan dan mengelola risiko pada *e-Learning* yang ada di Universitas Sangga Buana.

Tujuan dari Penelitian ini dilakukan untuk mengetahui sistem kemanan dan manajemen risiko, yaitu : (1) Untuk mengetahui dampak yang terjadi saat ini pada para pengguna terhadap sistem yang berlaku, (2) Untuk dapat mengetahui apa pendapat dari para pengguna tentang keuntungan dan kerugian dari diberlakukannya sistem kuliah online dengan menggunakan *e-Learning*, (3) Untuk mengidentifikasi sistem keamanan yang diterapkan pada sistem informasi di Universitas Sangga Buana, (4) Untuk menganalisa manajemen risiko yang dilakukan pada *e-Learning* di Universitas Sangga Buana, (5) Memberikan rekomendasi untuk meningkatkan sistem keamanan dan mengurangi jumlah risiko pada *e-Learning* di Universitas Sangga Buana.

2. Kajian Pustaka

2.1 Sistem Informasi

Sistem informasi yaitu suatu sistem yang terdapat dalam sebuah organisasi yang mana mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, dan bersifat manajerial juga kegiatan strategis dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan[6].

2.2 Audit Sistem Informasi

Audit sistem informasi merupakan kegiatan mengumpulkan dan mengevaluasi bukti yang digunakan untuk menentukan kemampuan suatu sistem komputer dalam melindungi aset, merawat integritas data, untuk mencapai tujuan organisasi dan menggunakan sumber daya yang efisien[7].

Terdapat tiga kriteria mendasar dari keamanan teknologi informasi yang harus diaudit keamanannya menurut ISACA, yaitu:

a. Kerahasiaan (*confidentiality*)
   Menjaga hak akses juga penggunaan wewenang yang bertujuan agar dapat melindungi *privacy* dan kepemilikan informasi.
b. Ketersediaan (*availability*)
   Memastikan dalam hal waktu dan kehandalan dalam mengakses dan menggunakan informasi agar selalu tersedia bagi penggunaa saat diperlukan.
c. Integritas (*integrity*)
   Menjaga informasi dari modifikasi atau perusakan dan juga biasanya termasuk untuk memastikan bahwa informasi yang tersedia merupakan informasi asli dan tidak ada penolakan (*non-repudiation*) jika dilakuan pembuktian terhadap sistem. Data harus komplit dan tidak diubah. Hilangnya integritas informasi berarti data tersebut telah tanpa adanya ijin atau ilegal[8].

2.3 NIST SP 800-26

Framework NIST SP 800-26 mengungkapkan ada setidaknya 17 kriteria yang harus dipenuhi. Kriteria tersebut, yaitu[9][10].

1. Management Control
   a. Risk Management
   b. Review of Security Controls
   c. Life Cycle
   d. Authorize Processing
   e. System Security Plan
2. Operational Control
   a. Personnel Security

b. Physical Security
c. Production, Input/Output Control
d. Contingency Planning
e. Hardware and System Software Maintenance
f. Data Integrity
g. Documentation
h. Security Awareness, Training, And Education
i. Incident Response Capability

3. Technical Control
a. Identification and Authentication
b. Logical Access Controls
c. Audit Trails

Pada NIST SP 800-26 disebutkan bahwa ada 5 tingkatan atau level keamanan pada teknologi informasi, yaitu [11] :

1. Level 1 - *Documented Policy* (Kebijakan terdokumentasi)
2. Level 2 - *Documented Procedures* (Prosedur terdokumentasi)
3. Level 3 - *Implemented Procedures and Controls* (prosedur dan pengendalian sudah dilakukan)
4. Level 4 - *Tested and Reviewed Procedures and Controls* (prosedur dan pengendalian yang telah diuji dan ditinjau)
5. Level 5 - *Fully Integrated Procedures and Controls* (prosedur dan pengendalian sudah sepenuhnya terintegrasi).

2.4 Manajemen Risiko

Manajemen risiko adalah suatu proses yang memungkinkan seorang manajer IT untuk bisa menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan juga data yang mendukung misi organisasi[11].

Manfaat dari melakukan analisis risiko yaitu menciptakan rasio *cost-to-value* yang jelas bagi perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfiguras *hardware* dan design sistem *software*[12].

Menurut Stoneburn melalui publikasi khusus framework NIST SP 800-30 tentang *Risk Management Guide For Information Technology System* mengatakan, setiap kerangka kerja yang terdapat pada manajemen risiko memiliki tahapan masing-masing. Tahapan-tahapan tersebut adalah:

1.Risk Assessment
a. Identifikasi Sistem
b. Identifikasi Ancaman
c. Identifikasi Kerentanan
d. Analisis Pengendalian
e. Penilaian Kecenderungan Risiko
f. Analisis Dampak
g. Penilaian Tingkat Risiko
h. Rekomendasi Pengendalian[11]

2.5 E-Learning

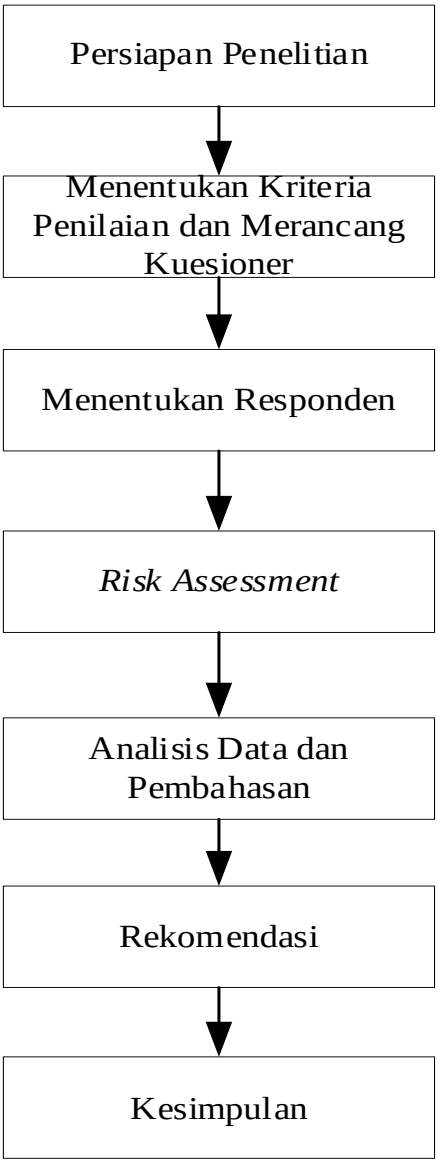
Kuliah Online atau sering disebut *e-Learning* merupakan suatu proses perkuliahan yang menggunakan media teknologi informasi dan komunikasi, dalam hal ini menggunakan internet. Dengan adanya perkuliahan online ini perkuliahan dapat dilakukan tanpa tatap

muka. Mahasiswa bisa mengikuti kuliah dari mana saja dan bisa kapan saja, selagi mereka dapat tersambung pada koneksi internet[13].

3. Metode Penelitian

3.1 Tahapan Penelitian

Penelitian ini dilakukan dalam beberapa tahapan dimulai dari persiapan penelitian sampai kesimpulan seperti pada gambar 1.



Gambar 1. Tahapan Penelitian

Tahapan dalam penelitian ini adalah:

1. Persiapan Penelitian

   Persiapan penelitian ini berupa menentukan latar belakang, mengidentifikasi dan merumuskan masalah serta menentukan tujuan yang ingin dicapai dari hasil penelitian.

Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Untuk itu maka dilakukan studi literatur dan observasi sesuai dengan teori-teori yang berhubungan dengan penelitian ini.

2. Menentukan Kriteria Penilaian dan Merancang Kuesioner
   Kriteria penelitian ditentukan berdasarkan *Framework* NIST *Special Publication* 800-26 yang dipublikasikan oleh *National Institute of Standards and Technology* dan dijadikan dasar untuk merancang kuesioner.
3. Menentukan Responden
   Responden yang ditunjuk adalah mahasiswa Univesitas Sangga Buana, Yang merupakan pengguna dari sistem *e-Learning*.
4. *Risk Assessment*
   Risk Assessment dilakukan berdasarkan tahapan yang terdapat pada *framework* NIST *Special Publication* 800-30.
5. Analisa Data dan Pembahasan
   Data yang sudah diisi oleh para responden melalui kuesioner diolah dan dianalisa untuk dapat menarik kesimpulan terkait kondisi objek penelitian.
6. Rekomendasi
   Hasil dari analisis data dan pembahasan dari penelitian yang berupa rekomendasi dari peneliti. Rekomendasi ini diberikan untuk memaksimalkan peran dari sistem.
7. Kesimpulan
   Kesimpulan Dari semua penjelasan dapat menjadi acuan untuk hasil penelitian yang akan dilakukan.

Metode penelitian yang digunakan adalah metode kuantitatif, yaitu suatu proses dengan menggunakan sekumpulan angka-angka yang digunakan untuk dapat menganalisis apa yang ingin diketahui, secara struktur dari awal hingga akhir proses perhitungan.

3.2 Teknik Pengumpulan data

Jenis data yang digunakan adalah data primer, data yang dikumpulkan dari referensi buku-buku yang berhubungan dengan penelitian. Sumber data yang dibutuhkan dalam penelitian ini diperoleh dari beberapa data yang di dapat yaitu dari bagian Teknologi Informasi yang berhubungan dengan sistem *e-Learning* Universitas Sangga Buana. Dalam pengumpulan data menggunakan 3 metode, yaitu :

1. Observasi, untuk mendapatkan data primer dengan mengamati objek penelitian.
2. Wawancara, dengan melakukan tanya jawab secara langsung untuk mendapatkan data yang dibutuhkan dari objek penelitian.
3. Kuesioner, memberikan sebuah pernyataan yang diberikan kepada responden untuk dijawab.

3.3 Acunetix

Acunetix merupakan sebuah alat yang banyak digunakan oleh para pengembang website untuk dapat melihat keamanan pada sebuah *website* yang digunakan. Aplikasi ini akan melakukan pemindaian pada *website* yang ingin diketahui sejauh mana keamanan yang telah dijalankan pada *website*. Dengan menggunakan aplikasi ini, pengembang dapat memperbaiki kelemahan dalam *website* yang digunakan untuk mengurangi kelemahan dalam keamanan sebuah situs website[14][15].

3.4 Populasi

Kumpulan atau total dari sampel yang digunakan. Maka dari itu, yang menjadi populasi dari penelitian ini adalah mahasiswa Universitas Sangga Buana.

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

3.5 Sampel

Merupakan sebagian dari populasi yang dijadikan objek penelitian. Yang menjadi sampel pada penelitian kali ini adalah mahasiswa Universitas Sangga Buana sebagai pengguna fasilitas tersebut. Mahasiswa yang dijadikan sampel adalah mahasiswa mulai dari mahasiswa semester 3 keatas, dikarenakan sudah lebih sering menggunakan *e-Learning* Universitas Sangga Buana. Pengetahuan dari responden tentang keamanan sistem tidak diutamakan karena kuesioner mengacu pada standar yang diberikan NIST yang berisi tentang pertanyaan secara umum tentang *e-Learning*.

4. Hasil dan Pembahasan

Hasil dari penelitian ini berupa tingkat keamanan dan manajemen risiko yang terdapat pada sistem *e-Learning*. Untuk mengetahui hasil keamanan dilakukan penilaian dari hasil perhitungan yang didapatkan dari jawaban responden, yaitu mahasiswa sebagai pengguna sistem kuliah online, dan kuesioner sudah sesuai standar NIST sehingga responden dapat menjawab pertanyaan secara umum yang meliputi sistem kuliah online tanpa memandang tingkat pengetahuan dan kemahiran responden terhadap *cybersecurity*. Penilaian tingkat manajemen risiko pada sistem *e-Learning* dilakukan dengan menggunakan *tools* acunetix untuk mengetahui sejauh mana kerentanan yang terdapat pada sistem *e-Learning*.

4.1 Tingkat Keamanan

4.1.1 Penilaian Tingkat Manajemen Risiko

Pada Tabel 1 memperlihatkan hasil dari penilaian manajemen risiko pada *e-Learning* Universitas Sangga Buana yang dapat dilihat sebagai berikut:

Tabel 1. Penilaian Manajemen Risiko

No	Sub Kriteria Pertanyaan	Skala Likert					Jumlah Responden	Jumlah data	Rata-Rata	Persentase (%)
		5	4	3	2	1				
1	Apakah harus dilakukan backup secara rutin terhadap data yang ada di sistem e-learning	27	55	13	2	3	100	401	4,01	80,20
2	Apakah perlu menerapkan pengamanan untuk melindungi aset yang berhubungan dengan yang ada di sistem e-learning	51	41	7	0	1	100	441	4,41	88,20
3	Apabila terjadi salah input tapi sudah dilakukan penyimpanan, apakah sistem perlu memberikan keterangan gagal/salah	46	44	9	0	1	100	434	4,34	86,80
4	Apakah pengguna diberikan pelatihan (training) oleh pihak Teknologi Informasi (TI) sebelum sistem diimplementasikan	25	36	25	9	5	100	367	3,67	73,40
5	Apakah perlu adanya pengamanan khusus untuk privasi pengguna	45	44	11	0	0	100	434	4,34	86,80
Jumlah		194	220	65	11	10	500	2077	20,77	415,40
Rata-Rata Keseluruhan									4,154	83,08

Pada proses kategori pengendalian manajemen memiliki nilai persentase mencapai 83,08%. Berdasarkan hasil ini bisa diketahui bahwa tingkat keamanan yang sudah diterapkan pada sistem kuliah online untuk kategori pengendalian manajemen (*management control*) pada manajemen risiko sudah berada pada level 4, yaitu prosedur dan kontrol yang diuji serta dievaluasi pada pengendalian sudah diimplementasikan secara konsisten. Berdasarkan

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

penjelasan yang merujuk pada NIST SP 800-26 menjelaskan tentang level keamanan teknologi informasi.

Dampak adanya sistem ini bisa dilihat dengan nilai persentase keseluruhan dengan mencapai nilai 83,08%. Manajemen risiko yang baik membantu meminimalisir banyaknya kesalahan maupun keluhan yang dirasakan para *user*.

4.1.2 Penilaian Tingkat Produksi, Pengendalian *Input/Output*

Tahapan penilaian tingkat produksi, pengendalian input/output yang dapat dilihat pada tabel 2 sebagai berikut.

Tabel 2. Penilaian Tingkat Produksi, Pengendalian Input / Output

No	Sub Kriteria Pertanyaan	Skala Likert					Jumlah Responden	Jumlah data	Rata-Rata	Persentase (%)
		5	4	3	2	1				
1	Apakah terdapat bantuan bagi pengguna untuk menggunakan sistem e-learning	22	44	22	10	2	100	374	3,74	74,80
2	Apakah terdapat saran bantuan yang ditawarkan oleh pihak Teknologi Informasi (TI)	18	42	23	15	2	100	359	3,59	71,80
3	Apakah terdapat proses untuk memastikan bahwa hanya pengguna yang sah yang dapat menggunakan sistem e-learning	18	47	22	9	4	100	366	3,66	73,20
4	Apakah tampilan layar untuk input mudah dimengerti oleh pengguna	13	44	26	15	2	100	351	3,51	70,20
5	Apakah terdapat proses untuk memastikan bahwa orang yang tidak berwenang tidak dapat mengetahui identitas pengguna ataupun mengubah informasi	22	31	20	25	2	100	346	3,46	69,20
	Jumlah	93	208	113	74	12	500	1796	17,960	359,20
	Rata-Rata Keseluruhan								3,592	71,84

Pada proses kategori pengendalian operasional memiliki nilai yang diperoleh dari produksi, pengendalian *input*/*output* mencapai nilai persentase 71,84%. Berdasarkan hasil ini bisa diketahui bahwa tingkat keamanan yang sudah diterapkan pada sistem kuliah online untuk kategori pengendalian operasional (*operational control*) pada produksi, pengendalian *input/output* sudah berada pada level 3 (*Implemented Procedures and Controls*), yaitu prosedur dan pengendalian kontrol keamanan sudah dilakukan secara konsisten merujuk pada NIST SP 800-26 yang menjelaskan tentang level keamanan teknologi informasi.

4.1.3 Penilaian Tingkat Kemampuan Respon Insiden

Pada tabel 3 memperlihatkan penilaian kemampuan respon terhadap suatu insiden pada sistem, dapat dilihat pada tabel 3.

Tabel 3. Penilaian Kemampuan Respon Insiden

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

No	Sub Kriteria Pertanyaan	Skala Likert					Jumlah Responden	Jumlah data	Rata-Rata	Persentase (%)
		5	4	3	2	1				
1	Apakah ada kemampuan untuk memberikan bantuan kepada pengguna ketika insiden keamanan terjadi dalam sistem	16	30	33	16	5	100	336	3,36	67,20
2	Apakah kemampuan dalam memberikan respon insiden harus dalam penyampaiannya	17	52	23	5	3	100	375	3,75	75,00
3	Menurut anda apakah terdapat proses untuk melaporkan insiden	15	46	21	17	1	100	357	3,57	71,40
4	Apakah keterangan insiden dapat diketahui sudah diterima dan ditanggapi	13	38	27	18	4	100	338	3,38	67,60
5	Apakah saat terjadi insiden perlu dilacak sampai terselesaikan	43	45	9	3	0	100	428	4,28	85,60
Jumlah		104	211	113	59	13	500	1834	18,34	366,80
Rata-Rata Keseluruhan									3,668	73,36

Pada proses kategori pengendalian operasional memiliki nilai yang diperoleh dari kemampuan respon insiden mencapai nilai persentase 73,36%. Berdasarkan hasil ini bisa diketahui bahwa tingkat keamanan yang sudah diterapkan pada sistem kuliah online untuk kategori pengendalian operasional (*operational control*) pada kemampuan respon insiden sudah berada pada Level 3 (*Implemented Procedures and Controls*), yaitu prosedur dan pengendalian kontrol keamanan sudah dilakukan secara konsisten. Berdasarkan penjelasan yang merujuk pada NIST SP 800-26 menjelaskan tentang level keamanan teknologi informasi.

Dalam pengendalian operasional pada sistem kuliah online ini dapat dikatakan sudah baik dengan jumlah jawaban tertinggi persentase keseluruhan mencapai 71,84% pada proses *input/output*. Selain itu, untuk respon insiden memiliki jumlah nilai persentase keseluruhan mencapai 73,36%.

4.1.4 Penilaian Keseluruhan

Dari tabel penilaian yang sudah dipaparkan sebelumnya mulai dari penilaian manajemen resiko, penilaian produksi, kontrol *input/output* dan penilaian kemampuan respon terhadap insiden maka tiga penilaian tersebut dikalkulasikan pada sebuah tabel penilaian keseluruhan yang dapat dilihat pada tabel 4.

Tabel 4. Penilaian Keseluruhan

No	Sub Kriteria Pertanyaan	Rata-Rata	Persentase (%)
1	Manajemen Resiko	4,154	83,08
2	Produksi, Kontrol Input / Output	3,592	71,84
3	Kemampuan Respon Insiden	3,668	73,36
Rata-rata Total		3,805	76,09

Pada proses perhitungan pada tingkat keamanan keseluruhan memiliki nilai yang diperoleh mencapai nilai persentase 76,09%. Berdasarkan hasil ini bisa diketahui bahwa tingkat keamanan yang sudah diterapkan pada sistem kuliah online untuk tingkat keamanan

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume 11 Nomor 1 Edisi April 2021
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

keseluruhan berada pada level 3 (*Implemented Procedures and Controls*), yaitu prosedur dan pengendalian kontrol keamanan sudah dilakukan secara konsisten berdasarkan penjelasan yang merujuk pada NIST SP 800-26 tentang level keamanan teknologi informasi.

4.2 Risk Assessment Berbasis NIST 800-30

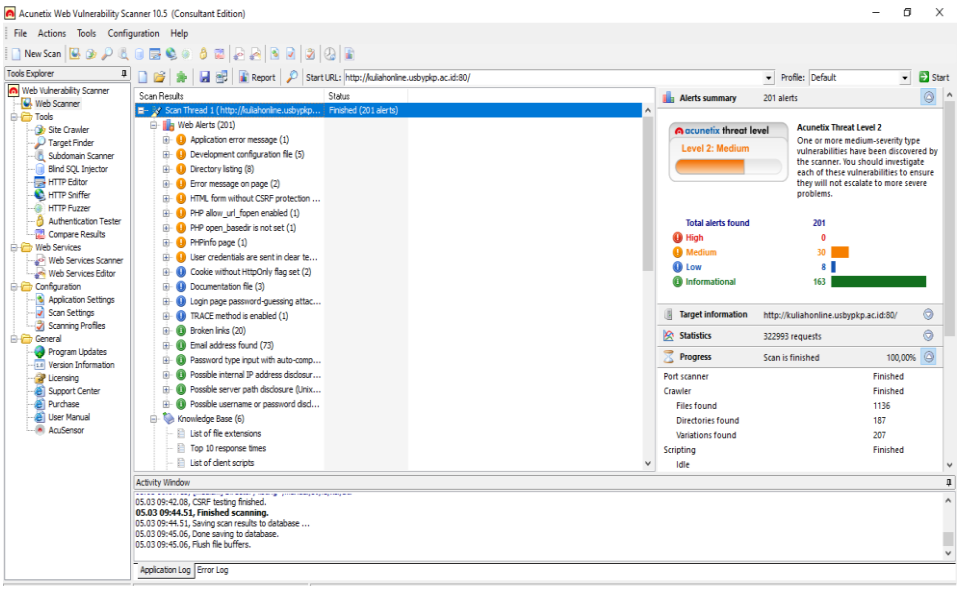
4.2.1 Identifikasi Ancaman

Dalam *framework* NIST SP 800-30 tercantum beberapa ancaman yang dapat mengakibatkan terganggunya proses sistem informasi, ancaman tersebut terbagi menjadi 3 (tiga) jenis ancaman yaitu:

a. Ancaman alam (*natural threat)* ialah ancaman yang berasal dari alam dan dapat terjadi secara mendadak.
b. Ancaman manusia (*human threat*) ialah ancaman yang berasal dari tingkah laku manusia yang ingin mendapatkan keuntungan pribadi maupun kelompok dan dilakukan dengan sengaja ataupun tidak disengaja.
c. Ancaman lingkungan (*environmental threat*) ialah ancaman yang bisa terjadi karena kondisi lingkungan yang berubah dan bisa mendukung ancaman tersebut menjadi kenyataan pada sistem.

4.2.2 Hasil Identifikasi Kerentanan

Hasil *scanning* sistem keamanan pada website e-Learning Universitas Sangga Buana (seperti pada gambar 2) memiliki kerentanan pada level *medium* (2). Sistem ini berada di level 2, dengan total peringatan kerentanan mencapai 201 buah. Tidak ditemukannya kerentanan yang tinggi dalam sistem ini hanya terdapat kerentanan yang *medium* dengan total peringatan mencapai 30 buah, kerentanan yang *low* dengan total peringatan mencapai 8 buah, dan yang bersifat *informational* mencapai 163 buah. Dengan demikian, sistem kuliah online ini bisa berada pada level *medium* (2).



Gambar 2. Hasil Scan Kerentanan Menggunakan Acunetix

4.2.3 Analisis Pengendalian

Sistem kuliah online menggunakan sistem operasi centOS 8 yang merupakan versi terbaru linux. Dalam sistem kuliah online menggunakan firewall Iptabless dan UFW untuk membantu mengidentifikasi dan memulihkan masalah dari kerentanan keamanan hingga masalah stabilitas. Hal ini dapat membantu administrator menghindari masalah dan waktu henti yang tidak direncakanan dilingkungan sekitar.

4.2.4 Penilaian Kecenderungan Risiko

Kecenderungan terhadap terjadinya risiko dapat dilihat sesuai dengan jenis ancaman yang mungkin menyerang, baik itu terhadap sistem maupun terhadap fisik servernya. Kecenderungan akan ancaman tersebut terhadap Universitas Sangga Buana adalah sebagai berikut.

1. *Natural threat*, bisa dikatakan tidak pernah terjadi karena lokasi Universitas Sangga Buana berada pada lokasi yang terlepas dari kemungkinan terjadinya bencana. Untuk kebakaran, disetiap tempat-tempat yang rentan kebakaran sudah disediakan Alat Pemadam Api Ringan (APAR) dan pihak instituti sudah melakukan kegiatan sesuai dengan standar opersional prosedur (SOP) dengan baik dan maksimal. Oleh karena itu, kecenderungan terjadinya *Natural threat* bisa dikategorikan rendah (*low*).
2. *Human threat* dapat terjadi karena tindakan yang disengaja maupun tidak oleh seseorang atau sekelompok manusia. Tindakan yang dapat dilakukan adalah dengan mengincar secara melewati sistem dengan menembus keamanan sistem ataupun dengan melakukan tindakan secara fisik atau langsung pada server sistem kuliah online. Untuk mengantisipasi hal tersebut pihak Information Teknology (IT) telah melakukan antisipasi pada keamanan sistem dengan menggunakan *firewall* Iptabless. Sedangkan untuk mengantisipasi secara fisik sudah terpasang CCTV untuk memantau keadaan disekitar server. Untuk itu, kecenderungan yang dapat terjadinya human threat dapat dikategorikan rendah (*low*).
3. *Environmental threat* dapat terjadi karena keadaan sekitar sistem/server yang berubah dan dapat mendukung terjadinya ancaman. Untuk menghindari kerusakan pada server dalam lingkungan sekitar, pihak *Information Teknology* (IT) telah menerapkan semua proses prosedur yang sesuai dengan yang berlaku untuk mengurangi ancaman tersebut. Oleh karena itu, kecenderungan yang dapat terjadinya *environmental threat* dapat dikategorikan rendah (*low*).

4.2.5 Analisis Dampak

Dampak yang ditimbulkan akibat dari terjadinya risiko pada sistem informasi akademik dapat menyerang *hardwre*, *software*, maupun data dan informasi yang tersimpan dalam server. Dampak tersebut bergantung pada risiko yang terjadi. Beberapa dampak yang dapat terjadi antara lain.

1. Dampak yang dapat menyebabkan fisik *hardware* server rusak bisa berupa banjir. Server akan mengalami kerusakan dan data yang sudah disimpan bisa hilang karena sistem tidak bisa dipakai ulang bila terbawa banjir.
2. Dampak yang menjadi server rusak atau berubah adalah masuknya *hacker*. Dengan masuknya *hacker* yang dapat dilakukan berupa merubah data dan informasi yang sudah ada, mengambil informasi penting yang ada didalam sistem, dan merusak sistem yang sudah dibuat sesuai keperluan pihak institusi.
3. Penggunaan disekitar yang terus meningkat atau melebihi kapasitas *hardware* server dalam satu sesi dapat mengakibatkan kerusakan pada hardware server tersebut. Dengan terjadinya kerusakan pada sistem maka akan menghambat proses sistem kuliah online

yang sedang berjalan.

4.2.6 Penilaian Tingkat Risiko

Tingkat risiko yang mungkin terjadi terhadap sistem yang ada di Universitas Sangga Buana dapat ditentukan. Tingkat risiko pada Universitas Sangga Buana tersebut, yaitu:

1. Kebakaran menjadi ancaman alam yang akan serius jika terjadi. Tingkat risiko kebakaran yang terjadi pada sistem kuliah online Universitas Sangga Buana dapat dikatakan tinggi. Karena tidak akan hanya berupa server yang rusak dan kehilangan data, tetapi infrastruktur bangunan pun akan mengalami kerusakan. Untuk meminimalisir terjadi kebakaran pihak institusi telah menyediakan Alat Pemadam Api Ringan (APAR), melakukan aktifitas sesuai prosedur, dan meningkatkan keselamatan dalam bekerja.
2. *Hacker* termasuk ancaman yang memiliki dampak tinggi dalam risiko pada sebuah sistem. *Hacker* akan menembus sistem dengan cara merusak data keamanan ataupun dengan cara baru agar dapat masuk ke dalam sistem yang diinginkannya. Dalam mencegah masuknya *hacker*, pihak institusi melakukan pencegahan dengan memasang firewall Iptables dan UFW yang ada pada centOS 8 versi terbaru. Maka dari itu, tingkat risiko terjadinya *hacker* pada sistem kuliah online di Universitas Sangga Buana termasuk ke dalam kategori rendah.
3. Beberapa ancaman yang berasal dari lingkungan diantaranya kerusakan yang diakibatkan oleh penggunaan yang melebihi kapasitas sistem. Kerusakan ini dapat terjadi karena lingkungan sekitar bertambah dengan tidak dilakukannya penambahan kapasitas sesuai kebutuhan lingkungan yang berubah. Untuk mengantisipasi hal ini dari pihak Information Teknology (IT) perlu melakukan penambahan kapasitas secara berkala sesuai dengan kebutuhan yang diperlukan. Berdasarkan hal tersebut, tingkat risiko pada lingkungan dapat dikatakan kecil.

4.2.7 Rekomendasi Pengendalian

Dari hasil pencapaian tingkat keamanan sistem kuliah online yang ada pada Universitas Sangga Buana memiliki nilai rata–rata 76,09% atau pada level 3 (*Implemented Procedures and Controls*). Sementara itu level yang hendak dicapai adalah level 4 (*Tested and Review Procedures and Controls*). Untuk dapat mencapai level tersebut, berdasarkan *framework NIST* SP 800-26 sebaiknya dilakukan beberapa aktivitas rekomendasi yang sesuai dengan kriterianya, yaitu:

1. Pihak institusi mengembangkan program yang efektif untuk mengevaluasi kecukupan dan efektifitas kebijakan keamanan, prosedur, dan pengendalian.
2. Pihak institusi melakukan kontrol setiap kali ada perubahan sistem yang signifikan saat mengalami perubahan.
3. Pihak institusi melakukan pengecekan kerentanan yang diungkapkan oleh insiden keamanan atau peringatan keamanan.
4. Pihak institusi harus secara rutin menganalisis catatan insiden keamanan, yang merupakan aktivitas tidak wajar atau mencurigakan pada sistem keamanan.
5. Pihak institusi melakukan perpindahan ke PC khusus server.

5. Kesimpulan

Dari hasil penelitian yang telah dilakukan pada sistem kuliah online di Universitas Sangga Buana, dapat diambil kesimpulan sebagai berikut: (1) Dampak adanya sistem ini memiliki nilai persentase keseluruhan dengan mencapai nilai 83,08%, bisa dikatakan dampaknya sangat diperlukan untuk membantu proses perkuliahan saat ini dan dapat terus

digunakan. (2) Dalam pengendalian operasional pada sistem kuliah online ini memiliki nilai persentase keseluruhan mencapai 71,84% pada proses *input/output* dan respon insiden memiliki nilai persentase keseluruhan mencapai 73,36%. Dengan kondisi fitur yang ada saat ini sudah cukup baik tetapi masih perlu adanya pengembangan untuk meningkatkan kualitas pengendalian opersional. (3) Berdasarkan penilaian hasil audit pada sistem kuliah online di Universitas Sangga Buana memiliki nilai rata-rata keseluruhan untuk tingkat keamanan keseluruhan dengan nilai persentase mencapai 76,09%. Dapat disimpulkan bahwa keamanan pada sistem informasi akademik tersebut berada pada level 3, *implemented procedures and control*. (4) Pada penilaian kerentanan dan risiko dengan menggunakan aplikasi Acunetix pada website kuliahonline.usbypkp.ac.id menghasilkan total peringatan kerentanan mencapai 201 buah. Dengan tidak ditemukannya kerentanan yang tinggi dalam sistem ini hanya terdapat kerentanan yang *medium* dengan total peringatan mencapai 30 buah, kerentanan yang *low* dengan total peringatan mencapai 8 buah, dan yang bersifat *informational* mencapai 163 buah. (5) Rekomendasi yang dapat diberikan terkait hasil penilitian antara lain melakukan mengembangkan dan memperbaiki program yang efektif untuk meminimalisir kerentanan, melakukan kontrol secara berkala untuk mengurangi masalah keamanan, secara rutin menganalisis catatan insiden keamanan, melakukan perpindahan ke PC khusus *server*, dan dapat mendokumentasikan semua aktivitas yang dilakukan *user*.

Daftar Pustaka

[1] H. Tohidi, "The Role of Risk Management in IT systems of organizations," *Procedia Computer Science*, vol. *3*, pp. 881-887, 2011.

[2] E. Supristiowadi dan Y.G. Sucahyo, "Manajemen Risiko Keamanan Informasi Pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan," *Indonesian Treasury Review: Jurnal Perbendaharaan, Keuangan Negara dan Kebijakan Publik*, vol. *3*, *no.* 1, pp. 23-33, 2018.

[3] R. S. Perdana, "Audit Keamanan Sistem Informasi Akademik Menggunakan Framework NIST SP 800-26 (Studi Kasus: Universitas Sangga Buana YPKP Bandung)," J. Infotronik, 2018.

[4] A. Rezakhani, A. Hajebi, and N. Mohammadi. "Standardization of all information security management systems," *International Journal of Computer Applications*, vol.*18 no.* 8, pp. 4-8, 2011.

[5] D. A. Jakaria, R. T. Dirgahayu, and Hendrik, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro," in Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2013, pp. E37–E42.

[6] H. M. Jogiyanto, "Analisa dan Desain Sistem Informasi, edisi kedua," Yogyakarta Andi Offset, 2005.

[7] Evi Maria and Endang Haryani, "Audit Model Development Of Academic Information System: Case Study On Academic Information System Of Satya Wacana," J. Arts, Sci. Commer., E-Vol.– I, no. Issue –2, p. ISSN 2229-4686, ISSN 2231-4172.

[8] ISACA (Information System Audit and Control Association), IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance Control Professionals. 2010.

[9] M. Swanson, "Security Self-Assessment Guide for Information Technology Systems," NIST Spec. Publ. 800-26, 2001.

[10] E. Jonsson and L. Pirzadeh, "Identifying Suitable Attributes for Security and Dependability Metrication," *SECURWARE 2013 The Seventh International*

Conference on Emerging Security Information, Systems and Technologies, pp. 1-7, 2013.

[11] et al Stoneburner, "Risk Management Guide for Information Technology Systems," NIST Spec. Publ. 800-30, 2002.

[12] R. L. dan D. R. V. Krutz, The CISSP Prep Guide – Mastering the Ten Domains of Computer Security. CA: Wiley Computer Publishing John Wiley & Sons, Inc, 2006.

[13] K. Praktis, "Pengertian dan Proses Kuliah Online - Sistem Perkuliahan Berbasis Daring," 2018. https://www.komunikasipraktis.com/2018/05/pengertian-proses-kuliah-online-daring.html (accessed Aug. 07, 2020).

[14] Acunetix, "Introduction to Acunetix - Why You Need To Secure Your Web Applications." https://www.acunetix.com/support/docs/introduction/ (accessed Aug. 07, 2020).

[15] Centerklik, "Amankan Website Dengan Acunetix Web Vulnerability Scanner," 2016. https://www.centerklik.com/amankan-website-dengan-acunetix-web-vulnerability-scanner (accessed Aug. 07, 2020).