MANAJEMEN RISIKO APLIKASI PEMBELAJARAN BERBASIS ONLINE PADA UNIVERSITAS DENGAN MENGGUNAKAN METODE OKTAVE ALLEGRO

[1)]Henki Bayu Seta, [2)]Theresiawati, [3)]Tri Rahayu

[1)] Teknik Informatika UPN "Veteran"Jakarta
[2,3)] Manajemen Informatika UPN "Veteran"Jakarta
Jl RS. Fatmawati, Pondok Labu, Jakarta Selatan 12450
Email : henkiseta@upnvj.ac.id[1] theresiawati@upnvj.ac.id[2],

Abstrak

Keamanan informasi beserta asset –asetnya merupakan hal yang sangat penting bagi pihak organisasi. Banyak dampak negatif yang ditimbulkan bagi organisasi jika keamanan informasi tidak dijaga dengan baik. Untuk menjaga keamanan informasi diperlukan penilaian risiko sistem informasi terkait dengan core bisnis organisasi UPN "Veteran" Jakarta yaitu pembelajaran dan pengajaran.

UPN "Veteran" Jakarta belum pernah melakukan penilaian manajemen risiko pada aplikasi pembelajaran berbasis online (e-learning) untuk melindungi asset dan menjaga keberlangsungan proses bisnis pada UPN "Veteran" Jakarta. Metode yang digunakan yaitu Metode OCTAVE Allegro terdiri dari empat fase yaitu membangun drivers (establish drivers), membuat profil aset informasi (profile assets), mengidentifikasi ancaman (identify threats) mengidentifikasi dan mengurangi risiko (identify and mitigate risks).

Hasil akhir dari penelitain ini yaitu berupa rekomendasi pendekatan mitigasi untuk perlindungan system informasi diantaranya mengadakan training secara regular terhadap staff mengenai tanggung jawab dalam melindungi informasi asset dan dilakukan penyuluhan mengenai pentingnya keamanan password, melakukan pergantian password secara berkala kepada seluruh pengguna e-learning, jika terjadi penyebaran password maka staff yang bersangkutan akan dikenakan sanksi, menambahkan fungsi log transaksi dan mereview log secara berkala serta menambahkan fungsi logout otomatis jika lebih dari lima menit tidak ada aktivitas.

Kata kunci: *Manajemen Risiko, Octave Allegro, Keamanan Informasi,*

1. Pendahuluan

Keberlangsungan proses bisnis dapat terganggu jika aplikasi pembelajaran online ini mengalami suatu gangguan baik karena kesalahan teknis, kesalahan perangkat keras, kesalahan di dalam penulisan sintak perangkat lunak, kesalahan logika, gangguan lingkungan, kegagalan arus listrik karena petir dan kesalahan manusia. Untuk mencegah terjadinya hal tersebut, perlu dilakukan manajemen risiko yang dapat mengurangi dampak kerusakan, diantaranya yaitu dampak terhadap financial, penurunan reputasi Universitas, terganggu dan terhentinya proses bisnis dan lain sebagainya.

Secara rinci permasalahan penelitian ini dapat diajukan dalam beberapa pertanyaan penelitian sebagai berikut:

- Bagaimana pihak manajemen melakukan penilaian risiko dan menjaga keberlangsungan proses bisnis pada aplikasi pembelajaran secara online (e-learning) Universitas Pembangunan Nasional "Veteran" Jakarta?
- Bagaimana mendeskripsikan dan mengidentifikasi Resiko keamanan aplikasi pembelajaran secara online (e-learning) pada e-learning UPN "Veteran" Jakarta dengan menggunakan Metode Octave Allegro ?
- Bagaimana tindakan mitigasi yang dilakukan terhadap resiko-resiko yang mungkin terjadi?

Tujuan Penelitian

- Untuk mendeskripsikan dan mengidentifikasi Resiko keamanan aplikasi pembelajaran berbasis online pada e-learning UPN "Veteran" Jakarta
- Untuk mengukur keamanan yang telah diterapkan
- Untuk membuat tindakan mitigasi terhadap risiko-risiko yang mungkin terjadi.

Manajemen risiko merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja [1].

OCTAVE Allegro merupakan salah satu metoda manajemen risiko sistem informasi yang dapat diterapkan pada perguruan tinggi tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya [1]. Serangkaian langkah dalam penilaian risiko adalah:

Step 1 – Establish risk measurement criteria. Menetapkan kriteria pengukuran risiko. *Impact area* yang dipilih adalah reputasi dan kepercayaan pelanggan, financial, produktivitas, keamanan dan kesehatan, dan denda dan penalti. Kemudian dilakukan penilaian kondisi, *low* (kecil) jika hanya sedikit terpengaruh dan hampir tidak ada usaha dibutuhkan dalam perbaikan reputasi, *moderate* (sedang) apabila terkena dampak buruk dan diperlukan usaha dan biaya dalam perbaikan dan *high* (tinggi) jika dampak yang disebabkan sangat buruk dan hampir tidak dapat diperbaiki.

Step 2 – Develop and Information Asset Profile, aset informasi kritikal yang berhasil diidentifikasikan dalam penulisan ini adalah Profil Dosen, Profile Mahasiswa, Transaksi Nilai Mahasiswa, Konten Materi Kuliah, Soal – soal latihan dan ujian, Informasi Akademik, Matakuliah dan Tugas Mahasiswa

Step 3 – Identify Information Asset Containers: Information asset containers. Dengan Menggunakan worksheet *Information Asset Risk Environment Map*, peneliti mengidentifikasikan kontainer dimana aset informasi berada, yang dibagi dalam tiga kategori, Technical, Physical dan People

Step 4 – Identify Areas of Concern. Langkah 4 dilakukan dengan cara Melakukan review terhadap setiap *container* yang telah didaftarkan untuk melihat *areas of concern* yang potensial. Mendokumentasikan setiap *area of concern* yang diidentifikasikan pada *Information Asset Risk Worksheet.* Pada *worksheet* ini, catat nama dari *information asset* dan dokumentasikan *area of concern* sedetil mungkin. Perluas *areas of concern* untuk menghasilkan *threat scenarios*. *Threat scenario* merupakan detil atribut dari *threat*. Dokumentasikan bagaimana *threat* yang disebut mempengaruhi *security requirement* yang telah diatur untuk *information asset*. Teruskan aktivitas ini untuk setiap *Information Asset Risk Worksheet* sampai semua *areas of concern* telah mendetail. Informasi yang tersisa akan dikumpulkan di langkah selanjutnya.Lanjutkan dengan setiap *container* yang didaftarkan pada *Information Asset Risk Environment Maps* dan dokumentasikan *areas of concern* sebanyak mungkin.

Step 5 – Identify Threat Scenarios. Langkah 5 dilakukan dengan cara melengkapi *Information Asset Risk Worksheet*s untuk tiap *Threat scenarios* umum yang diidentifikasikan. Dan menentukan probabilitas kedalam deskripsi *Threat scenario* yang telah dibuat pada *Information Asset Risk Worksheet*s.

Step 6 – Identify Risks. Mengidentifikasi dampak *high* (tinggi) , *medium*, dan *low* untuk universitas dan menghitung *relative risk score.scenario* yang telah dicatat dalam dapat memberikan dampak bagi Universitas.

*Step 7 – Analyze Risks. M*elakukan review *risk measurement criteria* yang telah ditetapkan pada langkah 1. Mulai dengan *risk worksheet* yang pertama, lakukan *review* dari pernyataan konsekuensi yang telah dicatat. Dan dilakukan perhitugan *relative risk score* yang akan digunakan untuk menganalisa resiko dan membantu organisasi untuk memutuskan strategi terbaik menghadapi risiko.

Step 8 – Select Mitigation Approach. Melakukan penyotiran tiap - tiap risiko yang telah diidentifikasikan berdasarkan nilai resiko. Resiko – resiko yang telah terindentifikasi dikategorikan berdasarkan *relative risk score* yang dimiliki. Selanjutnya diambil langkah mitigasi risiko – risiko tersebut.

Tahun 2013 Jakaria [1], melakukan penelitian mengenai manajemen risiko sistem informasi akademik. Hasil penelitiannya menyatakan octave allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perguruan tinggi tanpa memerlukan keterlibatan yang ekstensif didalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada asset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi. Pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga asset informasi kritikal secara tepat serta langkah – langkah pemulihan jika skenario ancaman benar – benar terjadi.

2. Pembahasan

Langkah 1 - *Establish Risk Measurement Criteria*. Dilakukan melalui wawancara terhadap pengelola e-learning, stakeholder atau pengguna e-learning yaitu dosen dan mahasiswa. Berdasarkan hasil wawancara dan diskusi, kriteria pengukuran resiko ditentukan. Ada dua aktivitas yang dilakukan di langkah 1 ini, yaitu penentuan *impact area*, dan penentuan skala prioritas pada *impact area* yang telah ditentukan. Impact area yang dipilih yaitu dipilih adalah reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dan kesehatan, dan denda dan penalti.

Tabel 1. *Impact Area* – Reputasi dan Kepercayaan Pelanggan

	Impact Area	Low	Moderate	High
Reputasi dan kepercayaan pelanggan	*Reputation*	Reputasi sedikit terpengaruh;tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk,dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
	Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

Impact area Reputasi dan kepercayaan yang dijadikan acuan yaitu *Reputation* dan *Customer loss.* Untuk

impact area Reputasi dan kepercayaan pelanggan, yang dijadikan acuan yaitu *reputation* (dampak terhadap reputasi perusahaan), *low* (kecil) jika reputasi hanya sedikit terpengaruh dan hampir tidak ada usaha dibutuhkan dalam perbaikan reputasi, *moderate* (sedang) apabila reputasi terkena dampak buruk dan diperlukan usaha dan biaya dalam perbaikan reputasi dan *high* (tinggi) jika dampak yang disebabkan sangat buruk dan reputasi hampir tidak dapat diperbaiki. *Customer Loss* atau kerugian pelanggan (dampak terhadap berkurangnya jumlah pelanggan), pengurangan pelanggan yang diakibatkan hilangnya kepercayaan adalah kurang dari 2% untuk kategori *low (*kecil), antara 2% - 10% untuk kategori *moderate* (sedang), dan lebih dari 10% untuk kategori *high* (tinggi).

Aktivitas selanjutnya adalah penentuan skala prioritas. *Impact area* yang lebih penting memiliki nilai skala prioritas yang lebih besar. Hasil dari aktivitas ini akan digunakan nanti di dalam penilaian risiko untuk mengembangkan nilai risiko relatif yang dapat membantu UPNVJ dalam menangani resiko yang telah diidentifikasi didalam penilaian.

Tabel 2. Skala Prioritas Impact Area

Priority	Impact Areas
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
2	Keamanan dan Kesehatan
1	Denda dan Penalti

Langkah 2 – Develop Information Asset Profile
Assessment dilakukan dengan berfokus pada *e-learning* sistem pembelajaran online yang digunakan untuk melakukan proses pembelajaran, *core process*nya yaitu pengajaran dan pembelajaran. Berdasarkan hasil wawancara dan diskusi dengan pengelola dan pengguna *e-learning*, peneliti melakukan mapping akan aset – aset yang penting dan kontainer teknikal yang mana dapat menyimpan, mengakses, dan memproses informasi tersebut. Asset informasi kritikal yaitu Profil Dosen, Profile Mahasiswa, Transaksi Nilai Mahasiswa, Konten Materi Kuliah, Soal – soal latihan dan ujian, Informasi Akademik, Matakuliah, Tugas Mahasiswa

Untuk langkah 3 sampai langkah 8 menggunakan *critical information asset profile* dalam bentuk *worksheet.* Dibawah ini merupakan penjelasan mengenai asset informasi kritikal di atas, terkait dengan aspek *rationale for selection, description, owner, security requirement,* dan *most important security requirement. Security requirement* terbagi lagi menjadi tiga bagian, yaitu *confidentiality*, *integrity*, dan *availability*. Penjelasan di bawah ini merupakan hasil mapping dari *information asset profiling* yang telah dilakukan sebelumnya.

Tabel 3. *Information asset profiling* - Transaksi Nilai Mahasiswa

Critical Asset		Transaksi Nilai Mahasiswa
Rationale for Selection		Informasi mengenai nilai yang didapat mahasiswa ketika mengerjakan tugas dan soal latihan yang diberikan oleh dosen
Description		Aset ini berisi nilai - nilai setiap aktifitas yang diberikan
Owner		UPT.Puskom
Security Requirement	*Confidentiality*	Informasi mengenai nilai bersifat pribadi hanya untuk mahasiswa yang mendapatkan nilai yang berhak mengetahui nilai yang diterimanya
	Integrity	nilai hanya dapat diisi oleh dosen yang mengampu matakuliah yang bersangkutan
	Availability	informasi nilai harus tersedia untuk mahasiswa
Most Important Security Requirement		Integrity Alasan: karena nilai bisa berpengaruh terhadap total keseluruhan nilai yang akan didapat oleh mahasiswa pada matakuliah tertentu

Langkah 3 – *Identify Information Asset Containers*
Mengidentifikasikan *information asset containers* (kontainer yang mana aset informasi disimpan, dipindahkan, atau diproses). Menggunakan worksheet *Information Asset Risk Environment Map*, peneliti mengidentifikasikan kontainer dimana aset informasi berada, yang dibagi dalam tiga kategori, yaitu Technical, Physical, People.

Tabel 4 *Information Asset Risk Environment Map* - Transaksi Nilai Mahasiswa

Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	Owner(s)
Aplikasi : elearning data transaksi nilai mahasiswa disimpan di database elearning	UPT.Puskom
External	
Container Description	Owner(s)
Information Asset Risk Environment Map (Physical)	
Internal	
Container Description	Owner(s)

Information Asset Risk Environment Map (People)	
Internal	
Container Description	Owner(s)
Staff Puskom	UPT.Puskom
Staff Akademis	Dikjar Fakultas
External	
Container Description	Owner(s)
Dosen	dosen
Mahasiswa	mahasiswa

Langkah 4 – *Identify Areas of Concern*

Pernyataan deskriptif yang menjabarkan kondisi atau situasi yang sebenarnya yang dapat mempengaruhi asset informasi. Melakukan review terhadap setiap *container* yang telah didaftarkan untuk melihat *areas of concern* yang potensial.

Tabel 5. *Area of Concern* – Transaksi Nilai Mahasiswa

No	Area of concern
1	Dikarenakan jumlah data nilai mahasiswa yang banyak, terjadi kesalahan dalam penginputan data oleh staff Bagian Dikjar fakultas atau oleh dosen
2	Penyebaran hak akses (password) terhadap aplikasi elearning yang dapat mengakses profil dosen oleh staff UPT.Puskom yang memiliki akses
3	Bug/error yang terdapat pada elearning yang muncul ketika staff IT melakukan maintenance
4	Pemanfaatan celah keamanan aplikasi elearning oleh pihak dalam/luar
5	Kesalahan dalam deployment aplikasi elearning
6	Staff IT yang dapat memasukkan malicious code

Langkah 5 – *Identify Threat Scenarios*

Pada langkah 5, identifikasi *threat Scenario* yang belum didefenisikan ke dalam *area of concern.*

Tabel 6 *Properties of Threat* - Transaksi Nilai Mahasiswa

No	Area of concern	Threat Properties	
1	Dikarenakan jumlah data nilai mahasiswa yang banyak, terjadi kesalahan dalam penginputan data oleh staff Bagian Dikjar fakultas atau oleh dosen	1.Actor	Staff bagian dikjar dan dosen
		2.Means	staff menggunakan aplikasi unisyss dan aplikasi elearning
		3.Motives	terjadi karena human error
		4.Outcome	modifikasi, interruption
		5.Security Requirement	penambahan validasi-validasi terhadap field-field yang diinput oleh staff dan dosen

Langkah 6 – *identify Risk.* Mengidentifikasi dampak *high* (tinggi) , *medium*, dan *low* untuk universitas dan menghitung *relative risk score. Relative risk score* digunakan untuk menganalisis risiko dan membantu organisasi memutuskan strategi terbaik dalam menghadapi risiko. *Score* diperoleh melalui perkalian *priority* dengan *value* dari *impact area*. Tujuan dari langkah ini menentukan bagaimana *threat scenario* yang telah dicatat dapat memberikan dampak bagi perusahaan. Tabel dibawah ini merupakan cara melakukan perhitungan score :

Tabel 7. Perhitungan *relative risk score*

Impact Areas	**Priority**	**Low**	**Moderate**	**High**
Reputasi dan kepercayaan pelanggan	5	5	10	30
Finansial	4	4	8	24
Produktivitas	3	3	6	18
Keamanan dan Kesehatan	2	2	4	12
Denda dan Penalti	1	1	2	6

Langkah 7 – *Analysis Risks.* Dilakukan dengan melakukan review *risk measurement criteria* yang telah ditetapkan pada langkah 1. Mulai dengan *risk worksheet* yang pertama, lakukan *review* dari pernyataan konsekuensi yang telah dicatat. Dan dilakukan perhitugan *relative risk score* yang akan digunakan untuk menganalisa resiko dan membantu organisasi untuk memutuskan strategi terbaik menghadapi risiko.

Tabel 8. - Analisis Risiko – Transaksi Nilai Mahasiswa

Area Of Concern	Risk			
Dikarenakan jumlah data nilai mahasiswa yang banyak, terjadi kesalahan dalam peng-inputan data	Consequences	Staff Dikjar Fakultas dan Dosen harus mendatakan ulang data-data nilai mahasiswa yang salah menggunakan aplikasi atau bantuan dari staff IT sehingga banyak waktu yang terbuang untuk menginputnya.		
	Seve Rity	Impact Area	Value	Score

oleh staff Bagian Dikjar fakultas atau oleh dosen Dikarenakan jumlah data nilai mahasiswa yang banyak, terjadi kesalahan dalam peng-inputan data oleh staff Bagian Dikjar fakultas atau oleh dosen	Proba-bility : High	Reputasi dan kepercayaan pelanggan	mod	10
		Finansial	Low	4
		Produktivitas	high	18
		Keamanan dan Kesehatan	Low	2
		Denda dan Penalti	Low	1
		Relative Risk Score		35

Langkah 8 – *Select Mitigation Approach*
Melakukan penyotiran tiap - tiap risiko yang telah diidentifikasikan berdasarkan nilai resiko. Resiko – resiko yang telah terindentifikasi dikategorikan berdasarkan *relative risk score* yang dimiliki.

Tabel 9. *Relative Risk Matrix*

Relative Risk Matrix			
Probability	Risk Score		
	30 to 45	**16 to 29**	**0 to 15**
High	POOL 1	POOL 2	POOL 2
Medium	POOL 2	POOL 2	POOL 3
Low	POOL 3	POOL 3	POOL 4

Dari pengelompokan risiko yang ada, selanjutnya diambil langkah mitigasi risiko – risiko tersebut. Pembagian pengambilan langkah mitigasi dikelompokkan menjadi:

Tabel 10. Langkah Mitigasi

Pool	**Mitigation Approach**
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

Tabel 11. *Risk Mitigation* – Transaksi Nilai Mahasiswa

1	*Risk Mitigation*	
	Area of Concern	Penyebaran hak akses (password) terhadap aplikasi elearning yang dapat mengakses transaksi nilai mahasiswa oleh staff UPT.Puskom yang memiliki akses
	Action	Mitigate or Defer
2	Area of Concern	Pemanfaatan celah keamanan aplikasi elearning oleh pihak dalam/luar
	Action	Defer or Accept

3. Kesimpulan

UPN "Veteran" Jakarta belum pernah melakukan evaluasi, penilaian risiko, perencanaan pengurangan risiko (mitigasi risiko) terkait aset informasi yang bersifat kritikal serta ancaman yang mungkin terjadi. Metode yang dgunakan untuk melakukan manajemen risiko sistem informasi yaitu metode Octave allegro *Worksheets* v1.0. Octave Allegro merupkan suatu metode untuk melakukan evaluasi risiko keamanan informasi yang sifatnya *self-directed* sehingga organisasi dapat membuat keputusan dalam perlindungan informasi berdasarkan risiko terhadap *confidentiality*, *integrity*, dan *availability* dari aset – aset informasi yang kritikal.

Berdasarkan tabel 11 *Risk Mitigation* terhadap transaksi nilai mahasiswa maka rekomendasi yang dapat dilakukan oleh UPN "Veteran" Jakarta yaitu mengadakan sosialisasi mengenai tanggung jawab dalam melindungi informasi dan dilakukan penyuluhan mengenai pentingnya keamanan *password*, melakukan pergantian *password* secara berkala kepada seluruh pengguna *e-learning*. Jika terjadi penyebaran password maka staff yang bersangkutan akan dikenakan sanksi, menambahkan fungsi *log* transaksi dan mereview *log* secara berkala serta menambahkan fungsi *logout* otomatis jika lebih dari lima menit tidak ada aktivitas.

Daftar Pustaka

[1] Jakaria Deni Ahmad, R Teduh Dirgahayu, Hendrik, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi dengan Menggunakan Metode Octave Allegro", Seminar Nasional Aplikasi Teknologi Informasi (SNATI), Yogyakarta, 2013.
[2] Aydm, Gengiz Hakan, "Measuring Readinesss for *e-learning*: Reflection from Emerging Country". Educational Technology and Society Journal, 8(4), pp. 244-257,2005.
[3] Bohl, O., Schellhase, J., Sengler, R., Winan, U, "The Sharable Content Object Reference Model (SCORM) – A Critical Review", Proceedings of the International Conference on Computers in Education. IEEE, 2002.
[4] Bramanti, Frita Lussie, "Pengukuran Kesiapan Organisasi Untuk Membangun Dan Mengimplementasikan *Elearning* Studi Kasus: Universitas Jenderal Achmad Yani". Tesis Magister Sistem Informasi ITB. Bandung, 2009.
[5] Caralli Richard A., James F. Stevens, Lisa R. Young and William R. Wilson, Introducing OCTAVE Allegro: Improving the

Information Security Risk Assessment Process. CERT Program. Software Engineering institute,2007.
[6] Chapnick, "*Are you ready for ELearning? – E-learning readiness assessment"* Diakses pada tanggal 15 September 2015 http://www.learning circuits.org/2000/nov2000/Chapnick.htm.
[7] Carman, J.M. "*Blended learning design: five key ingredients"*. diakses pada 18 November 2013, dari http://www.agilantlearning.com/pdf/Blended %20Learning%20Design.pdf
[8] Cisco. "*e-learning: Combines Communication, Education, Information, and Training",* http://www.cisco.com/warp /public/10/wwtraining/elearning, 2001.
[9] A Furchan, Pengantar Penelitian dalam Pendidikan, Pustaka Pelajar Offset ,Yogyakarta, 2004.
[10] Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View. NIST Special Publication 800-39, 2011
[11]Sukarno, Blended Learning Sebuah Alternatif Model Pembelajaran Mahasiswa Program Sarjana (S-1) Kependidikan Bagi Guru Dalam Jabatan, Program PGSD FKIP Universitas Sebelas Maret Surakarta
[12] M. M. Maulana dan S. H. Supangkat., "Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara berkembang". Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia, 121-126, 2006.
[13] Niah Kusumawati, Perpaduan Tatap Muka dan Kuliah Online Melalui Blended Learning, diakses pada http://edukasi.kompas.com/read/2012/06/06/11503150/Perpaduan.Tatap.Muka.dan.Kuliah.Online.Melalui.Blended.Learning,2012.
[14] R. L. Krutz dan D. R. Vines, The CISSP Prep Guide – Mastering the Ten Domains of Computer Security. CA: Wiley Computer Publishing John Wiley & Sons, Inc, 2006.
[15] S. K. Pandey dan K. Mustafa., "A Comparative Study of Risk Assessment Methodologies for Information Systems", Buletin TeknikElektro dan Informatika, 1(2),111-122,2012.
[16] Welly dan Mikewati., Penilaian Resiko Sistem Informasi Pada Bina Nusantara Menggunakan Metode Octave Allegro. http://library.binus.ac.id/Collections/ethesis_detail/TSA-2012-0023, 2011.
[17] Yudi Firman Santosa, Personal Assignment IT Risk Management and Disaster Recovery . Binus University, 2014.
[18] Tim Internal Cetak Biru TI UPNVJ dan Tim Konsultan PT. Multimedia Solusi Prima, Cetak Biru Teknologi Informasi, UPN Veteran Jakarta 2012-2016.

Biodata Penulis

Henki Bayu Seta, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika UPN "Veteran"Jakarta, lulus tahun 2005. Memperoleh gelar Magister Informasi Teknologi (MTI) Program Pasca Sarjana Magister Teknologi Informasi Universitas Indonesia, Jakarta, lulus tahun 2013.Saat ini menjadi Dosen di UPN "Veteran" Jakarta.

Theresiawati, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika UPN "Veteran"Jakarta, lulus tahun 2005. Memperoleh gelar Magister Informasi Teknologi (MTI) Program Pasca Sarjana Magister Teknologi Informasi Universitas Indonesia, Jakarta, lulus tahun 2013.Saat ini menjadi Dosen di UPN "Veteran" Jakarta.

Tri Rahayu, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika UPN "Veteran"Jakarta, lulus tahun 2003. Memperoleh gelar Magister Manajemen (MM) Program Pasca Sarjana UPN "Veteran" Jakarta, Jakarta, lulus tahun 2011.Saat ini menjadi Dosen di UPN "Veteran" Jakarta.