Pengukuran Risiko Sistem Informasi Perpustakaan Menggunakan Framework *National Institute of Standard and Technology* SP 800-30

Megawati[1], Irpandi Kurniawan[2], Idria Maita[3], Novi Yanti[4]
Sains dan Teknologi, Sistem Informasi, UIN Suska Riau, Pekanbaru, Indonesia
Jalan HR. Soebrantas Panam Km.15 No.155, Simpang Baru, Kec Tampan, Pekanbaru, Riau 28293
e-mail: [1]megawati@uin-suska.ac.id, [2]irpandi@student.uin-suska.ac.id, [3]idria@uin-suska.ac.id,
[4]novi_yanti@uin-suska.ac.id

Abstrak

Sistem informasi perpustakaan di era sekarang dapat menimbulkan risiko yang mengancam data dan kemamanan system. Beberapa risiko seperti kehilangan data, kebakaran, dan risiko akibat kelalaian manusia dapat terjadi. Penelitian ini bertujuan mengukur tingkat risiko sistem informasi perpustakaan dan memberikan rekomendasi perbaikannya. Pada penelitian ini metode yang digunakan adalah NIST (SP) 800-30. Sumber ancaman risiko, penilaian risiko, peringanan risiko, dan evaluasi risiko perlu dideteksi oleh Manajemen risiko sistem informasi Perpustakaan univeristas Lancang Kuning Riau. Pengukuran risiko dilakukan menggunakan Metode NIST (SP) 800-30 memiliki 9 (sembilan) tahapan. Hasil proses pengolahan data diperoleh ancaman yang dengan dampak ancaman risiko tinggi yaitu 1 (satu) high risk yaitu koneksi jaringan terputus. 3 (tiga) medium risk yaitu human error, database error, dan data corrupt. 4 (empat) low risk yaitu kehilangan data, kerusakan hardware, server down, dan bencana alam (petir).Berdasarkan hasil pengukuran risiko tersebut diberikan rekomendasi perbaikan system kedepan berupa disaster recovery plan. Manfaat penelitian ini adalah untuk mencari acuan bagi pihak pengelola system dalam mencegah dan meanggulangi risiko.

Kata kunci: *Manajemen Risiko IT, NIST SP 800-30, Sistem Informasi Perpustakaan*

Abstract

Library information systems in the present era can pose risks that threaten data and system security. Several risks such as data loss, fire, and risks due to human negligence can occur. This study aims to measure the risk level of library information systems and provide recommendations for improvement. In this study the Framework used was NIST (SP) 800-30. Sources of risk threats, risk assessment, risk mitigation, and risk evaluation need to be detected by the risk management information system of the Lancang Kuning library, Riau University. Measurement of risk is carried out using the NIST Framework (SP) 800-30 which has 9 (nine) stages. The results of the data processing process obtained threats with a high risk threat impact, namely 1 (one) high risk, namely the network connection was lost. 3 (three) medium risks, namely human error, database error, and data corrupted. 4 (four) low risks, namely data loss, hardware damage, server downtime, and natural disasters (lightning). Based on the results of the risk measurement, recommendations for future system improvements in the form of a disaster recovery plan are given. The benefit of this research is to find references for system managers in preventing and overcoming risks.

Keywords*: IT Risk Management, Library Information System, NIST SP 800-30*

1. Pendahuluan

Pengukuran risiko sistem informasi belum pernah dilakukan pada 'UPT (Unit Pelaksana Teknis) Perpustakaan UNILAK (Universitas Lancang Kuning)'. Pengukuran risiko sangat penting dilakukan untuk menunjang keamaman penerapan teknologi informasi yang ada pada UPT Perpustakaan UNILAK. Sistem informasi perpustakaan UNILAK pernah mengalami deface yaitu perubahan pada tampilan system tanpa diketahui pelakunya. Hal ini menjadi ancaman risiko yang bersumber dari ancaman manusia. Serangan *deface* dapat disebabkan karena kelalaian dari pihak Humas dan UPT Perpustakaan UNILAK. (lib.unilak). Selain itu system informasi perpustakaan unilak juga memiliki ancaman risiko lainnya seperti kebakaran, *virus, human error*, kegagalan jaringan.

Manajemen Risiko merupakanprosesantisipasi terhadap risiko agar kerugian tidak terjadikepada organisasi. Stoneburner et. Al berpendapat bahwa manajemen risiko adalah

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

proses mengidentifikasi menilai dan mengurangi dampakrisiko ke level yang dapat diterima organisasi [4]. Beberapa literature menyatakan bahwa manajemen risiko bermanfaat dalam menghindari kerugian yang disebabkan terjadinya berbagai dampak risiko. Galorath mengatakan kesuksesan sebuah organisasi bergantung pada bagaimana cara mengatasi potensi negatif (risiko) dan berbagai masalah yang terjadi dalam organisasi. Masih dalam penelitian yang sama diungkapkan bahwa organisasi menjadi sukses jika mampu mengantisipasi berbagai potensikerugian serta mengelola perubahan yang terjadi [6].

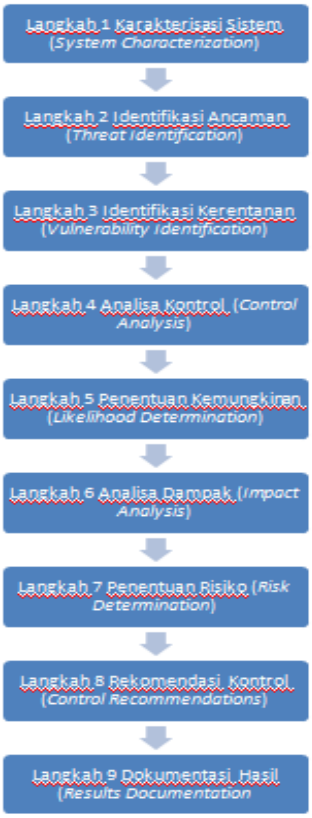
Proses bisnis dapat terganggu disebabkan oleh terdapatnya berbagai sumber Ancaman risiko. Untuk itu perlu dilakukan pengelolaan Manajemen risiko di sistem informasi yang berguna untuk identifikasi risiko, mengukur seberapa besar dampak oleh risiko, membuat penilaian risiko dan membuat susunan strategi mitigasi untuk mengurangi risiko. Metode *National Institute of Standard and Technology* (NIST) *Special Publication* (SP) 800-30 dapat digunakan untuk manajemen risiko teknologi informasi yaitu.

Makalah ini bertujuan untuk mengukur tingkat risiko, mendapatkan sumber ancaman dan menganalisa dampak risiko. Metode NIST juga akan memeriksa kembali dan mengevaluasi keamanan pada sistem dan informasi perpustakaan di Perpustakaan Universitas Lancang Kuning. Selanjutnya akan diberikan rekomendasi perbaikan untuk mengatasi dan mencegah risiko terjadi.

Risiko antara lain dapat diartikan sebagai keadaan ketidakpastiaan yang akan terjadi nantinya dimasa depan (*future*). Untuk mencegahnya diperlukan keputusan yang diambil berdasarkan berbagai pertimbangan kondisi saat ini (as-is).

Terdapat Ancaman terhadap keamanan yang dapat disebabkan oleh kondisi alam, manusia, atau yang berifat kelalaian maupun kesengajaan. NIST (*National Institute of Standard and Technology*) memberikan panduan rekomendasi. Panduan yang dibuat pada framework NIST menjadi acuan dalam pengukuran dan menanggulangan dampak risiko. Metodologi ini di desain untuk digunakan sebagai alat perhitungan kualitatif.

Proses manajemen risiko sebenarnya sangat komprehensif, meliputi segala sesuatu yang dimulai dari identifikasi sumber risiko ancaman, juga mengevaluasi dan memberi penilaian yang berkelanjutan. Terdapat 9 (Sembilan langkah dalam menggunakan metode ini seperti pada Gambar 1.



Gambar 1. Sembilan Langkah Metode NIST SP 800-30 [5]

2. Metode Penelitian

Metodolgi yang digunakan pada penelitian ini dapat dijelaskan sebagai berikut:

1) Tahap I Pendahuluan
   Merupakan tahapan menentukan tempat penelitian, menentukan objek penelitian dan menentukan judul penelitian. Tempat penelitian yaitu pada UNILAK, dengan system informasi perpustakaan sebagai objek penelitian.
2) Tahap II Perencanaan
   Merupakan tahapan mengidentifikasi masalah, dan menentukan jenis dan sumber data.
3) Tahap III Pengumpulan Data
   Merupakan tahapan mendapatkan referensi dari studi pustaka, melakukan observasi, dan melakukan kegiatan wawancara berdasarkan RACI chart. Berdasarkan hasil RACI diperoleh 6 orang pengelola system yang mengisi daftar pertanyaan mengenai risiko pada system informasi perpustakaan UNILAK.
4) Tahap IV Pengolahan Data
   Merupakan tahapan merekapitulasi data yang sudah di dapat dari observasi dan dari hasil wawancara
5) Tahap V Pembahasan
   Merupakan tahapan untuk menjelaskan dan menganalisis proses manajemen risiko pada sistem informasi perpustakaan berdasarkan metode NIST (SP) 800-30.

3. Hasil dan Pembahasan

1) Karakterisasi Sistem (*System Characterization*)
   Karakteristik system ini diidentifikasi berdasarkan lingkungan system informasi perpustakaan berada antara lain yaitu hardware, software, dan aplikasi. Dalam mendefenisikan karakteristik system dilakukan survey dan observasi ke tempat penelitian yaitu UNILAK unit system informasi perpustakaannya.

Tabel 1. Daftar *Hardware*

Jenis Hardware	Tipe/ Jenis	Keterangan
Mother-board	SATA (*Serial Advanced Technology Attachment)*	Papan sirkuit dimana berfungsi untuk tempat komponen-komponen komputer
Processor	Intel	Merupakan IC berfungsi mengontrol jalannya seluruh sistem komputer
Hard Disk	SATA (*Serial Advanced Technology Attachment) – 160GB*	Berfungsi sebagai perangkat keras komputer media penyimpanan sekunder
CPU Cooler	Intel 90 Mm 3pin	Perangkat ini dirancang untuk mengurangi panas pada CPU, system, dan komponen lain dalam casing komputer.
Monitor	VGA Resolusi 800 × 1200 pixel	Adalah perangkat keras yang berguna sebagai alat output. Juga berfungsi menampilkan hasil olah data berupa grafis
Optical Drive	DVD RW	Sebagai media penyimpanan kategori *programmable read-only memory* (PROM) dan *electically programmable read-only memory* (EPROM)
RAM	ECC (***Error-Correcting Code*****)** RAM	Sebagai suatu tipe RAM berfungsi mendeteksi serta memperbaiki error/kesalahan memori internal yang terjadi disebabkan oleh adanya data yang corrupt saat sistem beroperasi

2) Identifikasi Ancaman dan Sumber Ancaman (*Threat Identification dan Source – thread identification*)
   Identifikasi Ancaman yang dapat terjadi pada sistem informasi perpustakaan unilak antara lain ancaman kebakaran, *human error, deface, virus,* dan kegagalan pada koneksi jaringan.

Tabel 2. Identifikasi Penyebab Acaman

Ancaman	Penyebab Ancaman
Kebakaran	• Sambaran oleh petir
	• Korsleting Listrik
Human Error	• Desain kerja yang kurang baik
	• Manajemen tidak menerapkan disiplin
Deface	• Security Awareness
	• Tidaknya audit atau log
Virus	• Penggunaan Flasdisk
	• Antivirus tidak update
	• Mengunduh file tidak jelas
Kegagalan Jaringan	• Jaringan LAN terputus
	• Access point Terbatas

Sedangkan yang menjadi sumber ancaman dengan dampak terbesar kedua adalah Manusia. Sumber ancaman ini dapat terjadi secara sengaja atau tidak. Tabel 2 menunjukan gambar hasil identifikasi sumber ancaman yang disebabkan kesalahan manusia (*human error*).

Tabel 3. Identifikasi Sumber Ancaman Manusia

Ancaman	Tujuan Ancaman	Penyebab Ancaman
Kebakaran	Dapat Merusak perangkat lunak (software) dan perangkat keras (hardware)	Disebabkan oleh hubungan arus pendek listrik (korsleting listrik)
Human Error	Pengerusakan pada data dan informasi	• Rancangan atau desain sistem kerja yang kurang baik • Manajemen kurang menerapkan disiplin • Kurang Skill, pengalaman, atau factor psikologis
Deface	Kesengajaan merubah data	• Kurangnya kesadaran keamanan (*security awareness)* • Tidaknya adanya audit pada trail atau log aktivitas
Virus	Pengrusakan pada perangkat lunak (software)	• Penggunaan flashdisk tanpa pemeriksaan virus • Antivirus tidak update
Kegagalan jaringan	*Trobleshooting* yang terjadi pada jaringan LAN dan Internet.	• Teroputusnya Jaringan LAN • Terbatasnya *Acces point*

3) Identifikasi Kerentanan (*Vulnerability Identification*)
Daftar kerentanan sistem (kelemahan) yang dapat menjadi sumber ancaman yang potensial dilakukan pada langkah ini. Tabel 4 merupakan hasil identifikasi kerentanan *vulnerability* yang terjadi di dalam sistem informasi perpustakaan.

Tabel 4. Identifikasi Kerentanan

Ancaman	Sumber Ancaman	Sumber Kelemahan	Aksi Ancaman
Human Error	Manusia	Penggunaan ID karyawan yang nonaktif tidak dihapus	Karyawan yang sudah tidak aktif mengakses data dan informasi perpustakaan
Virus	Manusia	Lemahnya Sistem keamanan firewall perpustakaan	Dapat merusak data-data sensitif perpustakaan
Human Error	Manusia	Tamu seperti anak magang/praktek dapat mengakses sistem secara bebas	Ancaman Memanipulasikan data-data yang ada di dalam system
Human Error	Manusia	Karyawan yang tidak teliti	• perubahan data perpustakaan • Data tidak valid

4) Analisa Kontrol (*Control Analysis*)
Pada tahap ini menganalisis kontrol yang telah di laksanakan atau direncanakan pada sistem informasi perpustakaan. Analisa control ini dilakukan untuk meminimalkan dan menghilangkan kemungkinan adanya ancaman dari kelemahan system, seperti pada tabel 5.

Tabel 5. Daftar Kontrol saat ini dan Rencana Kontrol

No	Ancaman	Penyebab Ancaman	Risiko	Kontrol Saat ini	Rencana Kontrol
1	Kebakaran	Litrik yang konsleting	• Terhapus seluruh atau sebagian data • Terbakarnya Tempat penyimpanan data dan rusak • Kerusakan pada *Hardware* maupun *software*	Secara berkala dilakukan Pengecekan kelayakanpada peralatan	Merancang *Disaster Recove*ry *Planning* (DRP)
		Tidak benarnya instalasi listrik		Kesesuain Pemasangan instalasi dilistrik sesuai prosedur	Prosedur pemasangan pada listrik dan instalasinya
		Disambar Petir		Memasang instalasi penangkal petir	• *backup* dan restorasi pada data • *Disaster Recovery Planning* (DRP) sebagai pusat data
2	*Kesalahan Manusia / Human Error*	Desain system kurang baik	• Pelaporan data tidak akurat atau tidak benar • Laporan yang tidak sesuai dengan Data • Tidak dapat dibacanya Data	Belum adanya control	Melakukan pelatihan kepada pegawai secara berkala
		Manajemen yang tidak disiplin		Manual book untuk mem*backup*	membatasi hak untuk akses berdasarkan level kepentingan.
		Skill, pengalaman dan psikologis		Tidak ada kontrol	Karyawan internal dilakukan control internal
3	*Virus*	*Pemakaian flashdisk*	Data-data penting perpustakaan hilang	*backup* menggunakan *manual book*	• Data dikelompokkan berdasarkan kegunaansecara jelas lalu mem*backup*nya • Penggunaan *flashdisk* hanya yang telah disediakan oleh perpustakaan
		Tidak update *AntiVirus*	*Software* dan aplikasi tidak dapat diakses	*update antivirus* secara berperiodik	Instalasi perangkat *firewall*, *deep freeze*, dan antivirus yang berlisensi.
		Mendownload file yang sembarangan	Merusak adanya data dan informasi	Belum ada peraturan tertulis dan tidak mengikat	Membuat aperatuan tertulis manajemen pengunduhan file
4	*Deface*	*security awareness* tidak ada	• Data dan informasi dapat berubah • Tampilan sistem yang tidak terlalu signifikan • Kehilangan data yang disimpan pada sistem perpustakaan (eksemplar koleksi perpustakaan) • Merusak data denda anggota.	Lakukan Pengawasan terhadap hak akses pengguna system	
		audit trail atau *log* tidak dilakukan		Melakukan *backup* lewat *manual book*	Rutin *meng-Up date* dan perubahan hak akses secara periodic
				Melakukan *backup* lewat *manual book*	
5	Kegagalan Jaringan	Terputusnya Jaringan LAN	Terganggunya Proses pengolahan dan pelaporan data	Lakukan pemeriksaan dan perawatan secara periodik	Tingkatkan kehandalan jaringan dengan penggunaan teknologi terbaru
		Terbatasnya Access point yang disediakan			

5) Penentuan Kemungkinan (*Likelihood Determination*)
Langkah ini menentukan kemungkinan ancaman risiko yang mungkin terjadi. Tabel 6 adalah tabel kemungkinan ancaman yang terjadi pada sistem informasi perpustakaan.

Tabel 6. Kemungkinan dari Ancaman yang Terjadi

No	Ancaman	Penyebab Ancaman	Kemungkinan	Skor
1	Kebakaran	Adanya hubungan arus pendek listrik (korsleting listrik)	Tinggi	4
		Adanya instalasi listrik yang tidak benar	Tinggi	5
		Adanya sambaran petir	Tinggi	5
2	*Human Error*	Perancangan/ desain sistem kerja yang kurang baik	Tinggi	4
		Manajemen yang tidak menerapkan disiplin secara baik	Tinggi	5
		Skill, pengalaman dan psikologis	Sedang	3
3	*Virus*	*Penggunaan flashdisk*	Tinggi	5
		Tidak pernah memperbarui *AntiVirus*	Tinggi	4
		Mengunduh file yang tidak jelas dan sembarangan	Tinggi	5
4	*Deface*	Kurangnya *security awareness*	Tinggi	4
		Tidak adanya *audit trail* atau *log*	Tinggi	5
5	Kegagalan Jaringan	Jaringan LAN Terputus	Sedang	2
		Access point yang disediakan terbatas	Sedang	3

6) Analisa Dampak (*Impact Analysis*)
Analisa dampak dilakukan untuk ancaman yang mungkin terjadi di dalam sistem informasi perpustakaan Unilak yaitu diggambarkan seperti pada Tabel 7.

Tabel 7. Dampak dari Ancaman yang Terjadi

Ancaman	Dampak	Skor	Akibat
Kebakaran	Tinggi	5	• Seluruh data dan informasi terhapus • Terbakarnya tempat penyimpanan data • Hardware dan software mengalami kerusakan
Virus	Tinggi	4	• Merusak data-data yang ada didalam sistem • Software dan aplikasi tidak dapat digunakan atau tidak dapat diakses • Merusak sistem keamanan yang ada di dalam system
Kegagalan Jaringan	Tinggi	5	• Proses pengolahan dan pelaporan data terganggu
Human Error	Sedang	3	• Data tidak akurat atau tidak benar • Data tidak sesuai dengan laporan • Data tidak dapat dibaca
Deface	Sedang	2	• Data dan informasi berubah • Perubahan tampilan sistem yang tidak terlalu signifikan • Kehilangan data-data koleksi perpustakaan (eksemplar koleksi perpustakaan) • Rusaknya data denda anggota (perubahan nominal dari nominal sebelumnya)

7) Penentuan Risiko (*Risk Determination*)
Penentuan tingkat risiko yang dapat terjadi disebabkan oleh alam seperti terlihat pada Tabel 8.

Tabel 8. Penentuan Risiko

Ancaman	Dampak	Skor	Akibat
Kebakaran	Tinggi	5	• Seluruh data dan informasi terhapus • Terbakarnya tempat penyimpanan data • Hardware dan software mengalami kerusakan
Virus	Tinggi	4	• Merusak data-data yang ada didalam sistem • Software dan aplikasi tidak dapat digunakan atau tidak dapat diakses • Merusak sistem keamanan yang ada di dalam system
Kegagalan	Tinggi	5	• Proses pengolahan dan pelaporan data terganggu

Jaringan			
Human Error	Sedang	3	• Data tidak akurat atau tidak benar • Data tidak sesuai dengan laporan • Data tidak dapat dibaca
Deface	Sedang	2	• Data dan informasi berubah • Perubahan tampilan sistem yang tidak terlalu signifikan • Kehilangan data-data koleksi perpustakaan (eksemplar koleksi perpustakaan) • Rusaknya data denda anggota (perubahan nominal dari nominal sebelumnya)

8) Rekomendasi Kontrol (*Control Recommendations*)
Tahap ini bertujuan memberikan rekomendasi control agar mengurangi tingkat risiko pada aplikasi sistem teknologi informasi perpustakaan Universitas - Lancang Kuning seperti pada Tabel 9.

Tabel 9. Rekomendasi Kontrol

Sumber Ancaman	Motivasi	Tindakan Ancaman	Rekomendasi Pengendalian Keamanan
Kebakaran	Tidak disengaja	Karena adanya arus pendek aliran listrik Karena disambar petir Instalasi listrik yang tidak benar	*distater recov*ery plan harus dibuat *data center distater recovery center harus* dikuatat dan pertahankan terhadap bencana alam Melakukan *backup* dan restorasi data
Human Error	Pengerusakan	Menginputkan data tidak benar Penyalahgunaan hak akses Merusak data pada media penyimpanan	Melakukan pelatihan kepada pegawai Membuat pembatasan hak akses sesuai dengan tingkat kepentingannya Melakukan pengawasan secara internal terhadap apa saja dikerjakan
Virus	Pengerusakan	Kegagalan operasi *software* Perubahan data Kehilangan data	Menggunakan antivirus yang berlisensi Membuat *file log* yang membackup history dari sebuah data Mengelompokan data berdasarkan kegunaannya secara jelas lalu membuat *backup*nya
Deface	Pengerusakan	Perubahan tampilan sistem Perubahan data dan informasi Kerusakan data denda anggota	*Up date* dan perubahan hak akses secara periodic
Kegagalan Jaringan	*Trobleshooting* pada jaringan LAN dan Internet	Jaringan LAN terputus Permasalahan pada provider jaringan WAN dan internet	Meningkatkan kehandalan jaringan dengan penggunaan teknologi terbaru yaitu *recovery point objetive* (RPO) dan *recovery time objective* (RTO)

Rekomendasi yang diberikan berdasarkan dari framework NIST SP 800-30 khususnya manajemen risiko IT Sistem informasi perpustakaan juga berdasarkan dari temuan potensi risiko.

4. Kesimpulan

Kesimpulan pada penelitian menggunakan NIST SP 800-30 diperoleh terdapat 8 risiko teknologi informasi yang terdiri dari 1 (satu) *high risk* yaitu koneksi jaringan terputus. 3 (tiga) *medium risk* yaitu human *error*, database *error*, dan data *corrupt*. 4 (empat) *low risk* yaitu kehilangan data, kerusakan hardware, server *down*, dan bencana alam (petir). Rekomendasi yang dihasilkan pada tingkat risiko *high* dan *medium* berdasarkan perlakuan risiko yaitu mitigasi untuk mengurangi kemungkinan dan dampak risiko berupa *disaster recovery plan*.

Daftar Pustaka

[1] A. Syalim, Y. Horinoch K. Sakurai, *Comparison of Risk Analysis Method: Mehari. Magerit, NIST-800-30 and Microsoft's Security Management Guide, International Conference on Availabilty, Reliability, and Security.* Fukuoka, 2009
[2] Chen, Feiquan. *An Investigations and Evaluation Risk Assessment Method in Informations System.*

Journal Informations System. 2015
[3] Douramanis Michail. *Risk Assessment for Cyber thread to network Critical Infrastructure. Journal Informations System. Vol 1 No.1*. 2014.
[4] Irham Fahmi. *Manajemen Risiko Teori Kasus dan Solusi*. Edisi Revisi. Bandung: Alfabet. 2013.
[5] Galorath D, *Risk Management Succes Factor. PM World Today. Vol, VIII, Issue 12.* 2006.
[6] Shim, J.K., dan Siegel, J. G. *Operations management. Barron's Educational Series*. 1999.
[7] Sanyoto Gondodiyoto, Henny Hendarti. *Audit Sistem Informasi*. Jakarta: Mitra Wacana Media. 2006.
[8] Stoneburner, G., Goguen, A., & Feriga, A., *Risk Management guide tfor informations technology system Recommendation of National Institute of Standard and technology*. NIST Laboratory. 2013.
[9] Syafitri wenni. *Penilaian risiko keamanan informasi menggunakan metode NIST 800-30 (Studi kasus Sistem informasi Akademik Universitas XYZ,* Pekanbaru) 2016
[10] NIST. Version 4.1 NIST (*National Institute of Standards and Technology)*. Gaithersbug. 2012.
[11] Nasional, D. P. *Kamus Besar Bahasa Indonesia (KBBI*). Jakarta: Gramedia. 2008
[12] William, Michael G. A *Risk Assesment on Rasberry Pi using NIST Standard, Journal Computer Science. Vol. 15 No.6*. 2015.