Analisis Tingkat Keamanan Aplikasi SIMAK Menggunakan Standard ISO/IEC 27002:2013 (Studi Kasus: UPTTIK Universitas Siliwangi)

Iyos Rosidin Pajar

Program Studi Pascasarjana Magister Sistem Informasi, STMIK Likmi, Bandung

*Koresponden email: iyos@unsil.ac.id

Diterima: 26 Februari 2021

Disetujui: 8 Maret 2021

Abstract

One of the interesting problems to observe in the development of information technology is the issue of data security. Universitas Siliwangi information technology in carrying out its management processes, one of which is the SIMAK application. This study aims to determine the level of security of the SIMAK application so that researchers can provide recommendations to SIMAK managers which should be the basis for future improvements. Researchers used 4 domains from ISO / IEC 27002: 2013, namely domain 5 contains information security policies, domain 6 contains organizational information security, domain 9 contains access control and domain 11 contains physical and environmental security where if specified from the four domains, 38 controls are obtained. security. From the results of the questionnaire and weighting, the results of the 5 domain maturity value = 1.49, domain 6 maturity value = 1.52, domain 9 maturity value = 1.32 and domain 11 maturity value = 1.97 and if it is averaged that the Siliwangi University SIMAK application is at level 2 or repeatable.

Keywords: *SIMAK application, academic information system, system information security, maturity level, ISO 27002, CMMI*

Abstrak

Salah satu permasalahan yang menarik untuk dicermati dalam perkembangan teknologi informasi adalah permasalahan keamanan data. Universitas Siliwangi memanfaatkan teknologi informasi dalam menjalankan proses manajemennya salah satunya adalah aplikasi SIMAK. Penelitian ini bertujuan untuk mengetahui tingkat keamanan dari aplikasi SIMAK. Peneliti dapat memberikan sebuah rekomendasi kepada pengelola SIMAK yang harus menjadi dasar perbaikan dimasa mendatang terkait keamanan data. Peneliti menggunakan 4 domain dari ISO/IEC 27002:2013 yaitu domain 5 berisi kebijakan keamanan informasi, domain 6 berisi keamanan informasi organisasi, domain 9 berisi kontrol akses dan domain 11 berisi dengan keamanan fisik dan lingkungan dimana jika dirinci dari keempat domain tersebut didapat 38 kontrol keamanan. Dari hasil kuesioner dan pembobotan maka didapatkan hasil kematangan domain 5 nilai kematangan = 1,49, domain 6 nilai kematangan = 1,52, domain 9 nilai kematangan = 1,32 dan domain 11 nilai kematangan = 1,97 dan apabila di rata – ratakan bahwa aplikasi SIMAK Universitas Siliwangi berada pada *level 2* atau *repeatable*.

Kata Kunci: *aplikasi SIMAK, sistem informasi akademik, keamanan sistem informasi, tingkat kematangan, ISO 27002, CMMI.*

1. Pendahuluan

Sistem informasi saat ini pada perkembangannya menarik untuk diamati, kini berbagai bidang menggunakan sistem informasi dalam membantu memudahkan berjalannya proses bisnis. Salah satu bidang yang memanfaatkan sistem informasi adalah bidang pendidikan, bidang ini menggunakan sistem informasi dalam proses pengolahan data akademik dan dalam menunjang kelancaran penyampaian informasi kepada peserta didiknya. Perkembangan teknologi informasi mengilhami proses bisnis yang sebelumnya menggunakan cara tradisional, menjadi cara yang lebih efisien selain itu juga komunikasi antara pemasok dan perusahaan menjadi meningkat [1]. Masalah keamanan bisa muncul dari berbagai hal, seperti yang di timbulkan oleh manusia atau keamanan yang memang dari sistem informasi itu sendiri. Terjadinya masalah keamanan pada sistem informasi dapat menimbulkan kerugian, salah satu kerugian yang dapat terjadi adalah rusaknya data yang juga dapat memicu kerugian yang lain seperti kerugian materi pada suatu organisasi. Permasalahan keamanan eksternal dapat ditimbulkan dari adanya gangguan yang dilakukan oleh pihak lain yang tidak bertanggungjawab, aspek penting dari sebuah sistem

informasi adalah aspek keamanan, orang yang tidak bertanggungjawab bisa saja masuk kepada sistem atau aplikasi melalui suatu jaringan [2].

Beberapa ahli berpendapat tentang pengertian dari sistem informasi, yaitu sistem informasi merupakan kombinasi dari perangkat lunak, perangkat keras dan manusia yang bertugas mengolah dan mendistribusikan informasi pada suatu organisasi [3]. Sistem informasi adalah gabungan yang teratur dari *hardware, software, network*, kebijakan, dan data bertugas untuk mengumpulkan dan menghimpun selanjutnya mengolah dan mendistribusikan data sampai akhirnya mendapatkan data kembali [4]. Dalam membangun sebuah aplikasi yang mempunyai dukungan *forensic network* adalah tentang penentuan metode yang cocok untuk mempermudah dalam proses pengolahan data *log* menjadi suatu data yang mudah untuk diproses [5]. Sistem Informasi merupakan sekumpulan elemen atau subsistem yang digabungkan, saling keterkaitan atau berhubungan bertugas untuk mengelola dan mengolah data sehingga menjadi berarti bagi penerima, selain itu juga berfungsi untuk penentuan keputusan dimasa mendatang [6]. Sistem informasi merupakan suatu perkumpulan data yang terorganisasi dilengkapi dengan tata cara atau prosedur penggunaan mencakup lebih jauh dari sebuah perjanjian, istilah tersebut menyiratkan suatu maksud yang ingin dicapai dengan jalan memilih dan mengatur data serta menyusun tatacara penggunaanya [7]. Sistem informasi merupakan sebuah sistem yang berada pada sebuah organisasi, yang dapat berjalan untuk mendukung transaksi harian, juga berfungsi atau mendukung perusahaan pada bidang manajerial, selain itu juga dapat menghasilkan laporan yang berguna untuk pihak eksternal [8]. Sistem informasi adalah suatu sistem yang diciptakan oleh manusia yang berbasis sekumpulan alat yang berbasis komputer yang dibuat untuk mengumpulkan dan mengolah data untuk pengguna [9].

UPTTIK sebagai salah satu organisasi yang memanfaatkan sistem informasi dalam prakteknya untuk menjaga keamanan data yang dikelolanya haruslah menerapkan suatu standar keamanan yang diterapkan pada sistem kelolanya, aspek yang harus dimiliki sistem informasi yaitu aspek kerahasiaan, keutuhan dan ketersediaan atau yang biasa disingkat dengan *Confidentiality, Integrity, Availability* (CIA). Agar sistem berjalan sebagaimana mestinya maka diperlukan pengukuran kinerja dengan melakukan pemeriksaan, serta supaya sistem berjalan dengan baik maka diperlukan penerapan standar baku [10]. Dalam melakukan audit sistem informasi, tidak ada acuan baku bagi suatu organisasi dalam melakukan pemeriksaan.

Peneliti dan UPTTIK Universitas Siliwangi sepakat memakai ISO/IEC 27002:2013 dalam melakukan penelitian ini, alasannya adalah standar tersebut dianggap fleksibel, mudah disesuaikan dengan kebutuhan organisasi, persyaratan keamanan dan ukuran organisasi yang memakainya. Sedangkan untuk model perhitungan tingkat kematangan pada penelitian ini memakai *Capability Maturity Model Integration* (CMMI). Berikut ini adalah kriteria indeks kematangan pada CMMI [11]:

Tabel 1. Kriteria tingkat kematangan pada CMMI

Skor (skala)	Status	Keterangan
0 – 0.50	<i>Non-existent</i>	<i>Management processes are not applied at all</i>
0.51 – 1.50	<i>Initial</i>	<i>Processes are ad hoc and disorganized</i>
1.51 – 2.50	<i>Repeatable</i>	<i>Processes follow a regular pattern</i>
2.51 – 3.50	<i>Defined</i>	<i>Processes are documented and communicated</i>
3.51 – 4.50	<i>Managed</i>	<i>Processes are monitored and measured</i>
4.51 – 5.00	<i>Optimized</i>	<i>Good practices are followed and automated</i>

Sumber: Data penelitian, 2018

Penelitian atau audit ini dimaksudkan untuk melihat tingkat kematangan yang dimiliki oleh aplikasi SIMAK, sejauh mana kematangan aplikasi SIMAK pada sisi keamanan khususnya yang terkait dengan domain yang diambil pada penelitian ini. Proses penelitian ini diharapkan dapat mengidentifikasi persoalan atau penyebab yang berpotensi munculnya gangguan keamanan pada aplikasi SIMAK. Selanjutnya mengidentifikasi hasil temuan, membuat sebuah kesimpulan dan saran dimana saran tersebut menjadi bahan acuan untuk perbaikan aplikasi SIMAK dimasa mendatang.

Penelitian ini menyepakati 4 domain seperti yang terlihat pada **Tabel 2** [5]. Data yang didapatkan dalam penelitian ini diperoleh dari hasil observasi lapangan atau melakukan pengamatan langsung di lokasi penelitian, melakukan wawancara kepada narasumber yang juga berperan sebagai responden, dan yang terakhir adalah survei dengan membuat atau mengajukan kuesioner kepada narasumber.

Tabel 2. Domain yang dipakai dalam penelitian

Domain	Kaitan
5	Kebijakan keamanan informasi
6	Keamanan informasi organisasi
9	<i>Access Control</i>
11	Keamanan fisik dan lingkungan

Sumber: ISO/IEC 27002:2013

Kuesioner yang dibuat yaitu terkait dengan domain yang terdapat pada **Tabel 1**, kuesioner disebarkan pada responden yang berasal dari seluruh pegawai UPTTIK Universitas Siliwangi (7 orang), Hal ini dilakukan karena kuesioner yang dibuat terkait dengan hal teknis yang berada dan dilakukan di UPTTIK Universitas Siliwangi.

2. Metode Penelitian

Alur penelitian

Alur penelitian yang baik dapat berpengaruh terhadap hasil penelitian yang dilakukan. Berikut ini adalah alur penelitian yang dilakukan, dapat dilihat pada **Gambar 1**.

Gambar 1. Alur penelitian

Sumber: Data penelitian, 2020

Pada penelitian ini langkah pemilihan dan penentuan domain adalah berdasarkan hasil diskusi dan kesepakatan dengan pihak UPTTIK Universitas Siliwangi sebagai pengembang sekaligus penanggungjawab aplikasi SIMAK. Domain yang disepakati dapat dilihat pada **Tabel 2**. Pada langkah pengumpulan data, peneliti melakukan observasi lapangan. Selain itu peneliti juga melakukan wawancara dan diskusi dengan seluruh staff UPTTIK. Langkah terakhir yang dilakukan dalam penelitian ini yaitu penyebaran kuesioner. Kuesioner yang dibuat terkait dengan 4 domain dalam penelitian ini, yang juga mengacu kepada tingkat kematangan pada CMMI. Sedangkan untuk respondennya adalah seluruh staff UPTTIK mengingat seluruh staff UPTTIK adalah orang yang dianggap paling mengetahui terkait teknis pelaksanaan pengembangan dan pengelolaan aplikasi SIMAK. Kuesioner yang dibuat mengacu pada skala Guttman, ini adalah skala yang digunakan pada jawaban yang mempunyai sifat jelas atau tegas, seperti Ya – Tidak; Benar – Salah dan sebagainya [14]. Ini dilakukan mengingat peneliti hanya memerlukan jawaban tegas, yaitu Ya atau Tidak.

Setelah tahap penyebaran dan pengisian kuesioner selesai, maka langkah selanjutnya yaitu pengolahan data, pengolahan data dilakukan untuk mengetahui tingkat kematangan eksisting dan tingkat

kematangan harapan, setelah langkah tersebut selesai maka nilai kesenjangan yaitu antara nilai eksisting dan harapan dapat diketahui.

3. Hasil dan Pembahasan

Data – data yang dihimpun berupa dokumen foto, video atau dokumen lain yang menjadi data tambahan dalam penelitian. Hasil temuan pada domain 11 ISO/IEC 27002:2013 [15] disajikan pada **Tabel 3**.

Tabel 3. Hasil temuan (pemeriksaan) pada domain 11

Domain	A.11	Keamanan fisik dan lingkungan
Kategori keamanan utama	A.11.1	<i>secure area</i>
Kontrol keamanan	A.11.1.1	Perimeter atau pembatas keamanan fisik
No.	Pernyataan	Hasil Pemeriksaan
1.	Ruang server SIMAK dilindungi keamanan fisik berupa (pembatas kaca, dinding beton, dan kunci sidik jari)	Ruang server SIMAK telah dikendalikan dengan cukup baik, diantaranya terdapat pembatas kaca, pembatas dinding beton, kunci sidik jari sebanyak dua lapis.

Sumber: Data penelitian, 2020

Pemrosesan data dan kematangan

Bukti yang terkumpul dari hasil pemeriksaan dan pengumpulan barang bukti, maka akan dihasilkan perhitungan untuk setiap kontrol.

1. Perhitungan tingkat kematangan Domain A (Kebijakan keamanan informasi)

Berikut ini adalah hasil perhitungan tingkat kematangan domain A.5 yang dapat dilihat pada **Tabel 4**.

Tabel 4. Hasil perhitungan tingkat kematangan Domain A.5 (kebijakan keamanan informasi)

Domain	Kategori keamanan utama	Kontrol keamanan	Tingkat kemampuan	Rata – rata kontrol objektif
A.5 : Kebijakan keamanan informasi	A.5.1 : Arah manajemen untuk keamanan informasi	A.5.1.1 : Kebijakan untuk keamanan informasi	1,85	1,49
		A.5.1.2 : Review untuk kebijakan keamanan informasi		1,14
Tingkat kematangan domain A.5				1,49

Sumber: Data penelitian, 2020

Hasil perhitungan tingkat kematangan Domain A.5 dalam bentuk grafik, seperti yang terlihat pada **Gambar 2**.

Gambar 2. Hasil perhitungan tingkat kematangan Domain A.5

Sumber: Data penelitian, 2020

Hasil perhitungan menunjukkan bahwa domain A.5 mempunyai hasil kematangan 1,49 atau pada level *initial*, dimana pada hasil pemeriksaan tidak ditemukan kebijakan secara tertulis terkait keamanan informasi aplikasi SIMAK, seluruh instruksi dan kebijakan dilakukan secara lisan.

2. Perhitungan tingkat kematangan Domain A.6 (Keamanan informasi organisasi)

Berikut ini adalah hasil perhitungan tingkat kematangan domain A.6 yang dapat dilihat pada **Tabel 5**.

Domain	Kontrol objektif	Kontrol keamanan	Tingkat kemampuan	Rata – rata kontrol objektif
A.6 : Keamanan informasi organisasi	A.6.1 : Internal organisasi	A.6.1.1 : Peran dan tanggungjawab keamanan informasi A.6.1.2 : Pemisahan tugas A.6.1.3 : Kontak dengan pihak berwenang A.6.1.4 : Kontak dengan kelompok minat khusus A.6.1.5 : Keamanan informasi dalam manajemen proyek	2,14	1,56
	A.6.2 : Perangkat seluler dan teleworking	A.6.2.1 : Kebijakan perangkat seluler A.6.2.2 : Teleworking		
Tingkat kematangan domain A.5				1,49

Sumber: Data penelitian, 2020

Hasil perhitungan tingkat kematangan Domain A.6 dalam bentuk grafik, seperti yang terlihat pada **Gambar 3**.

Gambar 3. Grafik hasil perhitungan tingkat kematangan Domain A.6

Sumber: Data penelitian, 2020

Hasil perhitungan tingkat kematangan pada domain A.6 menunjukkan bahwa domain A.6 yaitu tentang keamanan informasi organisasi mempunyai nilai kematangan sebesar 1,52 atau pada level *repeatable*. Dimana organisasi berkomitmen untuk merencanakan proses standar. Namun banyak terdapat kontrol yang belum dilakukan secara terstandar, diantaranya adalah belum terdokumentasinya peran serta tanggungjawab terkait dengan keamanan informasi aplikasi SIMAK.

3. Perhitungan tingkat kematangan Domain A.9 (Kontrol akses)

Berikut ini adalah hasil perhitungan tingkat kematangan domain A.9 yang dapat dilihat pada **Tabel 5**.

Tabel 5. Hasil perhitungan tingkat kematangan Domain A.9 (kontrol akses)

Domain	Kontrol objektif	Kontrol keamanan	Tingkat kemampuan	Rata – rata kontrol objektif
A.9 : Kontrol akses	A.9.1 : Persyaratan bisnis untuk kontrol akses	A.9.1.1 : Kebijakan kontrol akses	1,57	1,35
		A.9.1.2 : Akses ke jaringan	1,14	
	A.9.2 : Manajemen akses pengguna	A.9.2.1 : Pendaftaran dan pencabutan akses pengguna	1,57	1,47
		A.9.2.2 : Penyediaan akses pengguna	2,28	
		A.9.2.3 : Pengelolaan hak akses istimewa	2	
		A.9.2.4 : Pengelolaan informasi rahasia pengguna	1	
		A.9.2.5 : Review hak akses pengguna	0,57	
		A.9.2.6 : Penghapusan atau penyesuaian hak akses	1,42	
	A.9.3 : Tanggungjawab pengguna	A.9.3.1 : Penggunaan informasi rahasia	0,71	0,71
	A.9.4 : Kontrol akses sistem dan aplikasi	A.9.4.1 : Pembatasan akses informasi	1,71	1,76
		A.9.4.2 : Pengamanan prosedur log-on	1,85	
		A.9.4.3 : Manajemen password	1,57	
		A.9.4.4 : Penggunaan program utilitas dengan hak akses level tinggi	1,57	
		A.9.4.5 : Kontrol akses terhadap source code program	2,14	
Tingkat kematangan domain A.5				1,32

Sumber: Data penelitian, 2020

Hasil perhitungan tingkat kematangan Domain A.9 dalam bentuk grafik, seperti yang terlihat pada **Gambar 4**. Berdasarkan hasil perhitungan tingkat kematangan, domain A.9 mendapatkan rata-rata nilai 1,32, dimana itu berarti berada pada level *initial*. Pada kasus ini proses standar telah dilakukan namun belum mengacu pada suatu standar tertentu, namun begitu masih banyak pula kontrol keamanan yang masih belum diterapkan.

Gambar 4. Grafik hasil perhitungan tingkat kematangan Domain A.9
Sumber: Penelitian, 2020.

4. Perhitungan tingkat kematangan Domain A.11 (Keamanan fisik dan lingkungan)

Berikut ini adalah hasil perhitungan tingkat kematangan domain A.11, ditunjukkan pada **Tabel 6**.

Tabel 6. Hasil perhitungan tingkat kematangan Domain A.11 (keamanan fisik dan lingkungan)

Domain	Kontrol objektif	Kontrol keamanan	Tingkat kemampuan	Rata – rata kontrol objektif
A.11 : Keamanan fisik dan lingkungan	A.11.1 : Area aman	A.11.1.1 : Pembatas keamanan fisik	3,28	2,04
		A.11.1.2 : Kontrol entri fisik	2,28	
		A.11.1.3 : Keamanan ruang dan fasilitas kantor	1,85	
		A.11.1.4 : Perlindungan dari ancaman luar (eksternal)	1,14	
	A.11.2 : Peralatan	A.11.2.1 : Penempatan dan perlindungan peralatan	2,28	1,91
		A.11.2.2 : Utilitas pendukung	2,71	
		A.11.2.3 : Keamanan kabel	1,85	
		A.11.2.4 : Perawatan asset	2	
		A.11.2.5 : Penghapusan aset	1,71	
		A.11.2.6 : Keamanan asset diluar lokasi	1,85	
		A.11.2.7 : Pembuangan atau penggunaan kembali peralatan	2,14	
		A.11.2.8 : Peralatan user yang tidak	1	

diawasi tanpa
pengawasan
A.11.2.9 : Kebijakan 1,71
clear screen dan
clear desk

Tingkat kematangan domain A.11	1,97
--------------------------------	------

Sumber: Data penelitian, 2020

Hasil perhitungan tingkat kematangan Domain A.9 dalam bentuk grafik, seperti yang terlihat pada Gambar 5.

Gambar 5. Grafik hasil perhitungan tingkat kematangan Domain A.11
Sumber: Data penelitian, 2020

Dari perhitungan tingkat kematangan domain A.11 atau terkait dengan keamanan fisik dan lingkungan, maka di dapatlah nilai 1,97, atau dengan kata lain domain A.11 berada pada level *repeatable*, itu artinya organisasi telah berkomitmen untuk merencanakan proses standar.

4. Kesimpulan

Untuk mengukur tingkat kematangan keamanan suatu aplikasi atau sistem informasi, dapat menggunakan kontrol keamanan pada domain ISO/IEC 27002:2013, langkah awalnya yaitu dengan identifikasi permasalahan yang terjadi pada sistem informasi, selanjutnya memilih dan menentukan domain yang akan digunakan untuk mengetahui tingkat keamanan pada sistem informasi. Setelah langkah tersebut selesai, selanjutnya yaitu dengan membuat kuesioner yang dibagikan kepada responden, pada penelitian ini responden yang dilibatkan adalah karyawan dan pimpinan dari UPTTIK yaitu yang bertanggungjawab sekaligus yang dianggap mengetahui tentang kondisi teknis sistem informasi akademik atau aplikasi SIMAK. Kuesioner yang dibuat yaitu terkait dengan domain yang pilih dalam penelitian yang dilakukan. Hasil dari kuesioner tersebut yang menjadi dasar acuan penilaian tingkat kematangan keamanan aplikasi SIMAK. Setelah kuesioner selesai, maka langkah selanjutnya yaitu melakukan pembobotan pada setiap kontrol keamanan yang dihasilkan dari setiap responden, selanjutnya adalah mencari rata – rata dari keseluruhan nilai yang dihasilkan dari setiap kontrol keamanan, nilai yang didapat dari penelitian yang telah dilakukan adalah domain 5 = 1,49 (*level initial*), domain 6 = 1,52 (*repeatable*), domain 9 = 1,32 (*initial*) dan domain 11 = 1,97 (*repeatable*) dari keempat domain yang dipakai dalam penelitian ini maka disimpulkan bahwa aplikasi SIMAK Universitas Siliwangi berada mempunyai nilai kematangan sebesar 1,57 atau berada pada level *repeatable*.

5. Singkatan

ISO International Organization for Standardization
IEC International Electrotechnical Commission

<i>SIMAK</i>	Sistem Informasi Akademik
<i>UPTTIK</i>	Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi
<i>ISMS</i>	Information Management System
<i>SMKI</i>	Sistem Manajemen Keamanan Informasi

7. Referensi

- [1] A. Hall, James, *Accounting Information Sistem*, Edisi ke 4, Salemba Empat, Jakarta, 2011.
- [2] Hermaduant, I. Riadi, *Automation framework for rogue access point mitigation in IEEE 802.1X-based WLAN*, *Journal of Theoretical and Applied Information Technology*, 2016.
- [3] Yakub, *Pengantar sistem informasi*, Edisi 1, Graha Ilmu, Yogyakarta, 2012.
- [4] O'Brien, A. James. G. M. Marakas, *Analisa Sistem Informasi*, Ed 1, Andy, Yogyakarta, 2016.
- [5] Riadi, Imam, J. E. Istiyanto, A. Ashari, Subanar, "Internet Forensics Framework Based-on Clustering," *Int. J. of Advanced Computer Science and Applications (IJACSA)*, 4(12), 2013.
- [6] Nugroho, Anggun, Perancangan Sistem Informasi Pengelolaan UKM STIMIK STIKOM Bali Berbasis Client Server, Konferensi Nasional Sistem & Informatika, 2015.
- [7] Krismaji, Sistem Informasi Akuntansi, Edisi Ketiga, Sekolah Tinggi Ilmu Manajemen, Yogyakarta, 2015.
- [8] Hutahae, Jeperson, *Konsep Sistem Informasi*, 1th ed. Budi Utama, Yogyakarta, 2014.
- [9] Stair, R, Reynolds, G, *Principles of Information System, Tenth Edition*, Nelsol Education, Boston, 2012.
- [10] Rosmiati, Riadi, Imam, Prayudi, Yudi, A Maturity Level Framework for Measurement of Information Security Performance, *Int. J. of Computer Applications*, 141. 975-8887. 10.5120/ijca2016907930, Yogyakarta, 2016.
- [11] Kurniawan, Endang Riadi, Imam, *Security Level Analysis of Academic Information System Based on Standard ISO 27002:2013 Using SSE CMM*, *IJCSIS Vol.16 No.1*, 2018.
- [12] Gelindas, Ulrich, Dull, B. Richard, *Accounting Information Systems 9th Edition*, South Westrn Cengage Learning, Natorp Boulevard Mason, USA, 2012.
- [13] Imelda, Erik, Muhammad, Perancangan Sistem Inofrmasi Akdemik pada Sekolah Dasar Negeri Sukajadi 9 Bandung, Volume 3, JATI, Jurnal Teknologi dan Informasi UNIKOM, BANDUNG 2013.
- [14] Sugiyono, *Metode Penelitian Bisnis*, Edisi 2, CV. Alfabeta. Bandung, 2011.
- [15] ISO/IEC 27002, International Standard, Information technology - security techhniques - code of practice for information security control, Second Edition, 2013.